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

Linara Stéfani Facini

Uma introdução aos corpos não abelianos de grau menor ou igual a 6

São José do Rio Preto
2021

Linara Stéfani Facini

Uma introdução aos corpos não abelianos de grau menor ou igual a 6

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

Orientador: Prof. Dr. Antonio Aparecido de Andrade
UNESP - Câmpus de São José do Rio Preto

Financiadora: CNPq

São José do Rio Preto
2021

F141i

Facini, Linara Stéfani
Uma introdução aos corpos não abelianos de grau menor ou igual a 6 / Linara Stéfani Facini. -- São José do Rio Preto, 2021
190 p. : tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientador: Antonio Aparecido de Andrade

1. Teoria Algébrica dos Números. 2. Corpos de Números. 3. Anel de inteiros algébricos. 4. Reticulados algébricos. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Linara Stéfani Facini

Uma introdução aos corpos não abelianos de grau menor ou igual a 6

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

Financiadora: CNPq

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
UNESP - Câmpus de São José do Rio Preto
Orientador

Prof. Dr. Leandro Bezerra de Lima
UFMS - Câmpus de Aquidauana

Profa. Dra. Andréia Cristina Ribeiro
UFMS - Câmpus de Paranaíba

São José do Rio Preto
01 de outubro de 2021

A Deus e à minha família,
dedico.

AGRADECIMENTOS

Ao concluir este trabalho agradeço:

A Deus, pela força, sabedoria e saúde em todos os momentos da minha vida.

À minha mãe, Zilda, pelo cuidado, carinho e amor incondicional. Obrigada por ser minha grande inspiração e tenha certeza que lhe dar orgulho é minha motivação de viver.

À minha irmã, Lorena, pelo carinho, apoio e por proporcionar que os momentos difíceis fossem mais doces.

Ao meu noivo, Marlon, pelo incentivo ao estudo e por sempre estar ao meu lado me aconselhando e compartilhando cada momento com carinho e amor.

Ao meu pai do coração, Marcos, pelos conselhos sábios, pelo incentivo, pela cumplicidade e por toda ajuda durante esta jornada.

Aos amigos da Matemática, pela amizade, pelos momentos incríveis, pelo apoio e por todas as alegrias que compartilhamos; Gabriel Fazoli pela inspiração e pelos melhores ensinamentos; Eliani, Giovana, Jaqueline, Mariele, Natália, Raquel, André, Carlos, João Pedro, Lucas, Mateus, Maurício, Pedro, Vinícius e Yuri pela harmoniosa convivência durante a graduação; Lucas, Yen e Drielly pelo apoio e amizade; Livea, Maria Clara, Maria Fernanda, Murillo e Plínio por compartilhar o amor pela álgebra e pelas inúmeras discussões produtivas.

Aos meus professores, pelos grandes ensinamentos durante toda minha vida acadêmica. Em especial, às professoras Daniela Mazzoco, Profa. Dra. Aparecida Francisco da Silva, Profa. Dra. Maria Gorete Carreira Andrade e Profa. Dra. Adriana Barbosa Santos por me conduzirem por esse mundo maravilhoso da matemática, sempre me aconselhando e incentivando.

Aos colaboradores da OBMEP, Victor, Adriana e Carlos, pelos momentos de descontração e pela amizade adquirida.

Ao meu orientador, Toninho, pela paciência, pelos valiosos ensinamentos e pelos melhores conselhos. Agradeço por toda confiança que depositou em mim ao desen-

volver este trabalho e por ser meu maior incentivador. "Se existe um jeito de crescer é através dos estudos", faço de suas palavras minha inspiração.

Aos professores titulares da comissão examinadora, Prof. Dr. Leandro Bezerra de Lima e Profa. Dra. Andréia Cristina Ribeiro e aos professores suplentes da comissão examinadora, Prof. Dr. Edson Donizete Carvalho e Profa. Dra. Tatiana Bertoldi Carlos, por aceitarem fazer parte deste momento tão especial e pelas valiosas contribuições.

Ao CNPq, pelo auxílio financeiro que possibilitou a dedicação deste trabalho.

À Universidade Estadual Paulista, "Júlio de Mesquita Filho- Instituto de Biociências, Letras e Ciências Exatas - Câmpus de São José do Rio Preto, por me proporcionar a estrutura necessária para que este sonho fosse realizado. Em especial, à equipe da seção de pós graduação, que sempre estiveram de prontidão para atender minhas dúvidas.

A todos que direta ou indiretamente contribuíram na realização deste trabalho.

"Não se esqueça todos os dias de olhar em 6 direções,
Para frente: para saber onde você está indo e planejar com antecedência;
Para trás: para lembrar de onde você veio e evitar os erros do passado;
Para baixo: para se certificar de que não está pisando em outras pessoas e que está edificando seu caminho;
Para os lados: para ver quem está lá para apoia-lo, e ver quem precisa do seu apoio;
Para cima: para se lembrar que Deus está no controle e cuida de tudo e todos;
Para dentro: Para sermos gratos pelo que temos, encontrar a paz quando não temos, crescer e contribuir com compaixão quando devemos".
(Mahatma Gandhi, [1])

RESUMO

Neste trabalho apresentamos os conceitos básicos da Teoria Algébrica dos Números com o objetivo da construção de reticulados por intermédio dos corpos de números de grau $n = 2, 3, 4, 5, 6$. Neste contexto, apresentamos os corpos de números construídos através dos polinômios irredutíveis $p(x) = x^n + ax + b$, com a e b inteiros não nulos e $p(x) = x^n - d$, com d inteiro livre de quadrados. Além disso, apresentamos o anel de inteiros algébricos e o discriminante desses corpos e através do homomorfismo de Minkowski construímos reticulados algébricos a partir da aplicação via o anel de inteiros desses corpos.

Palavras-chave: Teoria Algébrica dos Números. Corpos de Números. Anel de inteiros algébricos. Reticulados algébricos.

ABSTRACT

In this work we present the basic concepts of Algebraic Number Theory with the objective of constructing lattices through the number fields of degree $n = 2, 3, 4, 5, 6$*. In this context, we present the number fields constructed through the irreducible polynomials* $p(x) = x^n + ax + b$*, with* a *and* b *non-zero integers and* $p(x) = x^n - d$*, with* d *an integer square free. Furthermore, we present the algebraic integer ring and the discriminant of these fields and through Minkowski homomorphism we build algebraic lattices via the algebraic integer ring of these fields.*

Keywords: Algebraic Number Theory. Numbers Fields. Ring of algebraic integers. Algebraic lattices.

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{C}$	Conjunto dos números complexos
A, B	Anéis
M	A-módulo
$\mathbb{K}, \mathbb{L}$	Corpos
$\mathbb{K} \subseteq \mathbb{L}$	O corpo $\mathbb{L}$ é uma extensão do corpo $\mathbb{K}$
$\sum$	Somatório
$\prod$	Produtório
$Ker(\varphi)$	Núcleo da função φ
$Im(\varphi)$	Imagem da função φ
$a \equiv b(mod\ m)$	a é congruente a b módulo m
$\frac{M}{N}$	Conjunto quociente
$\mathbb{Z}_m$	Conjunto das classes residuais módulo m
$A[\alpha]$	Menor anel que contém A e α
$\det(M)$	Determinante da matriz M
$\mathcal{O}_B(A)$	Anel de inteiros de B sobre A
p(x)	Polinômio em x
$\mathcal{O}_{\mathbb{K}}$	Anel de inteiros de $\mathbb{K}$
$\mathcal{T}r_{B\|A}(\varphi)$	Traço relativo a φ de B sobre A

$\mathcal{N}_{B\|A}(\varphi)$	Norma relativa a φ de B sobre A
$\mathbb{Q}(\theta)$	corpo de números com o elemento primitivo θ
$\mathcal{T}r(\alpha)$	Traço do elemento α via corpo de números
$\mathcal{N}(\alpha)$	Norma do elemento α via corpo de números
$f_\alpha(x)$	Polinômio característico de α via corpo de números
$\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n)$	Discriminante de $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ via corpo de números
$\mathcal{D}(\mathbb{K})$	Discriminante da base integral de $\mathbb{K}$
ξ_n^k	Raiz primitiva da unidade de $p(x) = x^n - 1$
$\partial(p)$	Grau do polinômio $p(x)$
$[\mathbb{K} : \mathbb{Q}]$	Grau da extensão $\mathbb{Q} \subseteq \mathbb{K}$
$\forall$	Para todo
$\nexists$	Não existe
Λ_B	Reticulado com base B
$\mathcal{P}_B$	Região fundamental do reticulado Λ sobre a base B
$\mathcal{V}(\Lambda)$	Volume do reticulado Λ
$\mathcal{V}(\mathcal{P})$	Volume da região fundamental $\mathcal{P}$
$(\Lambda_{\min})^2$	Norma mínima do reticulado Λ
ρ	Raio de empacotamento do reticulado
$\Delta(\Lambda)$	Densidade de empacotamento associada ao reticulado Λ
$\delta(\Lambda)$	Densidade de centro associada ao reticulado Λ
r_1	Quantidade de monomorfismos reais do corpo $\mathbb{K} = \mathbb{Q}(\theta)$
r_2	Metade da quantidade de monomorfismos complexos do corpo $\mathbb{K} = \mathbb{Q}(\theta)$
$\sigma_{\mathbb{K}}$	Homomorfismo de Minkowski
$\Re(x)$	Parte real de x
$\Im(x)$	Parte imaginária de x
$\mathcal{N}(\mathcal{I})$	Norma do ideal $\mathcal{I}$

Sumário

1 Introdução

Segundo o matemático Leopold Kronecker (1823-1891) "Deus criou os números inteiros e o resto é obra da humanidade". A Teoria dos Números é a mais bela constituição matemática, uma área que instiga o fascínio da mente humana desde as mais remotas épocas da antiguidade, desafiando inúmeras gerações de matemáticos e leigos, que apreciam os seus enunciados simples e intrigantes, cujas demonstrações estão além de qualquer simplicidade. A origem da Teoria dos Números é geralmente atribuída aos gregos, por volta de 600 a.C. Pitágoras e seus discípulos fizeram vários estudos interessantes e foram os primeiros a classificar os inteiros de várias maneiras como por exemplo: números pares, ímpares e primos. A Teoria dos Números é a área da matemática cujo objetivo é descobrir e estabelecer as relações profundas e sutis que números de tipos diferentes guardam entre si.

Ao decorrer das estações, novos problemas foram surgindo e novas teorias foram desenvolvidas. A ramificação da área chamada Teoria Algébrica dos Números, foi criada na segunda metade do século XIX nos trabalhos dos matemáticos Ernest Kummer (1810–1893), Richard Dedekind (1831–1916), Emmy Noether (1882-1935) e Leopold Kronecker (1823–1891). Essa teoria teve suas origens quando o matemático alemão Carl F. Gauss (1777–1855) estendeu a ideia de número inteiro definindo o anel dos inteiros algébricos gaussianos, $\mathbb{Z}[i]$, e posteriormente na tentativa de se demonstrar o Último Teorema de Fermat. Nestes parágrafos foram utilizadas as referências [2] e [3] para a descrição histórica.

Contudo, os estudos nesta área podem parecer um pouco complexos e até pouco tempo atrás não tinham aplicações diretas. Então, mais uma vez, a Teoria Algébrica dos Números surge de forma encantadora quebrando paradigmas e se eleva a era moderna como tendência à aplicações a comunicação. Em 1948, para achar os limites fundamentais no processamento de sinais e operações de comunicação como as de compressão de dados, o matemático Claude E. Shannon publicou o artigo *A Mathematical Theory of Communication*. Este artigo instigou a origem à Teoria da Informação, que possibilitou a junção entre a Matemática e a Engenharia Elétrica na qual se objetiva garantir uma transmissão segura e eficiente de informações por meio dos canais de comunicação, além da criação da Teoria de Códigos Corretores de Erros, que permitem uma melhor qualidade na transmissão de sinais e dados. Agora essa teoria tem várias aplicações nas mais diversas áreas, como a Álgebra, a Teoria dos Números Clássica e a Teoria Algébrica dos Números.

Um problema atual contido na Teoria da Informação é o empacotamento esférico, que consiste em dispor esferas de mesmo raio no espaço euclidiano n-dimensional de tal modo que no máximo duas delas se tangenciem e elas ocupem a maior fração deste espaço, ou seja, que esta distribuição tenha alta densidade. Ao conjunto de pontos centrais das esferas é dado o nome de reticulado. Com a publicação do artigo de Shannon, ficou

estabelecido que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes e assim, é possível associar o estudo dos códigos aos reticulados de modo que, ao transmitir uma mensagem (código) emitimos um vetor, se esse vetor for enviado diretamente ao centro da esfera a mensagem foi entregue com sucesso, caso o vetor atinja o interior da esfera no processo a mensagem foi entregue com erro, ou seja, aconteceu o chamado "ruído" mas é possível corrigi-la, agora se o vetor atingir os espaços entre as esferas a mensagem por sua vez acaba se perdendo e é menos provável de haver uma correção. Nestes parágrafos foram utilizadas as referências [3], [4] e [5].

Nesse sentido, o presente trabalho tem por objetivo estudar os anéis de inteiros algébricos de alguns corpos de números, os discriminantes associados e a aplicação à construção de reticulados via corpos de números (definiremos esses conceitos no texto). Para cumprir este propósito, organizamos este trabalho em nove capítulos, onde esta introdução é o primeiro. O segundo capítulo, é uma introdução à Teoria Algébricas dos Números e é fundamental a familiaridade com conceitos básicos como a teoria de anéis e a teoria de extensões de corpos, que podem ser encontradas nas referências [5] e [6], respectivamente. Os conteúdos explorados, neste capítulo, são módulos e módulos livres, anel dos inteiros, norma, traço, discriminante e a particularização de alguns resultados para os corpos de números. Em especial, como contribuição deste trabalho, a seção 2.6 apresenta resultados novos, não conhecidos na literatura, sobre os corpos de números $\mathbb{Q}(\sqrt[n]{d})$, com $d \in \mathbb{Z}$ livre de quadrados que surgiram como inspiração das referências [7], [8] e [9].

Do terceiro ao sétimo capítulo, apresentamos um investigação das extensões de corpos de números de grau 2, 3, 4, 5 e 6, respectivamente. A estes capítulos damos o devido reconhecimento, e atribuímos-os como os principais dessa dissertação. Através dos polinômios irredutíveis $p(x) = x^n + ax + b$, com a, b inteiros não nulos e $p(x) = x^n - d$, com d um inteiro livre de quadrados, permite-se encontrar o anel dos inteiros algébricos e o discriminante em cada caso. No capítulo 3, tratamos das extensões quadráticas cujo o polinômio minimal $p(x) = x^2 - d$, com d um inteiro livre de quadrados, embora para este caso a base integral seja conhecida, apresentamos a nossa versão da demonstração. No capítulo 4, tratamos das extensões cúbicas cujo o polinômio minimal $p(x) = x^3 - d$, com d um inteiro livre de quadrados, neste caso a base integral que encontramos é sutilmente diferente a da referência [7]. No capítulo 5, tratamos das extensões quárticas cujo o polinômio minimal $p(x) = x^4 - d$, com d um inteiro livre de quadrados, neste caso, a base integral encontrada na referência [8] não está completa, uma vez que não cobre o caso quando $d \equiv 1 \pmod 8$. Assim, nesse trabalho apresentamos uma nova versão (de nossa autoria) do anel dos inteiros desses corpos para qualquer inteiro $d \neq 1$ e livre de quadrados completando a referência [8]. Em especial, os capítulos 6 e 7 trazem consigo resultados novos de nossa autoria, não conhecidos na literatura, como o anel dos inteiros algébricos e o discriminante dos corpos $\mathbb{Q}(\sqrt[n]{d})$, com d um inteiro livre de quadrados e para $n = 5, 6$.

A aplicação aos reticulados é encontrado no oitavo capítulo. O ápice é construir alguns exemplos de reticulados algébricos a partir dos anéis de inteiros algébricos discutidos nos capítulos antecedentes. Para isso, definimos a estrutura de um reticulado no $\mathbb{R}^n$, matriz geradora, matriz de Gram, volume, raio de empacotamento e densidade de centro. Posteriormente, na seção de reticulados algébricos faremos a particularização para este caso.

No nono capítulo, apresentamos a conclusão deste trabalho e as perspectivas futuras com alguns caminhos em aberto que podem ser seguidos.

2 Introdução à Teoria Algébrica dos Números

Este capítulo tem como objetivo embasar e fundamentar todo o trabalho. Apresentamos, uma introdução da Teoria Algébrica dos Números, onde apresentaremos as principais definições e importantes resultados que envolvem-na. Abordaremos os conceitos de módulo e módulo livre na primeira seção, seguindo por anel dos inteiros, norma, traço e discriminante, todos esses assuntos citados serão cruciais para sustentar a última seção que se trata dos corpos de números. Algumas demonstrações serão omitidas, por serem resultados clássicos ou pela sua extensa demonstração, contudo estes resultados serão propriamente referenciados. Admitiremos os conhecimentos prévios da Álgebra Clássica que envolvem as estruturas de grupos, anéis e corpos, onde o leitor pode se familiarizar com estes assuntos em [6]. No mais, serão usados os conhecimentos da Álgebra Linear Clássica, como os espaços vetoriais, que podem ser reforçados pela leitura em [10]. Em especial, como contribuição deste trabalho, a seção 2.6 apresenta resultados novos, não conhecidos na literatura, sobre os corpos de números $\mathbb{Q}(\sqrt[n]{d})$, com $1 \neq d \in \mathbb{Z}$ livre de quadrados, que surgiram como inspiração das referências [8], [7] e [9].

2.1 Módulos e módulos livres

Na Álgebra Linear Clássica é comum usarmos os espaços vetoriais sobre corpos, principalmente sobre $\mathbb{R}$ ou $\mathbb{C}$. O conceito de módulos surgiu então da tentativa de usar anéis arbitrários no lugar de corpos. Faremos uma generalização dos espaços vetoriais como módulos e uma breve apresentação dos módulos livres, cuja as referências bases são o Capítulo 2 de [5], o Capítulo 3 de [11] e o Capítulo 2 de [12]. Ao longo deste capítulo, consideramos A como sendo um anel comutativo com unidade.

Definição 2.1.1. *Seja M um conjunto não vazio. A terna $(M, +, \cdot)$ com as operações $+ : M \times M \to M$ e $\cdot : A \times M \to M$ é chamada de um **A-módulo** (ou um módulo sobre A) se satisfaz as seguintes propriedades:*

1. *$(M, +)$ é um grupo abeliano;*
2. *$a(bm) = (ab)m$ e $(a + b)m = am + bm$, para todo $a, b \in A$ e $m \in M$;*
3. *$a(m + n) = am + an$, para todo $a \in A$ e $m, n \in M$;*
4. *$1m = m$, para todo $m \in M$.*

Exemplo 2.1.1. *São exemplos de A-módulos.*

1. *Todo espaço vetorial V sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo, pois as estruturas de espaço vetorial e módulo se assemelham ao analisarmos que $\mathbb{K}$ também é um anel.*

2. *Todo grupo abeliano G é um $\mathbb{Z}$-módulo, pois satisfaz o primeiro item da definição de módulo por ser um grupo abeliano e para os demais itens basta vermos que $nx = x + \cdots + x$, assim também são satisfeitos.*

3. *Sejam A um anel e $I \subseteq A$ um ideal. Assim, o ideal I de A é um A-módulo, este resultado segue pela definição de ideal que satisfaz as propriedades de módulo. Em particular, A é um módulo sobre si mesmo.*

Definição 2.1.2. *Seja M um A-módulo. Um subconjunto $N \subseteq M$ é chamado um* ***A-submódulo de M*** *se satisfaz:*

1. $0 \in N$;

2. $a + b \in N$, *para quaisquer* $a, b \in N$;

3. $an \in N$, *para quaisquer* $a \in A$ *e* $n \in N$.

Observação 2.1.1. *A definição de A-submódulo pode ser reformulada da seguinte maneira. Seja M um A-módulo. Um subconjunto não vazio N de M é chamado um A-submódulo de M quando N é um subgrupo de M e a operação "produto por escalar" é fechada em N. Observemos por essa definição que $0 \in N$, uma vez que $N \neq \emptyset$, e assim, existe $u \in N$ tal que $0 = u - u \in N$. Além disso, N é por si um A-módulo.*

Exemplo 2.1.2. *Seja V um espaço vetorial sobre um corpo K. Um subconjunto $U \subseteq V$ é um K-submódulo de V se, e somente se, U é um subespaço vetorial de V.*

Exemplo 2.1.3. *Seja M um A-módulo. Se $\{N_i\}_{i \in I}$ é uma família de A-submódulos de M, com $I = \{1, 2, \ldots, k\}$ um conjunto finito, então os seguintes conjuntos são A-submódulos de M:*

1. $\sum_{i=1}^{k} N_i := \{u_1 + u_2 + \cdots + u_k | u_i \in N_i\}$.

2. $\bigcap_{i=1}^{k} N_i := \{u | u \in N_i, \forall i \in I\}$.

Os próximos resultados serão referentes aos homomorfismos de A-módulos. De modo análogo ao caso de homomorfismo de anéis, apresentamos a definição, algumas propriedades e definimos o módulo quociente com o objetivo de provar uma versão do Teorema do Homomorfismo para módulos.

Definição 2.1.3. *Sejam A um anel e M e N A-módulos. Uma aplicação $\varphi : M \to N$ é um* ***homomorfismo de A-módulos*** *se satisfaz:*

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$, *para todo* $x, y \in M$.

2. $\varphi(ax) = a\varphi(x)$, *para todo* $a \in A$ *e* $x \in M$.

Se φ for bijetora, a aplicação φ é chamada um ***isomorfismo de A-módulos*** *e que M e N são isomorfos como A-módulos, e denotado por $M \cong_A N$.*

Observação 2.1.2. *Denotemos o conjunto de todos os A-homomorfismos de M em N por $Hom_A(M,N)$ (ou simplesmente por $Hom(M,N)$, se não houver dúvida sobre qual é o anel A). O conjunto $Hom_A(M,N)$ também é um A-módulo.*

Definição 2.1.4. *Sejam A um anel, M e N A-módulos e $\varphi : M \to N$ um homomorfismo de A-módulos.*

1. *O **núcleo** (kernel) de φ é definido por $Ker(\varphi) = \{x \in M | f(x) = 0\}$.*
2. *A **imagem** de φ é definida por $Im(\varphi) = Im(M) = \{\varphi(x) | x \in M\}$.*

Proposição 2.1.1. *Sejam M e N dois A-módulos e $\varphi : M \to N$ um homomorfismo de A-módulos.*

1. *$Ker(\varphi)$ é um A-submódulo de M.*
2. *$Im(\varphi)$ é um A-submódulo de N.*
3. *A aplicação φ é injetora se, e somente se, $Ker(\varphi) = \{0\}$.*

Demonstração. Para o prova dos itens (1) e (2) faremos uso da Observação 2.1.1 para provar que o kernel e a imagem são A-submódulos.

1. Vejamos que $Ker(\varphi) \neq \emptyset$, pois $\varphi(0) = 0$, e dessa forma, $0 \in Ker(\varphi)$. Agora, supomos que $u, v \in Ker(\varphi)$ e $a \in A$. Assim, $\varphi(u - v) = \varphi(u) - \varphi(v) = 0$, ou seja, $u - v \in Ker(\varphi)$. Por outro lado, $\varphi(au) = a\varphi(u) = 0$, e assim, $au \in Ker(\varphi)$. Portanto, $Ker(\varphi)$ é um A-submódulo de M.

2. Neste caso $Im(\varphi) \neq \emptyset$, pois $0 \in Im(\varphi)$. Agora, suponhamos que $u, v \in Im(\varphi)$ e $a \in A$. Logo, existem $m_1, m_2 \in M$ tal que $\varphi(m_1) = u$ e $\varphi(m_2) = v$, e assim, $u - v = \varphi(m_1) - \varphi(m_2) = \varphi(m_1 - m_2)$, ou seja, $u - v \in Im(\varphi)$. Por outro lado, $au = a\varphi(m_1) = \varphi(am_1)$, e deste modo, $au \in Im(\varphi)$. Portanto, $Im(\varphi)$ é um A-submódulo de N.

3. Suponhamos que φ é injetora e seja $x \in Ker(\varphi)$. Assim, $\varphi(x) = 0 = \varphi(0)$. Como φ é injetora, segue que $x = 0$, e consequentemente, $Ker(\varphi) = \{0\}$. Reciprocamente, suponhamos $u, v \in M$ tal que $\varphi(u) = \varphi(v)$. Logo, $\varphi(u - v) = \varphi(u) - \varphi(v) = 0$, e assim, $u - v \in Ker(\varphi) = \{0\}$. Portanto, $u - v = 0$, ou seja, $u = v$, implicando que φ é injetora.

Portanto, a proposição está provada. □

Neste momento, apresentamos algumas definições que acercam o módulo quociente, para defini-lo e provar o Teorema do Homomorfismo.

Definição 2.1.5. *Sejam M um A-módulo, N um A-submódulo de M.*

1. *Sejam $u, v \in M$. O elemento u é chamado **congruente** a v módulo N se $u - v \in N$. Esta relação é de equivalência e denotamos por $u \equiv v (mod\ N)$.*
2. *A **classe de equivalência** de $u \in M$ é dada por $\overline{u} = \{v \in M | u \equiv v (mod\ N)\}$.*

Definição 2.1.6. *Sejam M um A-módulo, $u \in M$ e N um A-submódulo de M.*

1. *O conjunto $u + N = \{u + v : v \in N\}$ é chamado de **classe lateral à esquerda**.*

2. *O conjunto* $N + u = \{v + u : v \in N\}$ *é chamado de* ***classe lateral à direita****.*

Definição 2.1.7. *Sejam* M *um* A*-módulo,* N *um* A*-submódulo de* M*. O conjunto quociente* $\frac{M}{N} = \{u + N | u \in M\}$ *com as operações:*

1. $(u + N) + (v + N) = (u + v) + N$*, com* $u, v \in M$*.*
2. $a(u + N) = au + N$*, com* $u \in M$ *e* $a \in A$*.*

é um A*-módulo e é chamado de* ***módulo quociente****.*

Teorema 2.1.1. *Se* $\varphi : M \to N$ *é um homomorfismo de* A*-módulos, então*

$$\frac{M}{Ker(\varphi)} \cong Im(\varphi).$$

Demonstração. A aplicação

$$\begin{aligned} \phi : \frac{M}{Ker(\varphi)} &\longrightarrow \varphi(M) \\ u + Ker(\varphi) &\mapsto \varphi(u) \end{aligned}$$

é um isomorfismo.

1. A aplicação ϕ está bem definida. Sejam $u + Ker(\varphi), v + Ker(\varphi) \in \frac{M}{Ker(\varphi)}$ tal que $u + Ker(\varphi) = v + Ker(\varphi)$. Assim, $u - v \in Ker(\varphi)$, ou seja, $\varphi(u - v) = 0$. Dessa forma, como φ é um homomorfismo, segue que $\varphi(u - v) = \varphi(u) - \varphi(v) = 0$. Assim, $\varphi(u) = \varphi(v)$, e por definição, $\phi(u + Ker(\varphi)) = \phi(v + Ker(\varphi))$. Portanto, ϕ está bem definida.

2. A aplicação ϕ é um homomorfismo, uma vez que

   (a) $\phi((u + Ker(\varphi)) + (v + Ker(\varphi))) = \phi((u + v) + Ker(\varphi)) = \varphi(u + v) = \varphi(u) + \varphi(v) = \phi(u + Ker(\varphi)) + \phi(v + Ker(\varphi))$,

   (b) $\phi(a(u + Ker(\varphi))) = \phi(au + Ker(\varphi)) = \varphi(au) = a\varphi(u) = a\phi(u + Ker(\varphi))$,

   para $u + Ker(\varphi), v + Ker(\varphi) \in \frac{M}{Ker(\varphi)}$ e $a \in A$. Assim, ϕ é um homomorfismo.

3. A aplicação ϕ é injetora. Suponhamos $\phi(u + Ker(\varphi)) = \phi(v + Ker(\varphi))$, com $u + Ker(\varphi), v + Ker(\varphi) \in \frac{M}{Ker(\varphi)}$. Logo, $\varphi(u) = \varphi(v)$, e assim, $\varphi(u - v) = \varphi(u) - \varphi(v) = 0$, ou seja, $u - v \in Ker(\varphi)$ e isso implica que $u + Ker(\varphi) = v + Ker(\varphi)$. Portanto, ϕ é injetora.

4. A aplicação ϕ é sobrejetora. Seja $v \in \varphi(M)$, assim existe $u \in M$ tal que $\varphi(u) = v$. Logo, podemos ver que existe $u + Ker(\varphi) \in \frac{M}{Ker(\varphi)}$ tal que $\phi(u + Ker(\varphi)) = \varphi(u) = v$. Portanto, ϕ é sobrejetora.

Concluímos dos itens 1), 2), 3) e 4) que ϕ é um isomorfismo, e portanto, $\frac{M}{Ker(\varphi)}$ e $Im(\varphi)$ são isomorfos. □

Definição 2.1.8. *Sejam $\{M_i\}_{i\in I}$ uma família de A-módulos e $M = \prod_{i\in I} M_i$. Seja $\{N_i\}_{i\in I}$ uma família de A-submódulos de M. A soma $M = \sum_{i\in I} N_i$ é a chamada* ***soma direta*** *de $\{N_i\}_{i\in I}$, e denotamos por $M = \oplus_{i\in I} N_i$, se satisfaz uma das seguintes afirmações.*

1. *Todo elemento $m \in M$ se escreve de maneira única na forma $m = \sum_{i\in I} n_i$, onde $n_i \in N_i$, e $(n_i)_{i\in I}$ é uma família quase nula, isto é, $n_i = 0$, exceto para um número finito de elementos.*

2. *Se $M = \sum_{i\in I} N_i$ e $\sum_{i\in I} n_i = 0$, então $n_i = 0$ para todo $i \in I$.*

3. *Se $M = \sum_{i\in I} N_i$ e $N_j \cap \left(\sum_{i\neq j} N_i\right) = \{0\}$.*

Definição 2.1.9. *Seja $\{M_i\}_{i\in I}$ uma família de A-módulos. O* ***produto direto*** *dos M_i's é definido como o A-módulo $\prod_{i\in I} M_i = \{(m_i)_{i\in I} | m_i \in M_i, \forall i \in I\}$ e cujas operações de adição e produto por escalar são definidas índice a índice.*

Observação 2.1.3. *Observamos que se o conjunto de índices I for finito, então o produto direto e a soma direta coincidem.*

Na próxima definição, apresentamos alguns conceitos essenciais para a definição de uma base.

Definição 2.1.10. *Sejam M um A-módulo e S um subconjunto de M não vazio.*

1. *Os elementos de S são chamados* ***linearmente independentes*** *se, para toda a família finita $\{v_1, v_2, \ldots, v_n\}$ de elementos de S e $a_1, a_2, \ldots, a_n \in A$ implicar que*

$$a_1v_1 + \cdots + a_nv_n = 0 \Rightarrow a_1 = a_2 = \cdots = a_n = 0.$$

   Caso contrário, os elementos de S são chamados ***linearmente dependentes****.*

2. *O conjunto S é chamado* ***gerador*** *de M se $M = \langle S \rangle$, ou seja, qualquer elemento $m \in M$ pode ser escrito como uma combinação linear (em geral, não única) de elementos de S dada por*

$$m = \sum_{i=1}^{k} a_i v_i,$$

   onde $a_i \in A$ e $v_i \in S$.

3. *O A-módulo M é chamado de* ***tipo finito*** *se o M possui um conjunto gerador finito.*

4. *Um conjunto S é chamado uma* ***base*** *de M se é um conjunto gerador cujos elementos são linearmente independentes. Neste caso, qualquer elemento $m \in M$ pode ser escrito de forma única como uma combinação linear de elementos de S, ou seja,*

$$m = \sum_{i=1}^{k} = a_i v_i,$$

   onde $a_i \in A$ e $v_i \in S$. O número de elementos da base é chamado de ***posto*** *de M.*

5. *O A-módulo M é chamado* ***livre*** *se o M possui uma base.*

Exemplo 2.1.4. *A seguir, apresentamos alguns exemplos de módulos livres.*

1. *Todo espaço vetorial é um módulo livre, pois tem base.*
2. *Nem todo A-módulo é livre. Por exemplo, $\mathbb{Q}$ não é um $\mathbb{Z}$-módulo livre.*
3. *O grupo $\mathbb{Z}_m$ é um $\mathbb{Z}$-módulo que não tem base, uma vez que $\mathbb{Z}_m$ é um $\mathbb{Z}$-módulo, pois é um grupo abeliano. Agora, para qualquer $a \in \mathbb{Z}_m$, segue que $1a = (m+1)a$, ou seja, não escrevemos de maneira única. Assim, $\mathbb{Z}_m$ não tem base, e portanto, não é um $\mathbb{Z}$-módulo livre.*

Definição 2.1.11. *Sejam I um conjunto arbitrário e A um anel. Se a cada $i \in I$ associarmos uma cópia de A como um A-módulo podemos formar o A-módulo livre $M = \oplus_{i\in I} A$. Neste caso, o módulo M é chamado de* ***módulo livre gerado*** *pelo conjunto I.*

Nas Definições 2.1.10 e 2.1.11 podemos introduzir a ideia de módulo livre do tipo finito e módulo finitamente gerado, considerando os conjuntos S e I finitos em cada uma delas.

Teorema 2.1.2. *Se M é um A-módulo livre, então duas bases finitas quaisquer de M devem ter a mesma cardinalidade (a qual é chamada de posto de M).*

Demonstração. Suponhamos que $\{u_1, u_2, \ldots, u_m\}$ e $\{v_1, v_2, \ldots, v_n\}$ são duas bases de M. Assim, existem $b_{ij}, c_{kl} \in A$, com $i, k \in \{1, 2, \ldots, m\}$ e $j, l \in \{1, 2, \ldots, n\}$ tal que

$$u_i = \sum_{j=1}^{n} b_{ij} v_j \text{ e } v_k = \sum_{l=1}^{m} c_{kl} u_l.$$

Reescrevendo esses termos, segue que

$$u_i = \sum_{j=1}^{n} b_{ij} v_j = \sum_{j=1}^{n} b_{ij} \sum_{l=1}^{m} c_{jl} u_l = \sum_{j=1}^{n} \sum_{l=1}^{m} b_{ij} c_{jl} u_l,$$
$$v_k = \sum_{l=1}^{m} c_{kl} u_l = \sum_{l=1}^{m} c_{kl} \sum_{j=1}^{n} b_{lj} v_j = \sum_{l=1}^{m} \sum_{j=1}^{n} c_{kl} b_{lj} v_j.$$

Agora, se $B = (b_{ij})_{m\times n}$ e $C = (c_{ji})_{n\times m}$, então $BC = I_m$ e $CB = I_n$. Como A é um anel comutativo, segue que $m = n$. Portanto, as bases tem o mesmo posto. □

Teorema 2.1.3. *Sejam A um domínio principal e M um A-módulo livre de posto n. Se M' é um A-submódulo de M, então:*

1. *M' é livre de posto r, para $0 \leq r \leq n$.*
2. *Se $M' \neq \{0\}$, então existe uma base $\{v_1, \cdots, v_n\}$ de M e elementos não nulos $a_1, \cdots, a_r \in A$ tal que $\{a_1 v_1, \cdots, a_r v_r\}$ é uma base de M' e que a_i divide a_{i+1}, para $1 \leq i \leq r-1$.*

Demonstração. Para $M' = \langle 0 \rangle = \{0\}$ (ideal nulo) satisfaz o item 1, pois é de posto 0, e também, satisfaz o item 2, pois não contradiz a mesma. Suponhamos, assim, que $M' \neq \{0\}$. Vamos dividir a demonstração em cinco passos.

1. Seja $L(M, A)$ o conjunto das formas lineares sobre M. Se $e \in L(M, A)$, então $e(M')$ é um ideal de A, uma vez que $e(M') \subseteq A$ e

(a) se $x, y \in e(M')$, então existem $x_0, y_0 \in M'$ tal que $e(x_0) = x$ e $e(y_0) = y$. Assim, $x_0 - y_0 \in M'$, e deste modo, $e(x_0 - y_0) = e(x_0) - e(y_0) = x - y$. Portanto, $x - y \in e(M')$.

(b) se $x \in e(M')$ e $r \in A$, então existe $x_0 \in M'$ tal que $e(x_0) = x$. Assim, $x_0 r \in M'$, e deste modo, $e(x_0 r) = re(x_0) = rx$. Portanto, $rx \in e(M')$.

Pelo fato de A ser um domínio principal, segue que os ideais de A são gerados por um elemento, e assim, $e(M') = Aa_e = \langle a_e \rangle$, com $a_e \in A$. Como A é principal, segue que o conjunto $e(M')$ tem um elemento maximal, $Aa_u = \langle a_u \rangle$, para algum $u \in L(M, A)$. Seja $\{x_1, \cdots, x_n\}$ uma base que identifica M com A^n e consideramos a seguinte aplicação

$$\begin{array}{rccc} p_i: & M & \to & A \\ & a_1x_1 + \cdots a_nx_n & \mapsto & a_i. \end{array}$$

Neste caso, $p_i(x_j) = \delta_{ij}$. Como $M' \neq \{0\}$, segue que $p_i(M') \neq \{0\}$, para algum i, onde $i \leq n$. Assim, $u(M') \supset p_i(M') \neq \{0\}$, e deste modo, $u(M') = \langle a_u \rangle \neq \{0\}$ e $a_u \neq \{0\}$. Por construção, segue que existe $v' \in M'$ tal que $u(v') = a_u \ \ (*)$.

2. Agora, vamos mostrar que para todo $e \in L(M, A)$, segue que $a_u | e(v')$. Para isso, suponhamos que $mdc(a_u, e(v')) = d$. Logo, $d = ba_u + ce(v')$, onde $b, c \in A$. Assim,

$$d = ba_u + ce(v') \overset{(*)}{=} bu(v') + ce(v') = (bu + ce)(v').$$

Como $(bu + ce)$ é uma forma linear de $L(M, A)$, segue que $Aa_u \subset A_d$, pois $d | a_u$ e $Aa_u \subset \langle a_{bu+ce} \rangle$, pois $d = (bu + ce)(v')$. Assim, $Aa_u \subset A_d \subset Aa_u \subset \langle a_{bu+ce} \rangle \subset Aa_u$, onde Aa_u é maximal. Logo, $Aa_u = A_d \Rightarrow a_u | d$. Portanto, $a_u | e(v')$.

3. Em particular, $a_u | p_i(v')$, para todo i, ou seja, $p_i(v') = a_u b_i$, com $b_i \in A$. Agora, sejam

$$v = \sum_{i=1}^{n} b_i x_i \text{ e } a_u v = \sum_{i=1}^{n} (b_i a_u) x_i \Rightarrow a_u = \sum_{i=1}^{n} p_i(v) x_i = v'.$$

Dessa forma, $v' = a_u v$, e aplicando u, segue que

$$u(v') = u(a_u v) \overset{(*)}{\Rightarrow} a_u = a_u u(v) \Rightarrow u(v) = 1, \ \ a_u \neq 0.$$

4. Agora, vamos mostrar os seguintes resultados.

(a) $M = Ker(u) \oplus Av$. Se $x \in M$, então $x = (x - u(x)v') + u(x)v$. Mas, $u(x)v \in A_v$, pois $u \in L(M, A)$. Agora, vamos provar que $u(x - u(x)v) = 0$, ou seja,

$$u(x - u(x)v) = u(x) - u(u(x)v) \overset{u(x) \ const.}{=} u(x) - u(x)u(v) = u(x) - u(x) = 0.$$

Assim, $x - u(x)v \in Ker(u)$, e portanto, $M \subset Ker(u) + Av$. Mas, também $Ker(u) \subset M$ e $Av \subset M$. Portanto, $Ker(u) + Av \subset M$, e assim, $M = Ker(u) + Av$. Agora, falta apenas verificarmos que a soma é direta. Para isso, se $t \in Ker(u) \cap Av$, então $u(t) = 0$, e também, $t = rv, \ \ r \in A$. Com isso, $u(t) = u(rv) = ru(v) = r$. Por outro lado, $u(t) = r = 0$, ou seja, $Ker(u) \cap Av = \{0\}$. Portanto, $M = Ker(u) \oplus Av$.

(b) $M' = (M' \cap Ker(u)) + Av'$, onde $v' = a_u v$. Para isso, se $y \in M'$, então $u(y) = ba_u$, com $b \in A$. Logo, $y \in M' \Rightarrow (y - u(y)v) + u(y)v = (y - u(y)v) + ba_u v = (u - u(y)v) + bv'$, com $bv' \in Av'$. Agora, $y - u(y)v \in Ker(u)$, uma vez que aplicando u, segue que

$$u(y - u(y)v) = u(y) - u(u(y)v) = u(y) - u(y)u(v) = u(y) - u(y) = 0,$$

e assim, $y - u(y)v \in Ker(u)$. Logo, $M' \subset (M' \cap Ker(u)) + Av'$. Como $M' \cap Ker(u) \subset M'$ e $Av' \subset M'$, segue que $M' = (M' \cap Ker(u)) + Av'$. Agora, vamos mostrar que a soma é direta. Para isso, seja $t \in (M' \cap Ker(u)) + Av'$. Como $t \in M'$, $t \in Ker(u) \Rightarrow u(t) = 0$ e $t \in Av' \Rightarrow t = rv'$, com $r \in A$, segue que $u(t) = u(rv') = 0 = ru(v') = ra_u$, onde $a_u \neq 0$. Com isso, $r = 0$, e assim, $t = 0$. Logo, $(M' \cap Ker(u)) + Av' = \{0\}$, e portanto, $M' = (M' \cap Ker(u)) + Rv'$.

5. Agora, vamos provar os itens 1 e 2 por indução.

   (a) Para o item 1, provaremos por indução sobre o posto r de M'. Se $r = 0$, então $M' = \{0\}$ e o resultado é verdadeiro. Agora, seja $r > 0$. Suponhamos que é verdadeira para $r = k - 1$ e vamos provar que vale para $r = k$, onde M' tem posto k. Como M' tem posto k, por 2) do passo anterior, segue que Av' tem posto 1 (uma vez a soma é direta). Logo, $M' \cap Ker(u)$ tem posto $k - 1$, $M' \cap Ker(u)$ é livre pela hipótese de indução e Av' é livre por ser gerado por um elemento. Como a soma é direta, segue que podemos escrever M' de forma única, e assim, M' é livre.

   (b) Para o item 2, provaremos por indução sobre o posto n de M. Para $n = 0$, o resultado é verdadeiro. Agora, suponhamos que seja verdadeiro para $n = k - 1$. Agora, $Ker(u)$ é livre de posto $k - 1$, uma vez que do passo 1) a soma é direta. Aplicando a hipótese de indução n módulo livre $Ker(u)$ e no seu submódulo $M' \cap Ker(u)$, segue que se $M' \cap Ker(u) \neq \{0\}$, então existe uma base $v_2, \cdots, v_n$ de $Ker(u)$, com $r \leq n$, e elementos não nulos $a_2, \cdots a_n$ de A, tal que $a_2 v, \cdots, a_n v$ é uma base de $M' \cap Ker(u)$ e $a_i | a_{i+1}$, para $2 \leq i \leq r - 1$. Agora, sejam $a_1 = a_u$ e $v_i = v$. Logo, pela primeira afirmação, segue que $v_2, \cdots, v_n$ é uma base para M. Pela segunda afirmação e do fato de $v' = a_u v \Rightarrow v' = a_1 v_1$, segue que $\{a_1 v_1, \cdots, a_r v_r\}$ para M'. Falta provarmos que $a_1 | a_2$. Seja $s \in L(M, A)$ definida por $s(a_1 v_1 + \cdots + a_r v_r) = a_1 + a_2$. Assim, $a_u = a_1 = s(a_1 v_1) = s(a_u v) = s(v') \in s(M')$. Logo, $Aa_u \subseteq s(M')$. Como Aa_u é maximal, segue que $s(M') = Aa_1$. Assim, $a_2 = s(a_2 v_2) \in e(M') \Rightarrow a_2 \in Aa_1$, isto é, $a_1 | a_2$.

Portanto, o teorema está provado. □

2.2 Anel de inteiros

Nesta seção, apresentamos os conceitos de elementos inteiros, anel dos inteiros e suas principais propriedades. As referências são [13] e [14].

Definição 2.2.1. *Sejam $A \subseteq B$ anéis e $\alpha \in B$.*

1. *O elemento α é chamado um **elemento inteiro** sobre A se α for raiz de um polinômio mônico não nulo $p(x)$ com coeficientes em A.*

2. *A relação $p(\alpha) = 0$ é chamada de* ***equação de dependência inteira*** *de α sobre A.*

Observação 2.2.1. *Quando $B \subseteq \mathbb{C}$ e $A = \mathbb{Z}$, o elemento α é chamado um* ***inteiro algébrico*** *(esta definição se encontra na Seção 2.2, p.39).*

Exemplo 2.2.1. *São exemplos de elementos inteiros (algébricos).*

1. *Se $\sqrt{2} \in \mathbb{R}$, então $\sqrt{2}$ é raiz do polinômio mônico $p(x) = x^2 - 2$ com coeficientes em $\mathbb{Z}$. Logo, $\sqrt{2}$ é um elemento inteiro de $\mathbb{R}$ sobre $\mathbb{Z}$ e sua equação de dependência inteira é $\alpha^2 - 2 = 0$.*

2. *Se $i \in \mathbb{C}$, então i é raiz do polinômio mônico $p(x) = x^2 + 1$ com coeficientes em $\mathbb{Z}$. Logo, i é um elemento inteiro de $\mathbb{C}$ sobre $\mathbb{Z}$ e sua equação de dependência inteira é $\alpha^2 + 1 = 0$.*

Definição 2.2.2. *Sejam $A \subseteq B$ anéis. O conjunto*

$$\mathcal{O}_B = \{\alpha \in B \ \mid \ \alpha \text{ é inteiro sobre } A\},$$

é chamado de ***anel dos inteiros*** *de B sobre A.*

Observação 2.2.2. *Podemos usar a notação $\mathcal{O}_B(A)$ para referenciar o anel dos inteiros de B sobre A e se não houver possibilidade de confusão usaremos simplesmente a notação $\mathcal{O}_B$.*

Sejam $A \subseteq B$ anéis e $\alpha \in B$. O conjunto $A[\alpha] = \{f(\alpha) : f(x) \in A[x]\}$ é definido como o menor anel que contém A e α contido em B.

Teorema 2.2.1. *Sejam $A \subseteq B$ anéis e $\alpha \in B$. As seguintes afirmações são equivalentes:*

1. *O elemento α é inteiro sobre A.*

2. *O anel $A[\alpha]$ é um A-módulo finitamente gerado.*

3. *Existe um subanel R de B que é finitamente gerado contendo α e A.*

Demonstração. Para mostrar as equivalências provaremos as relações (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3) e (3) $\Rightarrow$ (1). Para (1) implica (2), por hipótese α é inteiro sobre A, e assim, existe um polinômio mônico com coeficientes $a_0, a_1, a_2, \ldots, a_n$ em A cujo α é raiz, ou seja,

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Se $M = [1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$, então M é um A-módulo finitamente gerado. Vamos mostrar que $A[\alpha] = M$. Por definição, segue que $M \subseteq A[\alpha]$. Para a outra inclusão, como

$$\alpha^n = -(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}),$$

segue que $\alpha^n \in M$, pois é uma combinação linear do conjunto gerador de M. Portanto, $1, \alpha, \alpha^2, \ldots, \alpha^n \in M$, e por indução sobre n, mostraremos que $\alpha^k \in M$, com $k > n$. Para $k \leq n$, segue que o resultado é verdadeiro. Agora, suponhamos por hipótese de indução que $\alpha^k \in M$, para $k > n$. Assim, existem $b_0, b_1, b_2, \ldots, b_{n-1} \in A$ tal que

$$\alpha^k = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1},$$

e assim,

$$\alpha^{k+1} = b_0\alpha + b_1\alpha^2 + b_2\alpha^3 + \cdots + b_{n-1}\alpha^n$$

Substituindo o valor de α^n, segue que

$$\begin{aligned}\alpha^{k+1} &= b_0\alpha + b_1\alpha^2 + b_2\alpha^3 + \cdots + b_{n-1}[-(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1})] = \\ &= -a_0b_{n-1} + (b_0 - a_1b_{n-1})\alpha + \cdots + (b_{n-2} - a_{n-1}b_{n-1})\alpha^{n-1}\end{aligned}$$

Logo, α^{k+1} é escrito como combinação linear do conjunto gerador de M, e assim, $\alpha^{k+1} \in M$. Logo, $A[\alpha] \subseteq M$. Portanto, $A[\alpha] = M$ e é um A-módulo finitamente gerado. Para (2) implica (3), por hipótese $A[\alpha]$ é um A-módulo finitamente gerado. Como $\alpha \in A[\alpha]$ e $A \subseteq A[\alpha]$, segue que é suficiente tomar $R = A[\alpha]$. Para (3) implica (1), consideramos $R = [\beta_1, \beta_2, \ldots, \beta_n]$, e assim, podemos escrever $R = A\beta_1 + A\beta_2 + \cdots + A\beta_n$, pois $A \subseteq R$. Como $\alpha \in R$, segue que $\alpha\beta_i \in R$, para $i = 1, \ldots, n$, e assim,

$$\alpha\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j,$$

com $a_{ij} \in A$, para $i \leq j$ e $j \leq n$. Com isso,

$$\alpha\beta_i - \sum_{j=1}^{n} a_{ij}\beta_j = 0 \Leftrightarrow \sum_{j=1}^{n} \left(\alpha\frac{\beta_i}{\beta_j} - a_{ij}\right)\beta_j = 0.$$

Agora, se $\dfrac{\beta_i}{\beta_j} = \delta_{ij}$, então

$$\sum_{j=1}^{n} (\alpha\delta_{ij} - a_{ij})\,\beta_j = 0,$$

e assim, obtemos um sistema linear homogêneo com n equações dado por

$$\begin{cases} \sum\limits_{j=1}^{n} (\alpha\delta_{1j} - a_{1j})\,\beta_j = 0 \\ \sum\limits_{j=1}^{n} (\alpha\delta_{2j} - a_{2j})\,\beta_j = 0 \\ \vdots \\ \sum\limits_{j=1}^{n} (\alpha\delta_{nj} - a_{nj})\,\beta_j = 0. \end{cases}$$

Esse sistema pode ser escrito na forma matricial $MN = P$, da seguinte maneira

$$\begin{bmatrix} \alpha\delta_{11} - a_{11} & \alpha\delta_{12} - a_{12} & \cdots & \alpha\delta_{1n} - a_{1n} \\ \alpha\delta_{21} - a_{21} & \alpha\delta_{22} - a_{22} & \cdots & \alpha\delta_{2n} - a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha\delta_{n1} - a_{n1} & \alpha\delta_{n2} - a_{n2} & \cdots & \alpha\delta_{nn} - a_{nn} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Pela regra de Crammer, segue que

$$\beta_i det(M) = det(H),$$

onde $det(H)$ é o determinante da matriz M com a coluna i igual a coluna da matriz P. Logo, $det(H) = 0$, e assim, $\beta_i det(M) = 0$, para $i = 1, \ldots, n$. Portanto, $\beta \det(M) = 0$, para todo $\beta \in B$, e deste modo,

$$det(M) = 0.$$

Com isso, $det(M)$ é um polinômio mônico, onde α é uma raiz. O fato de ser mônico pode ser observado na expansão desse produto $\prod_{i=1}^{n}(\alpha - a_{ii})$ (diagonal principal da matriz M), e portanto, α é um elemento inteiro sobre A.

□

Lema 2.2.1. *Sejam $A \subseteq B$ anéis. Se $\alpha_1, \alpha_2 \in B$ são inteiros sobre A, então*

$$A[\alpha_1, \alpha_2] = A[\alpha_1][\alpha_2].$$

Demonstração. Consideramos os seguintes conjuntos

$$A[\alpha_1, \alpha_2] = \left\{ \sum_{i=1}^{n} a_i \alpha_1^i \alpha_2^i : a_i \in A \right\} \text{ e}$$

$$A[\alpha_1][\alpha_2] = \left\{ \sum_{j=1}^{m} b_i \alpha_2^j : b_i \in A[\alpha_1] \right\}.$$

Se $x \in A[\alpha_1, \alpha_2]$, então $x = \sum_{i=1}^{n} a_i \alpha_1^i \alpha_2^i$, com $a_i \in A$, para $i = 1, 2, \ldots, n$. Assim, $a_i, \alpha_1^i \in A[\alpha_1]$, para todo i, e desta forma, $b_i = a_i \alpha_1^i \in A[\alpha_1]$. Assim, $x = \sum_{i=1}^{n} b^i \alpha_2^i$, com coeficientes em $A[\alpha_1]$, e portanto, $x \in A[\alpha_1][\alpha_2]$. Logo, $A[\alpha_1, \alpha_2] \subseteq A[\alpha_1][\alpha_2]$. Agora, se $x \in A[\alpha_1][\alpha_2]$, então $x = \sum_{j=1}^{m} b_j \alpha_2^j$, com $b_j \in A[\alpha_1]$, para $j = 1, 2, \ldots, m$. Com isso podemos escrever os b_j's, como $b_j = \sum_{i=1}^{n} a_i \alpha_1^i$, com $a_i \in A$, para todo i. Assim, $x = \sum_{j=1}^{m} \sum_{i=1}^{n} a_i \alpha_1^i \alpha_2^j$, ou seja, escrevemos x como uma combinação finita de α_1 e α_2, com coeficientes em A. Logo, $x \in A[\alpha_1, \alpha_2]$, e assim, $A[\alpha_1][\alpha_2] \subseteq A[\alpha_1, \alpha_2]$. Portanto, $A[\alpha_1, \alpha_2] = A[\alpha_1][\alpha_2]$. □

Com base no Lema 2.2.1, obtemos o seguinte lema, que por sua vez é uma generalização do mesmo.

Lema 2.2.2. *Sejam $A \subseteq B$ anéis. Se $\alpha_1, \alpha_2, \ldots, \alpha_n \in B$ com α_i inteiro sobre A, para $i = 1, 2, \ldots, n$, então*

$$A[\alpha_1, \alpha_2, \ldots, \alpha_n] = A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n].$$

Demonstração. Se $x \in A[\alpha_1, \alpha_2, \ldots, \alpha_n]$, então

$$x = \sum_{i=1}^{n} a_i (\alpha_1 \alpha_2 \ldots \alpha_{n-1} \alpha_n)^i,$$

com $a_i \in A$, para todo $i = 1, 2, \ldots, n$. Agora, como $b_i = a_1(\alpha_1 \alpha_2 \ldots \alpha_{n-1})^i$ é um elemento de $A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$, segue que $x = \sum_{i=1}^{n} b_i \alpha_n^i$, e assim, $x \in A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$. Portanto, $A[\alpha_1, \alpha_2, \ldots, \alpha_n] \subseteq A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$. Agora, se $x \in A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$, então

$$x = \sum_{j=1}^{m} b_j \alpha_n^j,$$

com $b_j \in A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$, para $j = 1, 2, \ldots, m$. Assim, b_j pode ser escrito como $b_j = \sum_{i=1}^{n} a_i (\alpha_1 \alpha_2 \ldots \alpha_{n-1})^i$, com $a_i \in A$, para $i = 1, 2, \ldots, n-1$. Assim, $x = \sum_{j=1}^{m} \sum_{i=1}^{n} a_i \alpha_1^i \ldots \alpha_{n-1}^i \alpha_n^j$, ou seja, escrevemos x como combinação de $\alpha_1, \ldots, \alpha_n$ e coeficientes de A, e deste modo, $x \in A[\alpha_1, \alpha_2, \ldots, \alpha_n]$. Logo, $A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n] \subseteq A[\alpha_1, \alpha_2, \ldots, \alpha_n]$, e consequentemente, $A[\alpha_1, \alpha_2, \ldots, \alpha_n] = A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$. □

Proposição 2.2.1. *Sejam $A \subseteq B$ anéis e $\alpha_1, \alpha_2, \ldots, \alpha_n \in B$. Se α_i é inteiro sobre A e α_i é inteiro sobre $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$, para $i = 1, 2, \ldots, n$, então $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ é um A-módulo do tipo finito.*

Demonstração. Faremos essa demonstração usando indução sobre n. Para $n = 1$, o resultado segue diretamente do Teorema 2.2.1. Por hipótese de indução (H.I.), supomos que a tese seja verdadeira para $n = k-1$, ou seja, para $\alpha_1 \ldots, \alpha_{k-1} \in B$, onde α_i é inteiro sobre A, com $i = 1, \ldots, k-1$, também é inteiro sobre $A[\alpha_1, \ldots, \alpha_{k-1}]$ e $A[\alpha_1, \ldots, \alpha_{k-1}]$ é um A-módulo finitamente gerado, ou seja, existe um conjunto $\{\beta_1, \ldots, \beta_p\}$ tal que $[\beta_1, \ldots, \beta_p] = A[\alpha_1, \ldots, \alpha_{k-1}]$. Provaremos agora para $n = k$. Por definição, segue que

$$A[\alpha_1, \ldots, \alpha_{k-1}] = \left\{ \sum_{i=1}^{p} a_i \beta_i : a_i \in A \right\} = \sum_{i=1}^{p} A\beta_i = C.$$

Como α_k é inteiro sobre A, segue que α_k é inteiro sobre C, pois $A \subseteq C \subseteq C[\alpha_k] \subseteq B$. Pelo Teorema 2.2.1, segue que $C[\alpha_k]$ é um A-módulo finitamente gerado, ou seja, existe um conjunto $\{\gamma_1, \ldots, \gamma_q\}$ tal que $[\gamma_1, \ldots, \gamma_q] = C[\alpha_k]$. Por definição, segue que

$$C[\alpha_k] = \left\{ \sum_{j=1}^{q} b_j \gamma_j : b_j \in C \right\} = \sum_{j=1}^{q} C\gamma_j.$$

Agora, usando o Lema 2.2.2, segue que

$$\begin{aligned} A[\alpha_1, \ldots, \alpha_k] &= A[\alpha_1, \ldots, \alpha_{k-1}][\alpha_k] = C[\alpha_k] = \sum_{j=1}^{q} C\gamma_j \\ &\overset{H.I.}{=} \sum_{j=1}^{q} \left(\sum_{i=1}^{p} A\beta_i \right) \gamma_j = \sum_{j=1}^{q} \sum_{i=1}^{p} A(\beta_i \gamma_j), \end{aligned}$$

ou seja, o conjunto $\{\beta_1\gamma_1, \ldots, \beta_1\gamma_q, \beta_2\gamma_1, \ldots, \beta_2\gamma_q, \ldots, \beta_p\gamma_1, \ldots, \beta_p\gamma_q\}$ gera $A[\alpha_1, \ldots, \alpha_k]$. Portanto, o conjunto $A[\alpha_1, \ldots, \alpha_k]$ é um A-módulo finitamente gerado. □

Corolário 2.2.1. *Sejam $A \subseteq B$ anéis. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha + \beta$, $\alpha - \beta$ e $\alpha\beta$ são inteiros sobre A.*

Demonstração. Por hipótese, $\alpha+\beta, \alpha-\beta, \alpha\beta \in A[\alpha, \beta]$. Pela Proposição 2.2.1, segue que $A[\alpha, \beta]$ é um A-módulo finitamente gerado e pelo Teorema 2.2.1, segue que $\alpha + \beta$, $\alpha - \beta$ e $\alpha\beta$ são inteiros sobre A. □

Corolário 2.2.2. *Sejam $A \subseteq B$ anéis. O conjunto $\mathcal{O}_B(A)$ é um subanel dos B que contém A. Consequentemente, $\mathcal{O}_B(A)$ é um anel.*

Demonstração. Pelo Corolário 2.2.1, se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha + \beta$, $\alpha - \beta$ e $\alpha\beta$ também são inteiros sobre A. Dessa forma, segue que $\mathcal{O}_B(A)$ é um subanel dos B, ou seja, $\mathcal{O}_B(A)$ é um anel. Para mostrar a inclusão $A \subseteq \mathcal{O}_B$, consideramos $a \in A$. Assim, a é raiz do polinômio mônico $p(x) = x - a$, onde $p(x) \in A[x]$, e consequentemente, $a \in \mathcal{O}_B(A)$. Portanto, $A \subseteq \mathcal{O}_B(A)$. □

Pelo Corolário 2.2.2, segue que o conjunto $\mathcal{O}_B(A)$ é um anel, o qual chamamos de anel dos inteiros.

Definição 2.2.3. *Sejam $A \subseteq \mathcal{O}_B \subseteq B$ anéis.*

1. *O anel $\mathcal{O}_B$ é chamado de fecho inteiro de A em B.*

2. *Se $\mathcal{O}_B = B$, o anel B é chamado inteiro sobre A.*

Proposição 2.2.2. *Sejam C um anel, B um subanel dos C e A um subanel dos B, em outras palavas, sejam $A \subseteq B \subseteq C$ anéis. Assim, C é inteiro sobre A se, e somente se, C é inteiro sobre B e B é inteiro sobre A.*

Demonstração. Se C é inteiro sobre A, então $\mathcal{O}_C(A) = C$. Além disso, $\mathcal{O}_B(A) \subseteq B$ e $\mathcal{O}_C(B) \subseteq C$. Falta mostrar que $B \subseteq \mathcal{O}_B(A)$ e $C \subseteq \mathcal{O}_C(B)$.

1. Vamos mostrar que $B \subseteq \mathcal{O}_B(A)$. Seja $b \in B$. Como $B \subseteq C$, segue que $b \in C$. Como $b \in \mathcal{O}_C(A)$, segue que b é inteiro sobre A, ou seja, $b \in \mathcal{O}_B(A)$. Portanto, $B = \mathcal{O}_B(A)$, ou seja, B é inteiro sobre A.

2. Vamos mostrar que $C \subseteq \mathcal{O}_C(B)$. Seja $c \in C$. Por hipótese, C é inteiro sobre A, e assim, $a_0 + a_1c + \cdots + a_{n-1}c^{n-1} + c^n = 0$, com $a_i \in A$ e $i = 0, 1, \ldots, n-1$. Como $A \subseteq B$, segue que $a_i \in B$. Portanto, c satisfaz uma equação de dependência de inteiros com coeficientes em B, e assim, C é inteiro sobre B. Logo, $C \subseteq \mathcal{O}_C(B)$. Portanto, $C = \mathcal{O}_C(B)$, ou seja, C é inteiro sobre B.

Reciprocamente, suponhamos que B é inteiro sobre A e C é inteiro sobre B. Assim, $\mathcal{O}_B(A) = B$ e $\mathcal{O}_C(B) = C$. Queremos mostrar que $\mathcal{O}_C(A) = C$. Por definição, segue que $\mathcal{O}_C(A) \subseteq C$. Agora, falta mostrar que $C \subseteq \mathcal{O}_C(A)$. Para isso, seja $\alpha \in C$. Por hipótese, α é inteiro sobre B, e assim, existe uma equação de dependência de inteira $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n = 0$, com $b_i \in B$ e $i = 0, 1, \ldots, n-1$. Seja $B_0 = A[b_0, b_1, \ldots, b_{n-1}]$. Assim, α é inteiro sobre B, e também, b_i são inteiros sobre A. Pela Proposição 2.2.1, segue que

$$B_0 = A[b_0, b_1, \ldots, b_{n-1}][\alpha] = A[b_0, b_1, \ldots, b_{n-1}, \alpha]$$

é um A-módulo finitamente gerado. Pelo Teorema 2.2.1, como existe $R = B_0[\alpha]$ que contém A e α e é um A-módulo finitamente gerado, segue que $\alpha \in \mathcal{O}_C(A)$. Portanto, $\mathcal{O}_C(A) = C$, ou seja, C é inteiro sobre A. □

Apresentamos na próxima proposição uma relação entre o conceito de corpo e o anel dos inteiros.

Proposição 2.2.3. *Sejam $A \subseteq B$ anéis, com B um domínio tal que B é inteiro sobre A. Assim, A é um corpo se, e somente se, B é um corpo.*

Demonstração. Suponhamos que A é um corpo e consideramos $\alpha \in B$, com $\alpha \neq 0$. Como B é inteiro sobre A, segue que α é inteiro sobre A. Pelo Teorema 2.2.1, segue que $A[\alpha]$ é um A-módulo finitamente gerado. Como A é um corpo, segue que $A[\alpha]$ é um espaço vetorial. Logo, podemos considerar a seguinte transformação linear

$$\begin{aligned} \varphi : A[\alpha] &\to A[\alpha] \\ a &\mapsto \alpha a \end{aligned}$$

Assim,

1. A função φ está bem definida. De fato, se $a, b \in A[\alpha]$, com $a = b$, então $\alpha a = \alpha b$ o que implica em $\varphi(a) = \varphi(b)$.

2. A função φ é uma transformação linear. De fato,

   (a) $\varphi(a+b) = \alpha(a+b) = \alpha a + \alpha b = \varphi(a) + \varphi(b)$, para todo $a, b \in A[\alpha]$.

   (b) $\varphi(\beta a) = \alpha(\beta a) = \beta(\alpha a) = \beta\varphi(a)$, com $a, \alpha \in A[\alpha]$.

3. A função φ é injetora. De fato, $y \in Ker(\varphi) \Leftrightarrow \alpha y = 0 \Leftrightarrow y = 0$, uma vez que $\alpha \neq 0$. Portanto, $Ker(\varphi) = \{0\}$, e assim, φ é injetora.

4. A função φ é sobrejetora. De fato, se $\alpha a \in A[\alpha]$, então existe $a \in A[\alpha]$ tal que $\varphi(a) = \alpha a$.

Portanto, dos itens 3) e 4) concluímos que φ é bijetora. Agora, como $1 \in A[\alpha]$, segue que existe $a \in A[\alpha]$ tal que $\varphi(a) = \alpha a = 1$. Dessa forma, α é inversível sobre B, e portanto, B é um corpo. Reciprocamente, suponhamos que B é um corpo. Consideramos $\alpha \in A$, com $\alpha \neq 0$. Como $A \subseteq B$, segue que $\alpha \in B$. Logo, existe $\alpha^{-1} \in B$ tal que $\alpha\alpha^{-1} = 1$. Como B é inteiro sobre A, seque que α^{-1} é inteiro sobre A. Assim, existe uma equação de dependência de inteiros de α^{-1}, com $a_i \in A$ e $i = 0, 1, \ldots, n-1$, ou seja,

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

Multiplicando essa equação por α^{n-1}, segue que

$$a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1} + \alpha^{-1} = 0.$$

Agora, isolando α^{-1}, segue que

$$\alpha^{-1} = -(a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1}).$$

Logo, $\alpha^{-1} \in A$, e portanto, A é um corpo. □

Apresentamos, a seguir, mais um nome especial relacionando ao anel dos inteiros em determinada situação e vamos demonstrar alguns resultados sobre esta particularidade.

Definição 2.2.4. *Sejam $A \subseteq \mathcal{O}_{\mathbb{K}} \subseteq \mathbb{K}$, com A um domínio e $\mathbb{K}$ o seu corpo de frações. O anel A é chamado **integralmente fechado** se $A = \mathcal{O}_{\mathbb{K}}$.*

Proposição 2.2.4. *Se A é um domínio e $\mathbb{K}$ o seu corpo de frações, então o fecho inteiro $\mathcal{O}_{\mathbb{K}}$ de A (isto é, o fecho inteiro de A) é integralmente fechado.*

Demonstração. Consideramos $A \subseteq \mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}'_{\mathbb{K}} \subseteq \mathbb{K}$, onde

$$\mathcal{O}'_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha \ \textit{é inteiro sobre} \ \mathcal{O}_{\mathbb{K}}\} \text{ e}$$

$$\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha \ \textit{é inteiro sobre} \ A\}.$$

Por definição, segue que $\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}'_{\mathbb{K}}$. Assim, se $\alpha \in \mathbb{K}$, com α inteiro sobre $\mathcal{O}_{\mathbb{K}}$, então $\alpha \in \mathcal{O}'_{\mathbb{K}}$. Como $A \subseteq \mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}'_{\mathbb{K}}$, pela Proposição 2.2.2, segue que α é inteiro sobre A, e assim, $\alpha \in \mathcal{O}_{\mathbb{K}}$. Logo, $\mathcal{O}'_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado. □

Proposição 2.2.5. *Se A é um domínio principal, então A é integralmente fechado.*

Demonstração. Seja $\mathbb{K}$ o corpo de frações de A. Se $\alpha \in \mathbb{K}$ é inteiro sobre A, então $\alpha = \frac{a}{b}$, com $b \neq 0$, $a, b \in A$ e $mdc(a, b) = 1$. Além disso, existe uma equação de dependência de α, com $a_i \in A$, para todo i, ou seja,

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

Substituiremos α por $\frac{a}{b}$ nesta equação, segue que

$$a_0 + a_1\left(\frac{a}{b}\right) + \cdots + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \left(\frac{a}{b}\right)^n = 0.$$

Agora, multiplicando esta equação por b^n, segue que

$$a_0b^n + a_1ab^{n-1} + \cdots + a_{n-1}b + a^n = 0.$$

Isolando a^n, segue que

$$a^n = b(-a_0b^{n-1} - a_1ab^{n-2} - \cdots - a_{n-1}a^{n-1}),$$

e assim, $b|a^n$. Como $mdc(a, b) = 1$, segue que $b|a$, ou seja, existe $u \in A$ tal que $a = ub \Rightarrow \alpha = \frac{a}{b} = u \in A$. Assim, $\mathcal{O}_\mathbb{K} \subseteq A$, e como $A \subseteq \mathcal{O}_\mathbb{K}$, segue que $\mathcal{O}_\mathbb{K} = A$. Portanto, A é integralmente fechado. □

Exemplo 2.2.2. *O anel $\mathbb{Z}$ é integralmente fechado.*

Definição 2.2.5. *Seja $\mathbb{K} \subseteq \mathbb{C}$ um corpo.*

1. *Se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, então $\mathbb{K}$ é chamado de **corpo de números algébricos**, ou simplesmente, **corpo de números**.*

2. *Se $\mathbb{K}$ é um corpo de números, os elementos de $\mathbb{K}$ que são inteiros sobre $\mathbb{Z}$ são chamados de **inteiros algébricos** de $\mathbb{K}$.*

3. *Se $\mathbb{K}$ é um corpo de números, o conjunto dos elementos $\mathbb{K}$ que são inteiros inteiros algébricos é chamado de **anel dos inteiros algébricos** de $\mathbb{K}$, ou simplesmente, de **anel dos inteiros** de $\mathbb{K}$, o qual denotamos por $\mathcal{O}_\mathbb{K}$.*

2.3 Norma e traço

Norma e traço são funções tidas a partir dos monomorfismos, mas para isso faremos toda a construção usando os endomorfismos. Essas funções nos auxiliarão para determinar o anel dos inteiros algébricos nos próximos capítulos. As referências são [5] e [14].

Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto finito n. Consideramos φ um endomorfismo de B e $\{e_1, e_2, \ldots, e_n\}$ uma base de B sobre A. Assim, definimos a aplicação $\varphi : B \to B$ como

$$\begin{cases} \varphi(e_1) = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n \\ \varphi(e_2) = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n \\ \vdots \\ \varphi(e_n) = a_{n1}e_1 + a_{n2}e_2 + \cdots + a_{nn}e_n, \end{cases}$$

com $a_{ij} \in A$, para todo $i, j = 1, 2, \ldots, n$. Na forma matricial, é dada por

$$\begin{bmatrix} \varphi(e_1) \\ \varphi(e_2) \\ \vdots \\ \varphi(e_n) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}$$

Definição 2.3.1. *Seja φ um endomorfismo de B.*

1. *O **traço de** φ é definido por $\mathcal{T}r_{B|A}(\varphi) = \sum_{i=1}^{n} a_{ii}$.*
2. *A **norma de** φ é definida por $\mathcal{N}_{B|A}(\varphi) = det(a_{ij})$.*
3. *O **polinômio característico de** φ é definido por $det(xI_n - \varphi) = det(x\delta_{ij} - a_{ij})$, com $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$.*

Observação 2.3.1. *Se φ e ρ são dois endomorfismos, então*

1. *$\mathcal{T}r_{B|A}(\varphi + \rho) = \mathcal{T}r_{B|A}(\varphi) + \mathcal{T}r_{B|A}(\rho)$;*
2. *$\mathcal{N}_{B|A}(\varphi\rho) = \mathcal{N}_{B|A}(\varphi)\mathcal{N}_{B|A}(\rho)$;*
3. *$det(xI_n - \varphi) = x^n - \mathcal{T}r_{B|A}(\varphi)x^{n-1} + \cdots + (-1)^n\mathcal{N}_{B|A}(\varphi)$.*

Definição 2.3.2. *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto n. Para $\alpha \in B$, consideramos o endomorfismo $\varphi_\alpha : B \to B$ dado por $\varphi_\alpha(x) = \alpha x$. Definimos as seguintes funções de $\alpha \in B$ relativas a A como:*

1. *O **traço** de α é o traço do endomorfismo φ_α, ou seja,*

$$\mathcal{T}r_{B|A}(\alpha) = \mathcal{T}r_{B|A}(\varphi_\alpha).$$

2. *A **norma** de α é a norma do endomorfismo φ_α, ou seja,*

$$\mathcal{N}_{B|A}(\alpha) = N_{B|A}(\varphi_\alpha).$$

3. *O **polinômio característico** de α é o polinômio característico do endomorfismo φ_α, ou seja, é definido e denotado por:*

$$f_\alpha(x) = det(xI_n - \varphi_\alpha) = x^n - \mathcal{T}r_{B|A}(\varphi_\alpha)x^{n-1} + \cdots + (-1)^n\mathcal{N}_{B|A}(\varphi_\alpha).$$

Observação 2.3.2. *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre do posto finito. Se $\alpha, \beta \in B$ e $a \in A$, então:*

1. *$\varphi_\alpha + \varphi_\beta = \varphi_{\alpha+\beta}$;*
2. *$\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$;*
3. *$\varphi_{a\alpha} = a\varphi_\alpha$.*

Além disso, a matriz de φ_a em relação a uma base B sobre A é uma matriz diagonal, onde a é a entrada de todas as diagonais.

Observação 2.3.3. *Quando estivermos trabalhando com $\mathbb{K}$ um corpo de números, podemos simplesmente denotar a norma e o traço de $\alpha \in \mathbb{K}$ como $\mathcal{T}r(\alpha)$ e $\mathcal{N}(\alpha)$, respectivamente.*

Proposição 2.3.1. *Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ corpos e $[\mathbb{M} : \mathbb{K}] = n$. Se $\alpha, \beta \in \mathbb{M}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades*

1. $\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\alpha + \beta) = \mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\alpha) + \mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\beta)$;
2. $\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(a\alpha) = a\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\alpha)$;
3. $\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(a) = na$;
4. $\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\alpha) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\mathcal{T}r_{\mathbb{M}|\mathbb{L}}(\alpha))$;
5. $\mathcal{N}_{\mathbb{M}|\mathbb{K}}(\alpha\beta) = \mathcal{N}_{\mathbb{M}|\mathbb{K}}(\alpha)\mathcal{N}_{\mathbb{M}|\mathbb{K}}(\beta)$;
6. $\mathcal{N}_{\mathbb{M}|\mathbb{K}}(a\alpha) = a^n\mathcal{N}_{\mathbb{M}|\mathbb{K}}(\alpha)$;
7. $\mathcal{N}_{\mathbb{M}|\mathbb{K}}(a) = a^n$;
8. $\mathcal{N}_{\mathbb{M}|\mathbb{K}}(\alpha) = \mathcal{N}_{\mathbb{L}|\mathbb{K}}(\mathcal{N}_{\mathbb{M}|\mathbb{L}}(\alpha))$.

Demonstração. A demonstração segue diretamente das definições de norma e traço. □

Observação 2.3.4. *Sob as condições da Proposição 2.3.1, destacamos algumas propriedades que nem sempre são válidas:*

1. $\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\alpha\beta) \neq \mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\alpha)\mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\beta)$ *e*
2. $\mathcal{N}_{\mathbb{M}|\mathbb{K}}(\alpha + \beta) \neq \mathcal{N}_{\mathbb{M}|\mathbb{K}}(\alpha) + \mathcal{N}_{\mathbb{M}|\mathbb{K}}(\beta)$.

Exemplo 2.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números de grau 2.*

a) Como $\mathcal{T}r(2) = 4$, $\mathcal{T}r(3) = 6$, $\mathcal{T}r(2 \times 3) = \mathcal{T}r(6) = 12$ e $\mathcal{T}r(2)\mathcal{T}r(3) = 4 \times 6 = 24$, segue que $\mathcal{T}r(2 \times 3) \neq \mathcal{T}r(2)\mathcal{T}r(3)$.

b) Como $\mathcal{N}(2) = 4$, $\mathcal{N}(3) = 9$, $\mathcal{N}(2 + 3) = \mathcal{N}(5) = 25$ e $\mathcal{N}(2) + \mathcal{N}(3) = 4 + 9 = 13$, segue que $\mathcal{N}(2 + 3) \neq \mathcal{N}(2) + \mathcal{N}(3)$.

Teorema 2.3.1. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão algébrica, com $\mathbb{K}$ um corpo finito ou de característica zero, $[\mathbb{L} : \mathbb{K}] = n$ e $\alpha \in \mathbb{L}$. Se $\alpha_1, \alpha_2, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}(\alpha)]$-vezes, então*

1. $\mathcal{T}r_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i$.
2. $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i$.
3. $m_\alpha(x) = \prod_{i=1}^{n} (x - \alpha_i)$.

Além disso, o polinômio característico de α é a $[\mathbb{L} : \mathbb{K}(\alpha)]$-ésima potência do polinômio minimal de α sobre $\mathbb{K}$.

Demonstração. Vamos dividir a demonstração em dois casos:

1. Primeiro, consideramos que $[\mathbb{L} : \mathbb{K}(\alpha)] = 1$, ou seja, α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ o polinômio minimal de α sobre $\mathbb{K}$, com $a_i \in \mathbb{K}$ para $i = 0, 1, \ldots, n$. Como $\mathbb{L}$ é $\mathbb{K}$-isomorfo a $\dfrac{\mathbb{K}[x]}{< m_\alpha(x) >}$ e $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que a matriz do endomorfismo $\varphi_\alpha : \mathbb{L} \to \mathbb{L}$ com respeito a esta base é dada por

$$\begin{cases} \varphi_\alpha(1) = \alpha \\ \varphi_\alpha(\alpha) = \alpha^2 \\ \varphi_\alpha(\alpha^2) = \alpha^3 \\ \vdots \\ \varphi_\alpha(\alpha^{n-2}) = \alpha^{n-1} \\ \varphi_\alpha(\alpha^{n-1}) = \alpha^n \end{cases} \Rightarrow M = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}.$$

Vale observar que $\varphi_\alpha(k) = k\alpha$, para todo $k \in \mathbb{L}$ e α é algébrico. Outro fato que obtemos é que $det(xI_n - \varphi_\alpha) = det(xI_n - M)$, onde a matriz em questão é dada por

$$xI_n - M = \begin{bmatrix} x & 0 & 0 & \ldots & 0 & a_0 \\ -1 & x & 0 & \ldots & 0 & a_1 \\ 0 & -1 & x & \ldots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & x & a_{n-2} \\ 0 & 0 & 0 & \ldots & -1 & x + a_{n-1} \end{bmatrix}.$$

Logo, pelo cálculo do determinante da matriz $xI_n - M$, segue que o polinômio característico $f_\alpha(x)$ de α é igual ao polinômio minimal $m_\alpha(x)$ de α. Pela definição do polinômio característico, segue

$$f_\alpha(x) = x^n - \mathcal{T}r_{B|A}(\varphi_\alpha)x^{n-1} + \cdots + (-1)^n \mathcal{N}_{B|A}(\varphi_\alpha).$$

Por outro lado, como α é primitivo, segue que o polinômio minimal é dado por

$$m_\alpha(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) = x^n - \left(\sum_{i=1}^{n} \alpha_i\right) x^{n-1} + \cdots + (-1)^n \left(\prod_{i=1}^{n} \alpha_i\right).$$

Pela igualdade dos polinômios $f_\alpha(x) = m_\alpha(x)$, comparando seus coeficientes, segue que

$$\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\varphi_\alpha) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i \quad \text{e} \quad \mathcal{N}_{\mathbb{L}|\mathbb{K}}(\varphi_\alpha) = \mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i.$$

Portanto,

$$\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i,$$

$$\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i \quad \text{e} \quad f_\alpha(x) = \prod_{i=1}^{n} (x - \alpha_i).$$

2. Finalmente, quando $[\mathbb{L} : \mathbb{K}(\alpha)] = r$ é suficiente mostrarmos que o polinômio característico $f_\alpha(x)$ de α, com relação a $\mathbb{L}$ sobre $\mathbb{K}$, é igual a $r-$ésima potência do polinômio minimal de α sobre $\mathbb{K}$. Seja $\{y_i\}$, com $i = 1, \ldots, q$, uma base de $\mathbb{K}(\alpha)$

sobre $\mathbb{K}$ e $\{z_j\}$, com $j = 1, \ldots, r$, uma base de $\mathbb{L}$ sobre $\mathbb{K}(\alpha)$. Assim, $\{y_i z_j\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ com $n = qr$. Se $M = (a_{ih})$ é a matriz do endomorfismo multiplicado por α em $\mathbb{K}[\alpha]$ com relação a base $\{y_i\}$, segue que $ay_i = \sum_h a_{ih} y_h$, e assim, $\alpha(y_i z_j) = \left(\sum_h a_{ij} y_h\right) z_j = \sum_h a_{ih}(y_h z_j)$. Logo,

$$\begin{cases} \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{12} y_2 z_1 + \cdots + a_{1q} y_q z_1 \\ \alpha y_2 z_1 = a_{21} y_1 z_1 + a_{22} y_2 z_1 + \cdots + a_{2q} y_q z_1 \\ \vdots \\ \alpha y_q z_1 = a_{q1} y_1 z_1 + a_{q2} y_2 z_1 + \cdots + a_{qq} y_q z_1 \end{cases}$$

A matriz do endomorfismo de α em $\mathbb{L}$ em relação a base $\{y_i z_j\}$ é dada por

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

isto é, M se repete $r-$vezes na diagonal principal como blocos diagonais na matriz M_1. Logo, a matriz $xI_n - M_1$, consiste de r blocos diagonal, cada um tem a forma $xI_q - M$, e assim,

$$xI_n - M_1 = \begin{bmatrix} xI_q - M & 0 & \ldots & 0 \\ 0 & xI_q - M & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & xI_q - M \end{bmatrix}.$$

Logo, $det(xI_n - M_1) = det(xI_q - M_1)^r$. Com isso, $f_\alpha(x) = det(xI_n - M_1)$ é o polinômio característico de α sobre $\mathbb{K}$ e $det(xI_q - M)$ é o polinômio minimal de α sobre $\mathbb{K}$, de acordo com a primeira parte da demostração.

Portanto, os dois itens concluem a demonstração. □

Proposição 2.3.2. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações, onde $\mathbb{K}$ tem característica zero. Se $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e $\alpha \in \mathbb{L}$ é um elemento inteiro sobre A, então os coeficientes do polinômio característico $f_\alpha(x)$ são inteiros sobre A. Em particular, $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$ são inteiros sobre A.*

Demonstração. Pelo Teorema 2.3.1, segue que o polinômio característico de α é dado por $f_\alpha(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$, onde α_i's são as raízes do polinômio minimal de α . Como os coeficientes de $f_\alpha(x)$ (a menos de sinal), são da relação de Girard somas e produtos de $\alpha_i's$, segue que somente precisamos mostrar que α_i é um inteiro sobre A, para todo $i = 1, 2, \ldots, n$, uma vez que pelo Corolário 2.2.1, segue que a soma, a diferença e o produto de inteiros são inteiros sobre A. Como α_i é um conjugado de α sobre $\mathbb{K}$, segue que existe um $\mathbb{K}-$isomorfismo $\sigma_i : \mathbb{K}[\alpha] \to \mathbb{K}[\alpha_i]$, definido por $\sigma_i(\alpha) = \alpha_i$. Como α é inteiro sobre A, segue que

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

com $a_i \in A$. Aplicando σ_i, segue que

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

Assim, $\sigma_i(\alpha) = \alpha_i$ é inteiro sobre A, para todo $i = 1, 2, \ldots, n$. Portanto, os coeficientes de $f_\alpha(x)$ são inteiros sobre A. Em particular, $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos inteiros sobre de A. □

Corolário 2.3.1. *Se A é integralmente fechado, então os coeficientes do polinômio característico $f_\alpha(x)$ são elementos de A. Em particular, $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos de A.*

Demonstração. Os coeficientes do polinômio característico $f_\alpha(x)$ são elementos de $\mathbb{K}$ e são inteiros sobre A. Como A é integralmente fechado, segue que os coeficientes de $f_\alpha(x)$ pertencem a A. Em particular, $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos de A. □

Observação 2.3.5. *Quando tivermos $\alpha \in \mathbb{L}$ um inteiro algébrico, ou seja, um inteiro sobre $\mathbb{Z}$, segue que os coeficientes do polinômio característico $f_\alpha(x)$ são elementos inteiros, pois $\mathbb{Z}$ é integralmente fechado (Exemplo 2.2.2) e o resultado decorre do Corolário 2.3.1. Em particular, $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$ são números inteiros.*

Proposição 2.3.3. *Seja $\mathbb{K}$ um corpo de números. Então, $\alpha \in \mathbb{K}$ é um inteiro algébrico se, e somente se, seu polinômio característico tem coeficientes inteiros.*

Demonstração. Pela Observação 2.3.5, como α é um inteiro algébrico, segue que os coeficientes do seu polinômio característico são inteiros. Reciprocamente, por hipótese α tem o polinômio característico com coeficientes inteiros e $f_\alpha(\alpha) = 0$. Assim, α é um inteiro algébrico. □

Fizemos até agora a teoria geral de norma e traço, nos nossos estudos vamos particularizar esses casos para os corpos de números. Vamos considerar $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, com θ o elemento primitivo de $\mathbb{K}$.

Exemplo 2.3.2. *Se $\mathbb{K} = \mathbb{Q}(i)$, então i é um elemento algébrico, pois é raiz do polinômio $p(x) = x^2 + 1$ e $p(x)$ é de fato o polinômio minimal de i. Por este motivo, o conjunto $\{1, i\}$ é uma base para $\mathbb{Q}(i)$ sobre $\mathbb{Q}$. Se $\alpha \in \mathbb{Q}(i)$, então $\alpha = a + bi$, com $a, b \in \mathbb{Q}$. Como $-i$ e i são as raízes de $p(x)$, segue que os $\mathbb{Q}$-monomorfismos são dados por*

$$\sigma_1(a + bi) = a + bi \text{ e}$$

$$\sigma_2(a + bi) = a - bi.$$

No próximo resultado apresentamos de um modo mais geral esses $\mathbb{Q}$-monomorfismos em $\mathbb{K} = \mathbb{Q}(\theta)$.

Teorema 2.3.2. *Se $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números de grau n, então existem exatamente n monomorfismos distintos*

$$\sigma_i : \mathbb{K} \to \mathbb{C}$$

definidos por $\sigma_i(\theta) = \theta_i$, para $i = 1, 2, \ldots, n$, onde os elementos $\theta_1, \theta_2, \ldots, \theta_n$ são as raízes distintas em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.

Demonstração. Consideramos o polinômio minimal de θ sobre $\mathbb{Q}$ como

$$m_\theta(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n.$$

Assim,

1. $m_\theta(x)$ admite n raízes no seu corpo de raízes dadas por $\theta_1, \theta_2, \ldots, \theta_n$ e são elementos de $\mathbb{C}$. Por convenção, chamamos $\theta = \theta_1$.

2. As n raízes são distintas. De fato, suponhamos que exista $\theta_i = \theta_j$, para algum $i, j \in \{1, 2, \ldots, n\}$ distintos. Dessa forma, $m_\theta(x) = (x - \theta_i)^2 q(x)$. Vamos verificar que $m_\theta(x)$ não é o polinômio minimal de θ_i, pois se fosse teríamos que $m'_\theta(x) = 2(x - \theta_i)q(x)$ e $m'_\theta(\theta_i) = 0$ onde $\partial(m'_\theta) = n - 1$, o que é um absurdo. Assim, $m_\theta(x)$ não é o polinômio minimal de θ_i. Logo, suponhamos que $d(x)$ seja o polinômio minimal de θ_i sobre $\mathbb{Q}$, e assim, $d(x)$ divide $m_\theta(x)$ e $1 \leq \partial(d) < n$. Logo, existe $g(x) \in \mathbb{Q}[x]$ tal que $m_\theta(x) = d(x)q(x)$, com $\partial(g) = n - \partial(d)$. E assim, teríamos que θ é raiz de $d(x)$ ou de $q(x)$, e isso é um absurdo pois contraria a minimalidade de $p(x)$. Logo, $\theta_i \neq \theta_j$ para todo $i, j \in \{1, 2, \ldots, n\}$.

3. Agora, seja $\sigma : \mathbb{Q}(\theta) \to \mathbb{C}$ um monomorfismo (injetora e um homomorfismo). Sem perda de generalidade, suponhamos que $\sigma(a) = a$, para todo $a \in \mathbb{Q}$. Resta-nos provar qual o valor de $\sigma(\theta)$. Vamos mostrar que $\sigma(\theta) = \theta_i$, para algum $i = 1, 2, \ldots, n$. De fato, como
$$m_\theta(\theta) = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} + \theta^n = 0,$$
segue que
$$\sigma(m_\theta(\theta)) = \sigma(a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} + \theta^n) = \sigma(0),$$
e assim,
$$a_0 + a_1\sigma(\theta) + \cdots + a_{n-1}\sigma(\theta)^{n-1} + \sigma(\theta)^n = 0,$$
ou seja, $\sigma(\theta)$ é uma raiz de $p(x)$. Portanto, $\sigma(\theta) = \theta_i$, para algum $i = 1, 2, \ldots, n$. Consequentemente, existe no máximo n $\mathbb{Q}$-monomorfismos que são σ_i, com $i = 1, 2, \ldots, n$, dados por $\sigma(\theta) = \theta_i$.

4. Agora, vamos mostrar que existem exatamente n $\mathbb{Q}$-monomorfismos, ou seja, $\sigma_i \neq \sigma_j$ para i e j distintos em $\{1, 2, \ldots, n\}$. Se $\sigma_i = \sigma_j$, então $\sigma_i(\beta) = \sigma_j(\beta)$, para todo $\beta \in \mathbb{K}$. Em particular, $\sigma_i(\theta) = \sigma_j(\theta)$. Pelo item 3), segue que $\sigma_i(\theta) = \theta_i$ e $\sigma_j(\theta) = \theta_j$, ou seja, $\theta_i = \theta_j$, com i e j distintos e isso não ocorre. Portanto, $\sigma_i \neq \sigma_j$, para todo $i, j \in \{1, 2, \ldots, n\}$.

Com isso provamos o teorema. □

Proposição 2.3.4. *Sejam $\mathbb{K}$ um corpo de números com $[\mathbb{K} : \mathbb{Q}] = n$ e $\sigma_1, \ldots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Se $\alpha \in \mathbb{K}$, então*

1. *O **traço** de α sobre $\mathbb{K}$ é dado por*
$$\mathcal{T}r(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha). \tag{2.1}$$

2. *A **norma** de α sobre $\mathbb{K}$ é dada por*
$$\mathcal{N}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha). \tag{2.2}$$

3. O ***polinômio característico*** *de α sobre $\mathbb{K}$ é dado por*

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)). \tag{2.3}$$

Demonstração. A demonstração segue diretamente da junção do Teorema 2.3.1 e do Teorema 2.3.2. □

Observação 2.3.6. *O polinômio característico $\alpha \in \mathbb{K}$ também pode ser escrito como*

$$\begin{aligned} f_\alpha(x) &= x^n - \left(\sum_{i=1}^{n}\sigma_i(\alpha)\right)x^{n-1} + \cdots + (-1)^n\left(\prod_{i=1}^{n}\sigma_i(\alpha)\right) \\ &= x^n - (\mathcal{T}r(\alpha))\,x^{n-1} + \cdots + (-1)^n\,(\mathcal{N}(\alpha))\,. \end{aligned} \tag{2.4}$$

Exemplo 2.3.3. *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\alpha = 1 + \sqrt{7}$ um elemento de $\mathbb{K}$. Nesse caso, o elemento primitivo de $\mathbb{K}$ é o $\sqrt{7}$ e $m_{\sqrt{7}}(x) = x^2 - 7$. Assim, as raízes do polinômio minimal de $\sqrt{7}$ são $\sqrt{7}$ e $-\sqrt{7}$. Logo, consideramos $\sigma_i : \mathbb{K} \to \mathbb{C}$ os Q-monomorfismos que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\sqrt{7}) = \sqrt{7}$ e $\sigma_2(\sqrt{7}) = -\sqrt{7}$. Assim,*

1. $\mathcal{T}r(1+\sqrt{7}) = \sigma_1(1+\sqrt{7}) + \sigma_2(1+\sqrt{7}) = \sigma_1(1) + \sigma_1(\sqrt{7}) + \sigma_2(1) + \sigma_2(\sqrt{7}) = 2$,
2. $\mathcal{N}r(1+\sqrt{7}) = \sigma_1(1+\sqrt{7})\sigma_2(1+\sqrt{7}) = (\sigma_1(1) + \sigma_1(\sqrt{7}))(\sigma_2(1) + \sigma_2(\sqrt{7})) = -6$ *e*
3. $f_{(1+\sqrt{7})}(x) = x^2 - \mathcal{T}r(1+\sqrt{7})x + \mathcal{N}(1+\sqrt{7}) = x^2 - 2x - 6$.

2.4 Base integral e base potente

Nesta seção, apresentamos o conceito de base integral e base potente num contexto geral. Finalmente, veremos alguns resultados sobre essas bases nos corpos de números. As referências utilizadas foram [3] e [5].

Proposição 2.4.1. *Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_\mathbb{L}$ o anel dos inteiros de A em $\mathbb{L}$. Sejam $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$, onde $\det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$ e $\alpha \in \mathbb{L}$. Se $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = 0$ para todo $\beta \in \mathbb{L}$, então $\alpha = 0$.*

Demonstração. Consideramos $\alpha \in \mathbb{L}$. Como $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que podemos escrever

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n, \text{ com } a_i \in \mathbb{K} \text{ para } = 1, 2, \ldots, n.$$

Assim, é suficiente mostrar que $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\alpha_j) = 0$, para $j = 1, 2, \ldots, n$ e então $\alpha = 0$. Agora, $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$ se, e somente se, $\alpha\alpha_j = a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + \cdots + a_n\alpha_n\alpha_j$ se, e somente se, $0 = \mathcal{T}_{\mathbb{L}|K}(\alpha\alpha_j) = a_1\mathcal{T}_{\mathbb{L}|K}(\alpha_1\alpha_j) + a_2\mathcal{T}_{\mathbb{L}|K}(\alpha_2\alpha_j) + \cdots + a_n\mathcal{T}_{\mathbb{L}|K}(\alpha_n\alpha_j)$, para todo $j = 1, 2, \ldots, n$. Deste modo, na forma matricial

$$\begin{bmatrix} \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_1) & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_1) & \cdots & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_1) \\ \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_2) & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_2) & \cdots & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_n) & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_n) & \cdots & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Por hipótese, $\det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$, e assim, $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. □

Corolário 2.4.1. *A aplicação $\varphi : \mathbb{L} \to Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K})$ dado por $\varphi(\alpha) = S_\alpha$, onde $S_\alpha = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta)$, com $\beta \in \mathbb{L}$ é um isomorfismo.*

Demonstração. Vejamos a esquematização deste isomorfismo

$$\begin{array}{rccccccc} \varphi: & \mathbb{L} & \to & Hom_{\mathbb{K}}(\mathbb{L},\mathbb{K}) & & & & \\ & \alpha & \mapsto & S_\alpha: & \mathbb{L} & \to & \mathbb{K} \\ & & & & \beta & \mapsto & \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta). \end{array}$$

Vamos mostrar que φ é um homomorfismo.

1. Se $\alpha_1, \alpha_2 \in \mathbb{L}$ e $\beta \in \mathbb{L}$, então

$$\begin{aligned} \varphi(\alpha_1+\alpha_2)(\beta) = S_{\alpha_1+\alpha_2}(\beta) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}((\alpha_1+\alpha_2)\beta) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_1\beta) + \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_2\beta) = \\ = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = \varphi(\alpha_1)(\beta) + \varphi(\alpha_2)(\beta) = (\varphi(\alpha_1)+\varphi(\alpha_2))(\beta). \end{aligned}$$

2. Se $\alpha \in \mathbb{L}$, $a \in \mathbb{K}$ e $\beta \in \mathbb{L}$, então

$$\begin{aligned} \varphi(a\alpha)(\beta) = S_{a\alpha}(\beta) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}((a\alpha)\beta) = a\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = aS_\alpha(\beta) = a\varphi(\alpha)(\beta) = \\ = (a\varphi(\alpha))(\beta). \end{aligned}$$

Por outro lado, se $\alpha \in Ker(\varphi)$, então $\varphi(\alpha) = 0$, ou seja, $S_\alpha(\beta) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = 0$, para todo $\beta \in \mathbb{L}$. Pela Proposição 2.4.1, segue que $\alpha = 0$, o que implica que φ é injetora. Agora, como $\dim_{\mathbb{K}}(\mathbb{L}) = \dim_{\mathbb{K}}(Hom_{\mathbb{K}}(\mathbb{L} : \mathbb{K}))$, segue que φ é sobrejetora. Portanto, φ é um isomorfismo. □

Teorema 2.4.1. *Se A é um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre finitamente gerado de posto n.*

Demonstração. Consideramos $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como a extensão $\mathbb{K} \subseteq \mathbb{L}$ é finita, segue que a extensão é algébrica. Dessa forma, α_i é algébrico, para $i = 1, 2, \ldots, n$. Assim, consideramos $a_{ik} \in A$ não todos nulos para $i = 1, 2, \ldots, n$ e $k = 0, 1, \ldots, n$. Sem perda de generalidade, suponhamos que $a_{in} \neq 0$. Logo,

$$a_{i0} + a_{i1}\alpha_i + a_{i2}\alpha_i^2 + \cdots + a_{in}\alpha_i^n = 0.$$

Multiplicando por a_{in}^{n-1}, segue que $a_{i0}(a_{in}^{n-1}) + a_{i1}\alpha_i(a_{in}^{n-1}) + a_{i2}\alpha_i^2(a_{in}^{n-1}) + \cdots + a_{in}\alpha_i^n(a_{in}^{n-1}) = 0$ se, e somente se, $(a_{i0}a_{in}^{n-1}) + (a_{i1}a_{in}^{n-2})(a_{in}\alpha_i) + (a_{i2}a_{in}^{n-3})(a_{in}\alpha_i)^2 + \cdots + a_{in}(a_{in}\alpha_i)^n = 0$. Assim, $a_{in}\alpha_i = \beta_i \in \mathcal{O}_{\mathbb{K}}$, para $i = 1, 2, \ldots, n$. Agora, vamos mostrar que $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Para isso, suponhamos que

$$b_1\beta_1 + b_2\beta_2 + \cdots + b_n\beta_n = 0,$$

onde $b_i \in A$, para $i = 1, 2, \ldots, n$. Assim,

$$b_1a_{1n}\alpha_1 + b_2a_{2n}\alpha_2 + \cdots + b_na_{nn}\alpha_n = 0.$$

Como $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $b_ia_{in} = 0$ e como $a_{in} \neq 0$, segue que $b_i = 0$, para $i = 1, 2, \ldots, n$. Assim, $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é linearmente independente com n elementos. Logo, $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Agora, pelo Corolário 2.4.1, segue que existe $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ tal que $\varphi(\beta_i)(\gamma_j) = S_{\beta_i}(\gamma_j) =$

$\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_i\gamma_j) = \delta_{ij}$, para $i, j = 1, 2, \ldots, n$ ($\delta_{ij} = 0$, se $i \neq j$ e $\delta_{ij} = 1$ se $i = j$). Consideramos $\alpha \in \mathcal{O}_{\mathbb{L}}$, logo $\alpha\beta_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$. Como A é integralmente fechado, pelo Corolário 2.3.1, segue que $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta_i) \in A$. Agora, seja

$$\alpha = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_n\gamma_n, \text{ com } c_i \in \mathbb{K}, \text{ para } i = 1, 2, \ldots, n.$$

Multiplicando por β_i e aplicando a função traço, segue que

$$\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta_i) = c_1\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_i\gamma_1) + c_2\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_i\gamma_2) + \cdots + c_n\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_i\gamma_n), \text{ para } i = 1, 2, \ldots, n.$$

Logo, $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha\beta_i) = c_i \in A$, para $i = 1, 2, \ldots, n$. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um A-módulo livre gerado por $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$. □

Corolário 2.4.2. *Sejam A um anel principal e $\mathbb{K}$ seu corpo de frações.*

1. *$\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n.*
2. *Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{L}}$ é um ideal, então $\mathcal{I}$ é um A-módulo livre de posto n.*

Demonstração. Para o item (1), se A é um anel principal, então um submódulo é um A-módulo livre de posto menor ou igual a n (Teorema 2.1.3). Pelo Teorema 2.4.1, segue que $\mathcal{O}_{\mathbb{L}}$ contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$ que possui n elementos. Portanto, $\mathcal{O}_{\mathbb{L}}$ tem posto n. Para o item (2), sejam $\alpha \in \mathcal{I}$ não nulo e $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ um base de $\mathcal{O}_{\mathbb{L}}$. Se $a_1\alpha\alpha_1 + a_2\alpha\alpha_2 + \cdots + a_n\alpha\alpha_n = 0$, com $a_i \in A$, para $i = 1, 2, \ldots, n$, então $a_i\alpha = 0$ para $i = 1, 2, \ldots, n$. Como A é um domínio, segue que $a_i = 0$, para $i = 1, 2, \ldots, n$. Assim, $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n\} \in \mathcal{I}$ é linearmente independente sobre A. Portanto, $\mathcal{I}$ é um A-módulo livre de posto n. □

Agora, consideramos $\mathbb{K}$ um corpo de números e $A = \mathbb{Z}$. O resultado, a seguir, garante que todo anel dos inteiros é um Z-módulo livre com posto igual ao grau do corpo de números.

Corolário 2.4.3. *Se $\mathbb{K}$ é um corpo de números de grau n, então o seu anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.*

Demonstração. Como $\mathbb{Z}$ é um domínio principal, pelo Corolário 2.4.2, segue que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. □

Com a motivação do Corolário 2.4.3, podemos definir uma base integral.

Definição 2.4.1. *Se $\mathbb{K}$ é um corpo de números, então qualquer base do $\mathbb{Z}$-módulo livre $\mathcal{O}_{\mathbb{K}}$ é chamada de **base integral** de $\mathbb{K}$.*

Corolário 2.4.4. *Seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros do corpo de números $\mathbb{K}$ de grau n. Todo ideal não nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre finitamente gerado de posto n.*

Demonstração. Vejamos que $\mathcal{I}$ é um $\mathbb{Z}$-submódulo de $\mathcal{O}_{\mathbb{K}}$. Como $\mathbb{Z}$ é principal, segue do Teorema 2.1.3 que $\mathcal{I}$ é um $\mathbb{Z}$-módulo livre finitamente gerado de posto menor ou igual que n. E pelo Corolário 2.4.2, segue que $\mathcal{I}$ é um A-módulo livre de posto n. □

Observamos que, se $\mathbb{K}$ é um corpo de números de grau n, então toda base integral $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, uma vez que o conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathcal{O}_{\mathbb{K}} \subseteq \mathbb{K}$ é linearmente independente sobre $\mathbb{Q}$ e possui n elementos.

Definição 2.4.2. *Seja $\mathbb{K} = \mathbb{Q}(\alpha)$ um corpos de números de grau n, com $\alpha \in \mathbb{K}$. Se o conjunto $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ for uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, B é chamado de **base de potências** (ou **base potente**).*

Por consequente, pela teoria de corpos, segue que toda extensão de corpos de números admite uma base potente.

2.5 Discriminante

Nesta seção, apresentamos o conceito de discriminante de uma extensão de anéis para $A \subseteq B$ anéis tal que B é um A-módulo livre finitamente gerado de posto n e particularizaremos os resultados para os corpos de números. As referências utilizadas foram [5] e [13].

Definição 2.5.1. *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre finitamente gerado de posto n. Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ um conjunto de elementos de B. O* ***discriminante*** *de $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, é definido por:*

$$\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(\mathcal{T}r_{B|A}(\alpha_i\alpha_j)) \in A,$$

onde $i, j = 1, 2, \ldots, n$.

Observação 2.5.1. *Como no caso da norma e do traço, podemos simplesmente denotar o discriminante $\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ por $\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ quando não houver dúvidas. Mais especificamente, a notação compacta $\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ será utilizada para os corpos de números.*

Exemplo 2.5.1. *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\{1, \sqrt{7}\}$ uma conjunto em $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{T}r(1) = 2$, $\mathcal{T}r(\sqrt{7}) = 0$ e $\mathcal{T}r(7) = 14$, segue que*

$$\mathcal{D}(1, \sqrt{7}) = \det\begin{pmatrix} \mathcal{T}r(1.1) & \mathcal{T}r(1.\sqrt{7}) \\ \mathcal{T}r(\sqrt{7}.1) & \mathcal{T}r(\sqrt{7}.\sqrt{7}) \end{pmatrix} = \det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\sqrt{7}) \\ \mathcal{T}r(\sqrt{7}) & \mathcal{T}r(7) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 14 \end{pmatrix},$$

e assim, $\mathcal{D}(1, \sqrt{7}) = 28$.

Mantendo as notações da Definição 2.5.1, vamos explorar alguns resultados sobre os discriminantes.

Proposição 2.5.1. *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre finitamente gerado de posto n. Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ um conjunto de elementos de B. Se $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é um conjunto de elementos de B tal que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in A$, para $i = 1, 2, \ldots, n$, então*

$$\mathcal{D}_{B|A}(\beta_1, \beta_2, \ldots, \beta_n) = (\det(a_{ij}))^2\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Demonstração. Para o conjunto $\{\beta_1, \beta_2, \ldots, \beta_n\}$, por definição, segue que

$$\mathcal{D}_{B|A}(\beta_1, \beta_2, \ldots, \beta_n) = det(\mathcal{T}r_{B|A}(\beta_r\beta_s)), \text{ para } r, s = 1, 2, \ldots, n.$$

Por hipótese, se $\beta_r = \sum_{i=1}^{n} a_{ri}\alpha_i$ e $\beta_s = \sum_{j=1}^{n} a_{sj}\alpha_j$, então $\beta_r\beta_s = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ri}a_{sj}\alpha_i\alpha_j$. Aplicando a função traço, segue que

$$\mathcal{T}r_{B|A}(\beta_r\beta_s) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ri}a_{sj}\mathcal{T}r_{B|A}(\alpha_i\alpha_j),$$

e na forma matricial, podemos apresentar este resultado como

$$\mathcal{T}r_{B|A}(\beta_r\beta_s) = (a_{ri})(\mathcal{T}r_{B|A}(\alpha_i\alpha_j))(a_{sj})^t.$$

Assim,

$$\begin{aligned}\mathcal{D}_{B|A}(\beta_1,\beta_2,\ldots,\beta_n) &= det(\mathcal{T}r_{B|A}(\beta_r\beta_s)) = \\ &= \det((a_{ri})(\mathcal{T}r_{B|A}(\alpha_i\alpha_j))(a_{sj})^t) = \\ &= \det(a_{ri})\det(\mathcal{T}r_{B|A}(\alpha_i\alpha_j))\det((a_{sj})^t) = \\ &= (\det(a_{ri}))^2\det(\mathcal{T}r_{B|A}(\alpha_i\alpha_j)) = \\ &= (\det(a_{ri}))^2\mathcal{D}_{B|A}(\alpha_1,\alpha_2,\ldots,\alpha_n).\end{aligned}$$

Portanto, $\mathcal{D}_{B|A}(\beta_1,\beta_2,\ldots,\beta_n) = (\det(a_{ij}))^2\mathcal{D}_{B|A}(\alpha_1,\alpha_2,\ldots,\alpha_n)$. □

Corolário 2.5.1. *Seja A um anel dos integridade. Se $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ e $\{\beta_1,\beta_2,\ldots,\beta_n\}$ são bases de B sobre A, então $\mathcal{D}_{B|A}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ e $\mathcal{D}_{B|A}(\beta_1,\beta_2,\ldots,\beta_n)$ são associados (um divide o outro) ou ambos possuem determinantes nulos.*

Demonstração. Como $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ é uma base, segue que podemos escrever β_j como combinação linear da base $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$, ou seja, $\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$, para $j = 1,2,\ldots,n$ e com $a_{ij} \in A$. Pela Proposição 2.5.1, segue que

$$\mathcal{D}_{B|A}(\beta_1,\beta_2,\ldots,\beta_n) = (\det(a_{ij}))^2\mathcal{D}_{B|A}(\alpha_1,\alpha_2,\ldots,\alpha_n).$$

Como (a_{ij}) é inversível, segue que o determinante de (a_{ij}) é uma unidade do anel A. Portanto, $\mathcal{D}_{B|A}(\beta_1,\beta_2,\ldots,\beta_n)$ e $\mathcal{D}_{B|A}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ são associados ou ambos os determinantes são nulos. □

Exemplo 2.5.2. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números. Vamos calcular o discriminante de $\{1+\sqrt{7}, -4-\sqrt{7}\} \subseteq \mathcal{O}_K$ uma outra base de $\mathbb{K}$. Pelo Exemplo 2.5.1 calculamos o discriminante da base $\{1,\sqrt{7}\}$, $\mathcal{D}(1,\sqrt{7}) = 28$. Pela Proposição 2.5.1, segue que*

$$\mathcal{D}(1+\sqrt{7}, -4-\sqrt{7}) = \det\begin{pmatrix} 1 & 1 \\ -4 & -1 \end{pmatrix}^2 \mathcal{D}(1,\sqrt{7}) = (3)^2(28) = 756.$$

Proposição 2.5.2. *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre finitamente gerado de posto n. Seja A um anel dos integridade. O conjunto $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ de elementos de B é linearmente dependente sobre A se, e somente se, $\mathcal{D}_{B|A}(\alpha_1,\alpha_2,\ldots,\alpha_n) = 0$.*

Demonstração. Suponhamos que o conjunto $\{\alpha_1,\alpha_2,\ldots,\alpha_n\} \subseteq B$ é linearmente dependente sobre A. Assim, existem $a_i \in A$, com $i = 1,2,\ldots,n$, não todos nulos, tal que

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n = 0.$$

Consideramos $a_1 \neq 0$ e $\{\alpha_1',\alpha_2',\ldots,\alpha_n'\}$, onde $\alpha_1' = 0$ e $\alpha_i' = \alpha_i$, para $i = 2,3,\ldots,n$, ou seja, $\{\alpha_1',\alpha_2',\ldots,\alpha_n'\} = \{0,\alpha_2,\ldots,\alpha_n\}$. Pela definição de discriminante, segue que $\mathcal{D}_{B|A}(0,\alpha_2,\ldots,\alpha_n) = 0$, pois a matriz da forma traço possui a primeira linha nula. Logo,

$$\mathcal{D}_{B|A}(\alpha_1',\alpha_2',\ldots,\alpha_n') = \mathcal{D}_{B|A}(0,\alpha_2,\ldots,\alpha_n) = 0.$$

Podemos observar que α_i' se escreve como combinação de $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$, ou seja,

$$\begin{cases} \alpha_1' = 0 = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \\ \alpha_2' = \alpha_2 = 0\alpha_1 + 1\alpha_2 + \cdots + 0\alpha_n \\ \vdots \\ \alpha_n' = \alpha_n = 0\alpha_1 + 0\alpha_2 + \cdots + 1\alpha_n \end{cases}$$

Assim, na forma matricial, segue que

$$\begin{bmatrix} \alpha_1' \\ \alpha_2' \\ \vdots \\ \alpha_n' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

Pela Proposição 2.5.1, segue que

$$\mathcal{D}_{B|A}(\alpha_1', \alpha_2', \ldots, \alpha_n') = (\det(a_{ij}))^2 \mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Como $\det(a_{ij}) = a_1 \neq 0$, $\mathcal{D}_{B|A}(\alpha_1', \alpha_2', \ldots, \alpha_n') = 0$ e A é um domínio, segue que $\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. Reciprocamente, suponhamos que $\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. Pela definição de discriminante, segue que

$$\det(\mathcal{T}r_{B|A}(\alpha_i\alpha_j)) = \det \begin{pmatrix} \mathcal{T}r_{B|A}(\alpha_1\alpha_1) & \cdots & \mathcal{T}r_{B|A}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathcal{T}r_{B|A}(\alpha_n\alpha_1) & \cdots & \mathcal{T}r_{B|A}(\alpha_n\alpha_n) \end{pmatrix} = 0.$$

Dessa forma, as colunas $C_1, C_2, \ldots, C_n$ da matriz são linearmente dependentes sobre A. Logo, existem $a_i \in A$, para $i = 1, 2, \ldots, n$, não todos nulos, de modo que:

$$a_1C_1 + a_2C_2 + \cdots + a_nC_n = 0,$$

e assim,

$$\begin{bmatrix} \mathcal{T}r_{B|A}(\alpha_1\alpha_1) & \cdots & \mathcal{T}r_{B|A}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathcal{T}r_{B|A}(\alpha_n\alpha_1) & \cdots & \mathcal{T}r_{B|A}(\alpha_n\alpha_n) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Suponhamos que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é linearmente independente sobre A. Se $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, então $\alpha \neq 0$. Além disso, se $j = 1, 2, \ldots, n$, então

$$\begin{aligned} \mathcal{T}r_{B|A}(\alpha\alpha_j) &= \mathcal{T}r_{B|A}(a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + \cdots + a_n\alpha_n\alpha_j) = \\ &= a_1\mathcal{T}r_{B|A}(\alpha_1\alpha_j) + a_2\mathcal{T}r_{B|A}(\alpha_2\alpha_j) + \cdots + a_n\mathcal{T}r_{B|A}(\alpha_n\alpha_j) = \\ &= 0. \end{aligned}$$

Como $\alpha_1, \alpha_2, \ldots, \alpha_n$ são linearmente independentes sobre A, segue que formam uma base de B em A. Por outro lado, como $\alpha \neq 0$, segue que o conjunto $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n\}$ também é uma base de B sobre A. Agora, se $\beta \in B$, então β é uma combinação linear de $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n\}$. Logo $\mathcal{T}r_{B|A}(\beta) = 0$. Em particular, $\mathcal{T}r_{B|A}(1) = 0$, o que é um absurdo. Portanto, o conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é linearmente dependente. □

Corolário 2.5.2. *Sejam $A \subseteq B$ anéis tais que B é um A-módulo livre finitamente gerado de posto n. Seja A um anel dos integridade. O conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de elementos de B é linearmente independente sobre A se, e somente se, $\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$.*

Demonstração. O resultado segue da negação da Proposição 2.5.2. □

Observação 2.5.2. *Como consequência do Corolário 2.5.2, se o conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de B sobre A, então $\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$.*

Agora, apresentamos alguns resultados sobre corpos de números. Na Seção 2.4, vimos que o Corolário 2.4.3 afirma que o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre finitamente gerado de posto n, o que nos motiva a definir o discriminante dos corpos de números através da base integral.

Definição 2.5.2. *Seja $\mathbb{K}$ um corpo de números. O discriminante de $\mathbb{K}$ é definido como o discriminante de uma base integral de seu anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ e denotado por $\mathcal{D}(\mathbb{K})$.*

Lema 2.5.1. *(Lema de Dedekind) Se G é um grupo, $\mathbb{K}$ um corpo e $\sigma_1, \sigma_2, \ldots, \sigma_n$ são homomorfismos distintos e não nulos de G no grupo multiplicativo $\mathbb{K}^*$, então os $\sigma_i's$ são linearmente independentes sobre $\mathbb{K}$.*

Demonstração. Suponhamos, por absurdo, que os $\sigma_i's$ são linearmente dependentes. Logo, existem $a_i \in \mathbb{K}$, para $i = 1, 2, \ldots, n$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i = 0$ e consideramos r o número que representa a quantidade de $a_i's$ não nulos. Se $r = 1$, então $a_1\sigma_1 = 0$, ou seja, $a_1 = 0$ ou $\sigma_1 = 0$ o que não ocorre. Logo, $r \geq 2$, pois σ_i' são não nulos. Seja $g \in G$. Como $\sigma_i's$ são homomorfismos, segue que:

$$a_1\sigma_1(g) + a_2\sigma_2(g) + \cdots + a_r\sigma_r(g) = 0. \tag{2.5}$$

Logo, para gh, com $h \in G$, segue que

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_2(h) + \cdots + a_r\sigma_r(g)\sigma_r(h) = 0. \tag{2.6}$$

Multiplicando a Equação (2.5) por $\sigma_1(h)$, segue que

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_1(h) + \cdots + a_r\sigma_r(g)\sigma_1(h) = 0. \tag{2.7}$$

Fazendo a diferença das Equações (2.7) e (2.6), segue que

$$a_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \cdots + a_r(\sigma_1(h) - \sigma_r(h))\sigma_r(g) = 0. \tag{2.8}$$

Como isso vale para todo $g \in G$, e como tomamos r o menor possível segue que $a_2(\sigma_1(h) - \sigma_2(h)) = 0$. O que implica que $\sigma_1(h) = \sigma_2(h)$, para todo $h \in G$ pois $a_2 \neq 0$. Mas isso contradiz a hipótese de que os $\sigma_i's$ são distintos. Portanto, os $\sigma_i's$ são linearmente independentes. □

Proposição 2.5.3. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então*

$$\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2. \tag{2.9}$$

Demonstração. Pela definição, segue que o discriminante de $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é calculado por

$$\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\mathcal{T}r(\alpha_i\alpha_j)).$$

Pela Proposição 2.3.4, segue que

$$\mathcal{T}r(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Agora, como

$$\sum_{k=1}^{n}\sigma_k(\alpha_i)\sigma_k(\alpha_j)=\begin{bmatrix}\sigma_1(\alpha_1)&\sigma_2(\alpha_1)&\cdots&\sigma_n(\alpha_1)\\ \sigma_1(\alpha_2)&\sigma_2(\alpha_2)&\cdots&\sigma_n(\alpha_2)\\ \vdots&\vdots&\ddots&\vdots\\ \sigma_1(\alpha_n)&\sigma_2(\alpha_n)&\cdots&\sigma_n(\alpha_n)\end{bmatrix}\begin{bmatrix}\sigma_1(\alpha_1)&\sigma_1(\alpha_2)&\cdots&\sigma_1(\alpha_n)\\ \sigma_2(\alpha_1)&\sigma_2(\alpha_2)&\cdots&\sigma_2(\alpha_n)\\ \vdots&\vdots&\ddots&\vdots\\ \sigma_n(\alpha_1)&\sigma_n(\alpha_2)&\cdots&\sigma_n(\alpha_n)\end{bmatrix},$$

segue que

$$\det(\mathcal{T}r(\alpha_i\alpha_j))=\det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i)\sigma_k(\alpha_j)\right)=\det(\sigma_i(\alpha_j))^2.$$

Portanto, $\mathcal{D}(\alpha_1,\alpha_2,\ldots,\alpha_n)=\det(\sigma_i(\alpha_j))^2$. □

Corolário 2.5.3. $\mathcal{D}(\alpha_1,\alpha_2,\ldots,\alpha_n)=\det(\sigma_i(\alpha_j))^2\neq 0$.

Demonstração. Se $\det(\sigma_i(\alpha_j))^2=0$, então existem $a_1,a_2,\ldots,a_n\in\mathbb{C}$, não todos nulos, tal que $\sum_{i=1}^{n}a_i\sigma_i(\alpha_j)=0$, para $j=1,2,\ldots,n$. Pela linearidade, segue que que $\sum_{i=1}^{n}a_i\sigma_i(\alpha)=0$, para todo $\alpha\in\mathbb{K}$. Pelo Lema 2.5.1, segue que σ_i são linearmente independentes, o que chega num absurdo. Portanto, $\det(\sigma_i(\alpha_j))^2\neq 0$. □

Exemplo 2.5.3. *Seja $\mathbb{K}=\mathbb{Q}(\sqrt{7})$ um corpo de números. Vamos calcular o discriminante da base $\{1,\sqrt{7}\}$ de $\mathbb{K}$ sobre $\mathbb{Q}$ por meio dos monomorfismos. Neste caso, para $\alpha=a+b\sqrt{7}\in\mathbb{K}$ os monomorfismos são $\sigma_1(\alpha)=a+b\sqrt{7}$ e $\sigma_2(\alpha)=a-b\sqrt{7}$. Assim,*

$$\mathcal{D}(1,\sqrt{7})=\det\begin{pmatrix}\sigma_1(1)&\sigma_1(\sqrt{7})\\ \sigma_2(1)&\sigma_2(\sqrt{7})\end{pmatrix}^2=\det\begin{pmatrix}1&\sqrt{7}\\ 1&-\sqrt{7}\end{pmatrix}^2=(-2\sqrt{7})^2=28.$$

Proposição 2.5.4. *Seja $\mathbb{K}=\mathbb{Q}(\theta)$ um corpo de números de grau n, $\theta\in\mathbb{K}$ o seu elemento primitivo. Se $p(x)$ é o polinômio minimal de θ, então*

$$\mathcal{D}(1,\theta,\theta^2,\ldots,\theta^{n-1})=(-1)^{\frac{n(n-1)}{2}}\mathcal{N}(p'(\theta)),\tag{2.10}$$

onde $p'(x)$ é a derivada de $p(x)$.

Demonstração. Sejam $\theta_1,\theta_2,\ldots,\theta_n$ as raízes de $p(x)$ e, sem perda de generalidade, tomamos $\theta=\theta_1$. Consideramos σ_i os $\mathbb{Q}$-monomorfismos que fixam os elementos de $\mathbb{Q}$ e $\sigma_i(\theta)=\theta_i$, para $i=1,2,\ldots,n$. Pela Proposição 2.5.3, segue que o discriminante de $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ é calculado por:

$$\mathcal{D}(1,\theta,\theta^2,\ldots,\theta^{n-1})=\det(\sigma_i(\theta^j))^2=\det(\theta_i^j)^2,$$

onde $i=1,2,\ldots,n$ e $j=0,1,2,\ldots,n-1$. Assim,

$$\det(\theta_i^j)=\det\begin{pmatrix}1&\theta_1&\cdots&\theta_1^{n-1}\\ 1&\theta_2&\cdots&\theta_2^{n-1}\\ \vdots&\vdots&\ddots&\vdots\\ 1&\theta_n&\cdots&\theta_n^{n-1}\end{pmatrix}=\det\begin{pmatrix}1&1&\cdots&1\\ \theta_1&\theta_2&\cdots&\theta_n\\ \vdots&\vdots&\ddots&\vdots\\ \theta_1^{n-1}&\theta_2^{n-1}&\ldots&\theta_n^{n-1}\end{pmatrix}.$$

Esse determinante é conhecido como "determinante de Vandermonde", e assim,

$$\det(\theta_i^j)=\prod_{1\leq i<j\leq n}(\theta_i-\theta_j),$$

ou seja,

$$\mathcal{D}(1,\theta,\theta^2\ldots,\theta^{n-1}) = \prod_{1\leq i<j\leq n}(\theta_i-\theta_j)^2. \tag{2.11}$$

Por outro lado, pela Proposição 2.3.4, segue que o polinômio minimal de θ é dado por

$$p(x) = \prod_{i=1}^{n}(x-\theta_i).$$

Logo,

$$p'(x) = \sum_{j=1}^{n}\prod_{i=1,i\neq j}^{n}(x-\theta_i) \text{ e } p'(\theta_j) = \prod_{i=1,i\neq j}^{n}(\theta_j-\theta_i).$$

Dessa forma, $\prod_{j=1}^{n} p'(\theta_j) = \prod_{i,j=1,i\neq j}^{n}(\theta_j-\theta_i)$ e como $\prod_{j=1}^{n} p'(\theta_j) = \mathcal{N}(p'(\theta))$, segue que

$$\mathcal{N}(p'(\theta)) = \prod_{i,j=1,i\neq j}^{n}(\theta_j-\theta_i). \tag{2.12}$$

Agora, em $\prod_{i,j=1,i\neq j}^{n}(\theta_j-\theta_i)$ cada fator $(\theta_j-\theta_i)$, para $i<j$, aparece duas vezes, uma como $(\theta_i-\theta_j)$ e outra como $(\theta_j-\theta_i)$ e o produto das duas é $-(\theta_i-\theta_j)^2$. Assim, no produto da Equação (2.12) aparece o termo $(-1)^s$, onde s é o número de pares (i,j), com $1\leq i<j\leq n$, ou seja,

$$\mathcal{N}(p'(\theta)) = (-1)^s\prod_{1\leq i<j\leq n}(\theta_i-\theta_j)^2.$$

Agora, vamos calcular o valor de s. Para isso,

$$\begin{cases}\text{Se } i=1 \Rightarrow j=2,3,\ldots,n \text{ e } s=1\\ \text{Se } i=2 \Rightarrow j=3,4,\ldots,n \text{ e } s=2\\ \vdots\\ \text{Se } i=n-1 \Rightarrow j=n \text{ e } s=n-1.\end{cases}$$

Logo, $s = 1+2+\cdots+(n-1) = \dfrac{n(n-1)}{2}$. Dessa forma,

$$\mathcal{N}(p'(\theta)) = (-1)^{\frac{n(n-1)}{2}}\prod_{1\leq i<j\leq n}(\theta_i-\theta_j)^2,$$

e assim,

$$\prod_{1\leq i<j\leq n}(\theta_i-\theta_j)^2 = (-1)^{\frac{n(n-1)}{2}}\mathcal{N}(p'(\theta)). \tag{2.13}$$

Pelas Equações (2.11) e (2.13), segue que

$$\mathcal{D}(1,\theta,\theta^2,\ldots,\theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}}\mathcal{N}(p'(\theta)),$$

e portanto, segue o resultado. □

Proposição 2.5.5. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida no anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$. Se o discriminante $\mathcal{D}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ é livre de quadrados, então $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$.*

Demonstração. Se $\{e_1, e_2, \ldots, e_n\}$ é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$, então $\alpha_j = \sum_{i=1}^{n} a_{ij}e_j$, com $a_{ij} \in \mathbb{Z}$. Pela Proposição 2.5.1, segue que

$$\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\det(a_{ij}))^2 \mathcal{D}(e_1, e_2, \ldots, e_n).$$

Por hipótese, como $\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é livre de quadrados, segue que $\det(a_{ij}) = \pm 1$, ou seja, $\mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathcal{D}(e_1, e_2, \ldots, e_n)$, o que garante que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ também é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$. □

Proposição 2.5.6. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n. Se o polinômio minimal de θ é $p(x) = x^n + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, então*

$$\mathcal{D}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}}[n^n b^{n-1} + (-1)^{n+1}(n-1)^{n-1}a^n]. \tag{2.14}$$

Demonstração. Seja $p(x) = x^n + ax + b$ o polinômio minimal de θ. Assim,

$$p'(x) = nx^{n-1} + a \Leftrightarrow p'(\theta) = n\theta^{n-1} + a.$$

Por outro lado,

$$p(\theta) = \theta^n + a\theta + b = 0 \Leftrightarrow \theta^n = -a\theta - b \Leftrightarrow n\theta^{n-1} = -na - nb\theta^{-1}.$$

Logo, comparando as equações, segue que

$$p'(\theta) = n\theta^{n-1} + a = (-na - nb\theta^{-1}) + a = -(n-a) - nb\theta^{-1}.$$

Assim, $\theta^{-1} = (-nb)^{-1}(p'(\theta) + (n-1)a)$ e:

$$\theta = \frac{(-nb)}{p'(\theta) + (n-1)a}.$$

Como $p(\theta) = 0$, segue que:

$$\left(\frac{(-nb)}{p'(\theta) + (n-1)a}\right)^n + a\left(\frac{(-nb)}{p'(\theta) + (n-1)a}\right) + b = 0.$$

Dessa forma,

$$\frac{(-nb)^n}{[p'(\theta) + (n-1)a]^n} - \frac{(nab)}{[p'(\theta) + (n-1)a]} + b = 0.$$

Igualando os denominadores, segue que

$$\frac{(-nb)^n - nab[p'(\theta) + (n-1)a]^{n-1} + b[p'(\theta) + (n-1)a]^n}{[p'(\theta) + (n-1)]^n} = 0.$$

Como $(p'(\theta) + (n-1)a)^n \neq 0$, segue que

$$(-nb)^n - nab[p'(\theta) + (n-1)a]^{n-1} + b[p'(\theta) + (n-1)a]^n = 0.$$

Didivindo por b, segue que

$$[p'(\theta) + (n-1)a]^n - na[p'(\theta) + (n-1)a]^{n-1} + (-1)^n n^n b^{n-1} = 0.$$

Assim, o polinômio minimal de $p'(\theta)$ sobre $\mathbb{Q}$ é dado por

$$g(x) = [x + (n-1)a]^n - na[x + (n-1)a]^{n-1} + (-1)^n n^n b^{n-1}.$$

Agora, o termo constante de $g(x)$ é calculado por

$$\begin{aligned} k &= (n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1} = \\ &= (-1)(n-1)^{n-1}a^n + (-1)^n n^n b^{n-1}. \end{aligned}$$

Como a norma de $p'(\theta)$ é $(-1)^n$ vezes o termo constante k do polinômio $g(x)$ (Proposição 2.3.4), segue que

$$\begin{aligned} \mathcal{N}(p'(\theta)) &= (-1)^n k = \\ &= (-1)^n[(-1)(n-1)^{n-1}a^n + (-1)^n n^n b^{n-1}] = \\ &= n^n b^{n-1} + (-1)^{n+1}(n-1)^{n-1}a^n. \end{aligned}$$

Pela Proposição 2.5.4, segue que

$$\begin{aligned} \mathcal{D}(1, \theta, \theta^2, \ldots, \theta^n) &= (-1)^{\frac{n(n-1)}{2}} \mathcal{N}(p'(\theta)) = \\ &= (-1)^{\frac{n(n-1)}{2}} [n^n b^{n-1} + (-1)^{n+1}(n-1)^{n-1}a^n], \end{aligned}$$

o que prova a proposição. □

Exemplo 2.5.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, com θ o seu elemento primitivo, cujo polinômio minimal é $p(x) = x^3 + x + 1 \in \mathbb{Z}[x]$. Pela Proposição 2.5.6, segue que o determinante de $\{1, \theta, \theta^2\}$ é calculado por*

$$\mathcal{D}(1, \theta, \theta^2) = (-1)^{\frac{3(3-1)}{2}}[3^3 1^{3-1} + (-1)^{3+1}(3-1)^{3-1}1^3] = -(27+4) = -31.$$

Como $\mathcal{D}(1, \theta, \theta^2) = -31$ é livre de quadrados, pela Proposição 2.5.5, segue que o conjunto $\{1, \theta, \theta^2\}$ é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$, ou seja, $\mathcal{O}_\mathbb{K} = Z[\theta] = \{a + b\theta + c\theta^2 | a, b, c \in \mathbb{Z}\}$.

Corolário 2.5.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n. Se o polinômio minimal de θ é $p(x) = x^n - d \in \mathbb{Z}[x]$, com d não nulo, então*

$$\mathcal{D}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n^2+n+2}{2}}[n^n d^{n-1}]. \tag{2.15}$$

Demonstração. Seja $p(x) = x^n - d$ o polinômio minimal de θ. Assim,

$$p'(x) = nx^{n-1} \Leftrightarrow p'(\theta) = n\theta^{n-1}.$$

Por outro lado,

$$p(\theta) = \theta^n - d = 0 \Leftrightarrow \theta^n = d \Leftrightarrow n\theta^{n-1} = nd\theta^{-1}.$$

Logo, comparando as equações, segue que

$$p'(\theta) = nd\theta^{-1}.$$

Assim, $\theta^{-1} = (nd)^{-1}(p'(\theta))$ e

$$\theta = \frac{nd}{p'(\theta)}.$$

Como $p(\theta) = 0$, segue que:

$$\left(\frac{nd}{p'(\theta)}\right)^n - d = 0.$$

Dessa forma,

$$\frac{(nd)^n}{(p'(\theta))^n} - d = 0.$$

Igualando os denominadores, segue que

$$\frac{(nd)^n - d(p'(\theta))^n}{(p'(\theta))^n} = 0.$$

Como $(p'(\theta))^n \neq 0$, segue que

$$(nd)^n - d(p'(\theta))^n = 0.$$

Didivindo por $-d$, segue que

$$(p'(\theta))^n - n^n d^{n-1} = 0.$$

Assim, o polinômio minimal de $p'(\theta)$ sobre $\mathbb{Q}$ é dado por

$$g(x) = x^n - n^n d^{n-1}.$$

Agora, o termo constante de $g(x)$ é calculado por

$$k = -n^n d^{n-1}.$$

Como a norma de $p'(\theta)$ é $(-1)^n$ vezes o termo constante k do polinômio $g(x)$ (Proposição 2.3.4), segue que:

$$\begin{aligned}\mathcal{N}(p'(\theta)) &= (-1)^n k = \\ &= (-1)^n[-n^n d^{n-1}] = \\ &= (-1)^{n+1} n d^{n-1}.\end{aligned}$$

Pela Proposição 2.5.4, segue que

$$\begin{aligned}\mathcal{D}(1, \theta, \theta^2, \ldots, \theta^n) &= (-1)^{\frac{n(n-1)}{2}} \mathcal{N}(p'(\theta)) = \\ &= (-1)^{\frac{n(n-1)}{2}} [(-1)^{n+1} n d^{n-1}] = \\ &= (-1)^{\frac{n^2+n+2}{2}} [n^n d^{n-1}],\end{aligned}$$

o que prova o corolário. □

Exemplo 2.5.5. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, com θ o seu elemento primitivo, cujo polinômio minimal é $p(x) = x^3 - 2 \in \mathbb{Z}[x]$. Pela Proposição 2.5.4, segue que o determinante de $\{1, \theta, \theta^2\}$ é calculado por*

$$\mathcal{D}(1, \theta, \theta^2) = (-1)^{\frac{3^2+3+2}{2}} [3^3 2^{3-1}] = -27 \times 2^2 = -108.$$

2.6 O corpo $\mathbb{Q}(\sqrt[n]{d})$, d livre de quadrados

Neste seção, exploramos algumas proposições que remetem aos corpos de números do tipo $\mathbb{K} = \mathbb{Q}(\sqrt[n]{d})$, com $1 \neq d \in \mathbb{Z}$ livre de quadrados. Essas proposições são nossos resultados, não conhecidos na literatura, e preliminares para os capítulos seguintes para encontrar o anel dos inteiros algébricos dos corpos $\mathbb{K} = \mathbb{Q}(\sqrt[n]{d})$, cujo $n = 2, 3, 4, 5$ ou 6. Neste momento, a ideia é usar a generalização dos graus. Para o estudo dos números complexos as referências utilizadas foram [15] e [16] e os resultados posteriores são generalizações providas da inspiração das referências [7], [8] e [9].

Inicialmente, faremos uma pequena introdução aos números complexos com o objetivo de explorar as raízes de $p(x) = x^n - d$, com $d \in \mathbb{Z}$ livre de quadrados. Os números complexos $z = a + bi \in \mathbb{C}$, podem ser escritos na forma polar como

$$z = |z|[\cos(\theta) + i\,\mathrm{sen}(\theta)],$$

onde $|z| = \sqrt{a^2 + b^2}$ é o módulo de z e θ é o argumento satisfazendo $a = |z|\cos(\theta)$ e $b = |z|\,\mathrm{sen}(\theta)$.

Definição 2.6.1. *Seja $z \in \mathbb{C}$. A exponencial de z é definida por*

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \cdots = \sum_{k=1}^{\infty} \frac{z^k}{k!}. \tag{2.16}$$

Proposição 2.6.1 ([15], pág. 7)**.** *(Fórmula de Euler) Se $\theta \in \mathbb{R}$, então*

$$e^{i\theta} = \cos(\theta) + i\,\mathrm{sen}(\theta). \tag{2.17}$$

Observação 2.6.1. *No caso dos números complexos, para representar o resultado da potenciação é necessário apresentar o conceito da fórmula de Euler. Nela temos que as funções trigonométricas podem ser escritas com o uso da base neper (e), tal que*

$$\mathrm{sen}(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i} \;\; e \;\; \cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}.$$

Proposição 2.6.2. *(Primeira Fórmula de Moivre) Se $z \in \mathbb{C}$ é não nulo e $n \in \mathbb{Z}$, então*

$$z^n = |z|^n[\cos(n\theta) + i\,\mathrm{sen}(n\theta)]. \tag{2.18}$$

Demonstração. Consideramos z um número complexo. Assim, pode ser escrito como

$$z = |z|[\cos(\theta) + i\,\mathrm{sen}(\theta)].$$

Se elevarmos z a potência n, segue que

$$z^n = |z|^n[\cos(\theta) + i\,\mathrm{sen}(\theta)]^n.$$

Substituindo os valores de $\mathrm{sen}(\theta)$ e $\cos(\theta)$ da Observação 2.6.1, segue que

$$z^n = |z|^n \left(\frac{e^{i\theta} + e^{-i\theta}}{2} + i\frac{e^{i\theta} - e^{-i\theta}}{2i}\right)^n = |z|^n (e^{i\theta})^n = |z|^n e^{i(n\theta)}.$$

Da Proposição 2.6.1 (Fórmula de Euler), segue que

$$e^{i(n\theta)} = \cos(n\theta) + i\,\mathrm{sen}(n\theta).$$

Portanto, $z^n = |z|^n[\cos(n\theta) + i\,\mathrm{sen}(n\theta)]$. □

Proposição 2.6.3. *(Segunda Fórmula de Moivre) Se $z \in \mathbb{C}$ é não nulo e $n \geq 2$ um número natural, então existem n raízes n-ésimas de z que são da forma*

$$\delta_k = \sqrt[n]{|z|}\left[\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2k\pi}{n}\right)\right], \tag{2.19}$$

onde $k = 0, 1, 2, \ldots, n-1$.

Demonstração. Suponhamos que existe $\delta \in \mathbb{C}$ tal que $\delta^n = z$. Vamos escrever δ e z na forma polar como

$$\delta = |\delta|[\cos(\beta) + i\,\mathrm{sen}(\beta)] \text{ e } z = |z|[\cos(\theta) + i\,\mathrm{sen}(\theta)].$$

Assim, pela Proposição 2.6.2 (Primeira Fórmula de Moivre), segue que

$$\delta^n = |\delta|^n[\cos(n\beta) + i\,\mathrm{sen}(n\beta)].$$

Consequentemente,

$$\delta^n = z \Leftrightarrow |\delta|^n[\cos(n\beta) + i\,\mathrm{sen}(n\beta)] = |z|[\cos(\theta) + i\,\mathrm{sen}(\theta)].$$

Comparando os dois lados da igualdade, segue que $|\delta| = \sqrt[n]{|z|}$ e $\beta = \dfrac{\theta + 2k\pi}{n}$, com $k = 0, 1, 2, \ldots, n-1$. Logo,

$$\delta_k = \sqrt[n]{|z|}\left[\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2k\pi}{n}\right)\right], \text{ com } k = 0, 1, 2 \ldots, n-1.$$

Assim, as raízes n-ézimas de z são da forma

$$\sqrt[n]{z} = \delta_k, \text{ para } k = 0, 1, 2 \ldots, n-1.$$

Ainda podemos afirmar que

$$\begin{aligned} \sqrt[n]{z} &= \sqrt[n]{|z|[\cos(\theta) + i\,\mathrm{sen}(\theta)]} = \\ &= \sqrt[n]{|z|}\,\sqrt[n]{\cos(\theta) + i\,\mathrm{sen}(\theta)} = \\ &= \sqrt[n]{|z|}\left[\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2k\pi}{n}\right)\right], \end{aligned} \tag{2.20}$$

para $k = 0, 1, 2, \ldots, n-1$. Portanto, existem n raízes n-ésimas de z que são δ_k, para $k = 0, 1, 2, \ldots, n-1$. □

Definição 2.6.2. *Seja $n \geq 2$ um número natural.*

1. *Uma raiz do polinômio $x^n - 1$ é chamada de **raiz n-ésima da unidade**.*
2. *Se ξ_n é uma raiz de $x^n - 1$ (ou seja, $\xi_n^n = 1$) e se ξ_n não é raiz de $x^m - 1$ (ou seja, $\xi_n^m \neq 1$), para $1 \leq m < n$, então ξ_n é dita uma **raiz n-ésima primitiva da unidade**.*

Proposição 2.6.4. *Seja $n \geq 2$ um número natural. As raízes primitivas da unidade de $x^n - 1$ são calculadas como:*

$$\xi_n^k = e^{(\frac{2k\pi}{n})i} = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right), \tag{2.21}$$

com $k = 0, 1, \ldots, n-1$.

Demonstração. Consideramos $1 = \cos(0) + i\,\mathrm{sen}(0)$. Pela Proposição 2.6.3, segue que as raízes n-ésimas primitivas da unidade, denotadas por ξ_n^k, são calculadas por

$$\xi_n^k = \sqrt[n]{1} = \sqrt[n]{|1|[\cos(0) + i\,\mathrm{sen}(0)]} = \sqrt[n]{|1|}\left[\cos\left(\frac{0+2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{0+2k\pi}{n}\right)\right] =$$
$$= \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right),$$

para $k = 0, 1, 2, \ldots, n-1$. Usando a Proposição 2.6.1 (Fórmula de Euler), conseguimos a igualdade

$$e^{(\frac{2k\pi}{n})i} = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right), \text{ para } k = 0, 1, 2, \ldots, n-1,$$

o que prova a proposição. □

Proposição 2.6.5. *Seja $n \geq 2$ um número natural. As raízes (complexas) do polinômio $x^n - a$ são dadas por*

$$\sqrt[n]{a}\xi_n^k, \tag{2.22}$$

onde ξ_n^k são as raízes n-ésimas primitivas da unidade, para $k = 0, 1, 2, \ldots, n-1$.

Demonstração. Consideramos $\sqrt[n]{a} = \sqrt[n]{a.1} = \sqrt[n]{a}\sqrt[n]{1}$. Logo, pela Proposição 2.6.4, segue que as raízes n-ésimas primitivas da unidade são calculadas por ξ_n^k, com $k = 0, 1, 2, \ldots, n-1$. Assim, as raízes n-ésimas de a são $\sqrt[n]{a}\xi_n^k$, para $k = 0, 1, 2, \ldots, n-1$. □

Exemplo 2.6.1. *As raízes do polinômio $x^3 - 2$ são*

$$\sqrt[3]{2}\xi_3^0,\ \sqrt[3]{2}\xi_3^1 \text{ e } \sqrt[3]{2}\zeta_3^2,$$

onde $\xi_3^0 = 1$, $\xi_3^1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e $\xi_3^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Agora, vamos explorar o ambiente para $\mathbb{K} = \mathbb{Q}(\sqrt[n]{d})$ um corpo de números, com $d \in \mathbb{Z}$ livre de quadrados. O elemento $\sqrt[n]{d}$ é um inteiro algébrico, pois $p(x) = x^n - d$ é o seu polinômio minimal em $\mathbb{Z}$. Pela Teoria de Corpos, segue que $[\mathbb{Q}(\sqrt[n]{d}) : \mathbb{Q}] = \partial(p) = n$ e de fato $\mathbb{Q}(\sqrt[n]{d})$ é um corpo de números cujo elemento primitivo é o próprio $\sqrt[n]{d}$. Salvo menção contrária, $\theta = \sqrt[n]{d}$ é o elemento primitivo, com $d \in \mathbb{Z}$ livre de quadrados e o corpo de números em questão é o $\mathbb{K} = Q(\theta)$.

Definição 2.6.3. *Uma extensão $\mathbb{K} \subseteq \mathbb{L}$ é chamada de **extensão de Galois** ou **extensão galoisiana** se é uma extensão normal e separável.*

Definição 2.6.4. *Seja $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos. O **grupo de Galois** de $\mathbb{L}$ sobre $\mathbb{K}$ é definido por:*

$$Gal(\mathbb{L} : \mathbb{K}) = \{\sigma \in Aut(\mathbb{L}) | \sigma|_{\mathbb{K}} = id\}.$$

Definição 2.6.5. *Uma extensão $\mathbb{K} \subseteq \mathbb{L}$ de Galois é chamada de* ***extensão abeliana*** *se o grupo de Galois é abeliano.*

Chamamos a atenção para os corpos de números, ou seja, uma extensão da forma $\mathbb{Q} \subseteq \mathbb{K}$. Já vimos que a extensão $\mathbb{Q} \subseteq \mathbb{K}$ é separável, pois $\mathbb{Q}$ tem característica zero. Mas de maneira geral, devemos tomar cuidado com essas extensões, pois nem sempre são abelianas. Consideremos $\mathbb{K} = \mathbb{Q}(\sqrt[n]{d})$, com d livre de quadrados. O polinômio minimal dessa extensão é $p(x) = x^n - d$, que possui uma raízes em $\mathbb{Q}(\sqrt[n]{d})$, mas não sabemos se todas as raízes pertencem a $\mathbb{Q}(\sqrt[n]{d})$, nos deixando a dúvida quem nem sempre essas extensões são normais e por obséquio, nem sempre são abelianas.

Retomando as Proposições 2.6.4 e 2.6.5, sejam θ, $\theta\xi_n, \ldots, \theta\xi_n^{n-1}$ as raízes do polinômio $p(x)$, onde ξ_n^k são as raízes primitivas das unidade, para $k = 0, 1, 2, \ldots, n-1$. Assim,

$$\xi_n^k = e^{\frac{2\pi i}{n}k} = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right).$$

Pelo Teorema 2.3.2, podemos considerar σ_k os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_k(\theta) = \theta\xi_n^{k-1}$, com $k = 1, 2 \ldots, n$. Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim, podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$, tendo $a_i \in \mathbb{Q}$, com $i = 0, 1, 2, \ldots, n-1$.

As próximas proposições são resultados novos de nossa autoria, não conhecidos na literatura.

Proposição 2.6.6. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[n]{d}$ com $d \in \mathbb{Z}$ livre de quadrados, $n \in \mathbb{N}$. Se $\mathcal{O}_\mathbb{K}$ é o seu anel dos inteiros algébricos, então $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = d\mathbb{Z}$.*

Demonstração. Vamos mostrar que $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} \subseteq d\mathbb{Z}$. Se $x \in \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$, então $x \in \theta\mathcal{O}_\mathbb{K}$ e $x \in \mathbb{Z}$. Como $x \in \theta\mathcal{O}_\mathbb{K}$, segue que existe $a \in \mathcal{O}_\mathbb{K}$ tal que $x = \theta a$. Usando a Proposição 2.6.5, segue que

$$\begin{aligned}\mathcal{N}(x) = \mathcal{N}(\theta a) = \mathcal{N}(\theta)\mathcal{N}(a) = [\sigma_1(\theta)\sigma_2(\theta)\cdots\sigma_n(\theta)]\mathcal{N}(a) \overset{Prop.2.6.5}{=} \\ = [\theta \cdot \theta\xi_n^1 \cdots \theta\xi_n^{n-1}]\mathcal{N}(a) = \theta^n \xi_n^{\frac{n(n-1)}{2}}\mathcal{N}(a) = \xi_n^{\frac{n(n-1)}{2}} d\mathcal{N}(a).\end{aligned}$$

Pela Proposição 2.6.4, segue que

$$\begin{aligned}\xi_n^{\frac{n(n-1)}{2}} &= \cos\left(\frac{2n(n-1)\pi}{2n}\right) + i\,\mathrm{sen}\left(\frac{2n(n-1)\pi}{2n}\right) = \cos(n\pi - \pi) + i\,\mathrm{sen}(n\pi - \pi) = \\ &= [\cos(n\pi)\cos(\pi) + \mathrm{sen}(n\pi)\,\mathrm{sen}(\pi)] + i[\mathrm{sen}(n\pi)\cos(\pi) - \mathrm{sen}(\pi)\cos(n\pi)] = \\ &= -\cos(n\pi).\end{aligned}$$

Assim, quando n é par temos que $\xi_n^{\frac{n(n-1)}{2}} = -1$ e quando n é ímpar temos que $\xi_n^{\frac{n(n-1)}{2}} = 1$. Logo,

$$\mathcal{N}(x) = (-1)^{n+1} d\mathcal{N}(a).$$

Como $x \in \mathbb{Z}$, segue que $\mathcal{N}(x) = x^n$. Por outro lado, a norma de um elemento inteiro algébrico é um inteiro (Observação 2.3.5). Assim, como $a \in \mathcal{O}_\mathbb{K}$, segue que $\mathcal{N}(a) \in \mathbb{Z}$. Logo,

$$\mathcal{N}(x) = x^n = (-1)^{n+1} d\mathcal{N}(a),$$

ou seja, $d \mid x^n$. Como d é um inteiro livre de quadrados, segue que $d \mid x$. Logo, $x \in d\mathbb{Z}$, e assim, $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} \subseteq d\mathbb{Z}$. Agora, vamos mostrar que $d\mathbb{Z} \subseteq \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$. Se $x \in d\mathbb{Z}$, então existe $a \in \mathbb{Z}$ tal que $x = da$. Mas,

$$x = da = \theta^n a = \theta(\theta^{n-1}a).$$

Assim, $a \in \mathcal{O}_\mathbb{K}$, pois $a \in \mathbb{Z} \subseteq \mathcal{O}_\mathbb{K}$. Como $\theta \in \mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2), segue que $\theta^{n-1}a \in \mathcal{O}_\mathbb{K}$. Consequentemente, $x = \theta(\theta^{n-1}a) \in \theta\mathcal{O}_\mathbb{K}$. Assim, $d\mathbb{Z} \subseteq \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$. Portanto, $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = d\mathbb{Z}$. □

Proposição 2.6.7. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[n]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\mathcal{O}_\mathbb{K}$ o seu anel dos inteiros algébricos. Se $x \in \theta\mathcal{O}_\mathbb{K}$, então $\mathcal{T}r(x) \in d\mathbb{Z}$.*

Demonstração. Se $x \in \theta\mathcal{O}_\mathbb{K}$, então $x = \theta\alpha$, com $\alpha \in \mathcal{O}_\mathbb{K}$. O elemento $x = \theta\alpha$ é um elemento inteiro algébrico, pois θ e α também são inteiros algébricos no anel $\mathcal{O}_\mathbb{K}$ (Corolário 2.2.2). Assim,

$$\begin{aligned}\mathcal{T}r(x) &= \mathcal{T}r(\theta\alpha) = \sigma_1(\theta\alpha) + \sigma_2(\theta\alpha) + \cdots + \sigma_n(\theta\alpha) = \\ &= \theta[\sigma_1(\alpha) + \xi_n\sigma_2(\alpha) + \cdots + \xi_n^{n-1}\sigma_n(\alpha)] = \theta w,\end{aligned}$$

com $w = \sigma_1(\alpha) + \xi_n\sigma_2(\alpha) + \cdots + \xi_n^{n-1}\sigma_n(\alpha)$ e vamos provar que $w \in \mathcal{O}_\mathbb{K}$. Para isso, w precisa ser um inteiro algébrico e pertencer a $\mathbb{K}$. Assim,

1. w é um inteiro algébrico em $\mathbb{C}$. Como $\alpha \in \mathcal{O}_\mathbb{K}$, segue que existe $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k \in \mathbb{Z}[x]$ que é o polinômio minimal de α. Assim,

   $$\sigma_i(f(\alpha)) = \sigma_i(a_0+a_1x+\cdots+a_{k-1}x^{k-1}+x^k) = a_0+a_1\sigma_i(\alpha)+\cdots+a_{k-1}\sigma_i(\alpha)^{k-1}+\sigma_i(\alpha)^k,$$

   ou seja, como $\sigma_i(f(\alpha)) = 0$, segue que $\sigma_i(\alpha)$ é uma raiz de $f(x)$. Mas, $\sigma_i(\alpha) \in \mathcal{O}_\mathbb{C}$, para todo $i = 1, 2, \ldots, n$. Outro fato é que $\xi_n, \xi_n^2, \ldots, \xi_n^{n-1} \in \mathcal{O}_\mathbb{C}$, pois são raízes primitivas da unidade. Analisando os termos de $w = \sigma_1(\alpha) + \xi_n\sigma_2(\alpha) + \cdots + \xi_n^{n-1}\sigma_n(\alpha)$, identificamos que w é formado por somas e produtos de elementos inteiros algébricos e como $\mathcal{O}_\mathbb{C}$ é um anel (Corolário 2.2.2), segue que $w \in \mathcal{O}_\mathbb{C}$.

2. w é um elemento de $\mathbb{K}$. Vimos que x é um inteiro algébrico, e consequentemente, $\mathcal{T}r(x) \in \mathbb{Z}$ (Observação 2.3.5). Assim, $\mathcal{T}r(x) = \theta w = a$, com $a \in \mathbb{Z}$. Agora, $w = \dfrac{a}{\theta} \in \mathbb{K}$.

Pelos itens 1) e 2) concluímos que $w \in \mathcal{O}_\mathbb{K}$. Assim, $\mathcal{T}r(x) = \theta w \in \theta\mathcal{O}_\mathbb{K}$. Finalmente, $\mathcal{T}r(x) \in \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$. Pela Proposição 2.6.6, como $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = d\mathbb{Z}$, segue que $\mathcal{T}(x) \in d\mathbb{Z}$. □

Proposição 2.6.8. *Se $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números, onde $\theta = \sqrt[n]{d}$ com $d \in \mathbb{Z}$ livre de quadrados, então*

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, \ldots, n-1, \\ nd^s, \text{ se } k = ns, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > n \text{ e } k \not\equiv 0 (mod\ n). \end{cases} \tag{2.23}$$

Demonstração. Dividimos essa prova em três casos:

1. Calculamos $\mathcal{T}r(\theta^k)$, com $k = 1, 2, \ldots, n-1$. Para isso, seja $p(x) = x^n - d$ o polinômio minimal de $\theta = \sqrt[n]{d}$. Assim, pelas Proposições 2.6.4 e 2.6.5, segue que as raízes de $p(x)$ são $\theta, \theta\xi_n, \theta\xi_n^2, \ldots, \theta\xi_n^{n-1}$. Agora, com o auxílio dos monomorfismos σ_i, com $i = 1, 2, \ldots, n$, segue que

$$\begin{aligned}\mathcal{T}r(\theta^k) =& \sigma_1(\theta^k) + \sigma_2(\theta^k) + \sigma_3(\theta^k) + \cdots + \sigma_n(\theta^k) = \\ &= (\sigma_1(\theta))^k + (\sigma_2(\theta))^k + (\sigma_3(\theta))^k + \cdots + (\sigma_n(\theta))^k = \\ &= \theta^k + \theta^k\xi_n^k + \theta^k\xi_n^{2k} + \cdots + \theta^k\xi_n^{(n-1)k} = \\ &= \theta^k(1 + \xi_n^k + \xi_n^{2k} + \cdots + \xi_n^{(n-1)k}).\end{aligned}$$

   Como $1 + \xi_n^k + \xi_n^{2k} + \cdots + \xi_n^{(n-1)k}$ é uma progressão geométrica de n termos, cujo o primeiro termo é 1 e a razão é ξ_n^k, segue que sua soma é calculada por

$$1 + \xi_n^k + \xi_n^{2k} + \cdots + \xi_n^{(n-1)k} = \frac{1((\xi_n^k)^n - 1)}{\xi_n^k - 1} = \frac{1((\xi_n^n)^k - 1)}{\xi_n^k - 1} = \frac{1^k - 1}{\xi_n^k - 1} = \frac{1 - 1}{\xi_n^k - 1} = 0.$$

   Portanto,

$$\mathcal{T}r(\theta^k) = 0, \text{ com } k = 1, 2, \ldots, n-1.$$

2. Calculamos $\mathcal{T}r(\theta^k)$, sendo k um múltiplo de n, ou seja, $k = ns$, para $s \in \mathbb{N}$. Como $\theta^n = d \in \mathbb{Z}$ e usando as propriedades de traço, segue que

$$\mathcal{T}r(\theta^k) = \mathcal{T}r(\theta^{ns}) = \mathcal{T}r((\theta^n)^s) = \mathcal{T}r(d^s) = nd^s.$$

3. Calculamos $\mathcal{T}r(\theta^k)$ sendo $k > n$ e k não múltiplo de n, ou seja, $k \not\equiv 0(mod\ n)$. Como $k \not\equiv 0(mod\ n)$, segue que $k = ns + r$, com $s \in \mathbb{Z}$ e $r \in \{0, 1, 2, \ldots, n-1\}$. Pelo item 1, segue que $\mathcal{T}r(\theta^r) = 0$. Usando as propriedades de traço e recordando que $\theta^n = d \in \mathbb{Z}$, segue que

$$\mathcal{T}r(\theta^k) = \mathcal{T}r(\theta^{ns+r}) = \mathcal{T}r((\theta^n)^s\theta^r) = \mathcal{T}r(d^s\theta^r) = d^s\mathcal{T}r(\theta^r) = d^s \cdot 0 = 0.$$

Portanto, pelos itens 1, 2 e 3 segue o resultado. □

Proposição 2.6.9. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[n]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \in \mathbb{K}$, com $a_0, a_1, a_2 \ldots, a_{n-1} \in \mathbb{Q}$. Se α é um inteiro algébrico, então $na_0, na_1, na_2 \ldots, na_{n-1} \in \mathbb{Z}$.*

Demonstração. Se $\alpha \in \mathbb{K}$ é um inteiro algébrico, então θ também é um inteiro algébrico. Como $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2), segue que $\theta^i\alpha$ é um inteiro algébrico, para $i = 1, 2, \ldots, n-1$. Por outro lado, o traço de um elemento inteiro algébrico é um número inteiro (Observação 2.3.5). Agora, da Proposição 2.6.8, segue que $\mathcal{T}r(\theta^x) = 0$, para $x = 0, 1, 2, \ldots, n-1$. Dessas observações chegamos em

$$\mathcal{T}r(\alpha) = \mathcal{T}r(a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}) = \mathcal{T}r(a_0) = na_0 \in \mathbb{Z}.$$

Como $\theta^i\alpha \in \theta\mathcal{O}_\mathbb{K}$ para $i = 1, 2, \ldots, n-1$ e usando as Proposições 2.6.7 e 2.6.8, segue que

$$\begin{aligned}&\mathcal{T}r(\theta\alpha) = \mathcal{T}r(a_0\theta + a_1\theta^2 + \cdots + a_{n-2}\theta^{n-1} + a_{n-1}d) = \mathcal{T}r(a_{n-1}d) = na_{n-1}d \in d\mathbb{Z}, \\ &\mathcal{T}r(\theta^2\alpha) = \mathcal{T}r(a_0\theta^2 + a_1\theta^3 + \cdots + a_{n-2}d + a_{n-1}d\theta) = \mathcal{T}r(a_{n-2}d) = na_{n-2}d \in d\mathbb{Z}, \\ &\vdots \\ &\mathcal{T}r(\theta^{n-1}\alpha) = \mathcal{T}r(a_0\theta^{n-1} + a_1d + \cdots + a_{n-2}d\theta^{n-3} + a_{n-1}d\theta^{n-2}) = \mathcal{T}r(a_1d) = na_1d \in d\mathbb{Z}.\end{aligned}$$

Como $na_id \in d\mathbb{Z}$ para $i = 1, 2, \ldots, n-1$, segue que $na_i \in \mathbb{Z}$ para $i = 1, 2, \ldots, n-1$. Portanto, $na_0, na_1, na_2, \ldots, na_{n-1}$ são números inteiros. □

3 Extensões Quadráticas

Os corpos quadráticos $\mathbb{K}$ são corpos de números providos de uma extensão quadrática, ou seja, $[\mathbb{K} : \mathbb{Q}] = 2$. Neste capítulo, apresentamos o estudo completo dos corpos quadráticos, envolvendo o seu elemento primitivo, anel dos inteiros, norma, traço e discriminante. Neste caso, para as extensões quadráticas cujo o polinômio minimal é $p(x) = x^2 - d$, com d um inteiro livre de quadrados, embora a base integral seja conhecida, apresentamos nossa versão da demonstração. Este capítulo foi inspirado pelas referências [3], [7], [8] e [9].

Definição 3.0.1. *Seja $\mathbb{K}$ um corpo de números, com o grau da extensão $[\mathbb{K} : \mathbb{Q}] = 2$.*

1. *O corpo de números $\mathbb{K}$ é chamado de **corpo quadrático**.*
2. *A extensão de corpos $\mathbb{Q} \subseteq \mathbb{K}$ é chamada de **extensão quadrática**.*
3. *O polinômio $p(x) \in \mathbb{Q}[x]$, cujo grau é $\partial(p) = 2$, é chamado de **quádrica**.*

3.1 Corpos quadráticos

Para alguns graus de extensões de corpos de números não é tão simples encontrar o elemento primitivo. Mas diferentemente destes, os corpos quadráticos possui essa característica interessante, assim nesta seção, apresentamos os elementos primitivos dos corpos quadráticos. Como a extensão tem $[\mathbb{K} : \mathbb{Q}] = 2$ é finita e também separável, pelo Teorema do Elemento Primitivo, segue que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$. Essa é nossa motivação para descobrir o elemento primitivo dos corpos quadráticos.

Definição 3.1.1. *Um inteiro d é chamado **livre de quadrados**, se não é múltiplo de nenhum quadrado perfeito. Ou seja, na sua fatoração em primos, as potências não aparecem aos pares.*

Exemplo 3.1.1. *Neste exemplo, apresentamos alguns casos para a definição de inteiros livre de quadrados.*

1. *Seja $d = 6$. Sua fatoração em números primos é $6 = 2 \times 3$, e assim, 6 é um número inteiro livre de quadrados.*
2. *Seja $d = 45$. Sua fatoração em números primos $45 = 3^2 \times 5$, e assim, 45 não é livre de quadrados, pois na sua fatoração aparece 3^2 um primo com potência par.*

Proposição 3.1.1. *Todo corpo quadrático $\mathbb{K}$ é da forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ livre de quadrados.*

Demonstração. Seja α o elemento primitivo de $\mathbb{K}$, ou seja, $\mathbb{K} = \mathbb{Q}(\alpha)$. Outro fato importante, é que a extensão em questão é finita e consequentemente algébrica. Logo, podemos considerar $p(x) = x^2 + ax + b$ o polinômio minimal de α com coeficientes em $\mathbb{Q}$. Usando a fórmula de Báskara para resolver a equação de segundo grau $x^2 + ax + b$, segue que

$$\alpha = \frac{-a \pm \sqrt{\Delta}}{2},$$

com $\Delta = a^2 - 4b$ e $\Delta \neq 0$. Assim, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$. Como $\Delta \in \mathbb{Q}$, segue que

$$\Delta = \frac{u}{v} = \frac{uv}{v^2},$$

com $u, v \in \mathbb{Z}$. Logo,

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}\left(\sqrt{\frac{uv}{v^2}}\right) = \mathbb{Q}\left(\frac{\sqrt{uv}}{|v|}\right) = \mathbb{Q}(\sqrt{uv}).$$

Suponhamos que $uv = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, com p_i primos e β_i as potências dos respectivos primos, para $i = 1, 2, \ldots, s$. Essas potências podem aparecer aos pares e assim podemos "tirar" alguns primos da raiz, mantendo apenas os primos cujos as potências sejam 1. Formalmente, consideramos $\alpha_i = 2\beta_i + r_i$, com r_i sendo 0 ou 1. Assim,

$$\begin{aligned}\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{uv}) &= \mathbb{Q}\left(\sqrt{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}}\right) = \mathbb{Q}\left(\sqrt{p_1^{2\beta_1 + r_1} p_2^{2\beta_2 + r_2} \cdots p_s^{2\beta_s + r_s}}\right) \\ &= \mathbb{Q}\left(p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s} \sqrt{p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}}\right) = \mathbb{Q}\left(\sqrt{p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}}\right).\end{aligned}$$

O número $d = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ é um número inteiro, pois as potências r_i descritas são 0 ou 1 e os $p_i's$ são primos, para todo i. Portanto, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados. □

Pela Proposição 3.1.1, segue que os corpos quadráticos são escritos da forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, por este motivo o polinômio minimal do elemento primitivo das extensões quadráticas vão ser sempre da forma $p(x) = x^2 - d$.

3.2 A quádrica $p(x) = x^2 + ax + b$

Nesta seção, consideramos $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 2, onde a quádrica $p(x) = x^2 + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, é o polinômio minimal do elemento primitivo θ. O objetivo é descobrir o anel dos inteiros desses corpos de números através do discriminante.

Pela Teoria de Corpos, segue que o conjunto $\{1, \theta\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_{\mathbb{K}}$. E mais, pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta) = (-1)^{\frac{2(2-1)}{2}}[2^2 b^{2-1} + (-1)^{2+1}(2-1)^{2-1} a^2] = a^2 - 4b.$$

Assim $\mathcal{D}(1, \theta) = a^2 - 4b$. Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta | a_0, a_1 \in \mathbb{Z}\}.$$

Exemplo 3.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 2 tal que $p(x) = x^2 - x - 1$ é o polinômio minimal do elemento primitivo θ. Como*

$$\mathcal{D}(1, \theta) = (-1)^2 - 4(-1) = 5 \text{ e}$$

$\mathcal{D}(1, \theta) = 5$ é livre de quadrados, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$.

3.3 A quádrica $p(x) = x^2 - d$, com d livre de quadrados

Considerando a Proposição 3.1.1, os corpos quadráticos podem ser escritos com $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados, cujo o polinômio minimal de $\sqrt{d}$ é $p(x) = x^2 - d$. Logo, vamos buscar o anel dos inteiros algébricos destes corpos (sobre $\mathbb{Z}$). Por questão de notação, consideramos $\theta = \sqrt{d}$.

O polinômio minimal de θ é $p(x) = x^2 - d$, e assim, suas raízes são θ e $-\theta$. Pelo Teorema 2.3.2, podemos considerar σ_1 e σ_2 os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$ e $\sigma_2(\theta) = -\theta$. Além disso, pela Teoria de Corpos, segue que o conjunto $\{1, \theta\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta$, onde $a_0, a_1 \in \mathbb{Q}$.

A próxima proposição sobre o polinômio característico será crucial para a representação do anel dos inteiro dos corpos quadráticos.

Proposição 3.3.1. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt{d}$ com $d \in \mathbb{Z}$ livre de quadrados, e $\alpha = a_0 + a_1\theta \in \mathbb{K}$, com $a_0, a_1 \in \mathbb{Q}$. O polinômio característico de α é dado por*

$$f_\alpha(x) = x^2 - (2a_0)x + (a_0^2 - a_1^2 d). \tag{3.1}$$

Demonstração. Consideramos $\alpha_i = \sigma_i(\alpha)$, com $i = 1, 2$. Assim,

$$\begin{aligned} \alpha_1 &= a_0 + a_1\theta, \\ \alpha_2 &= a_0 - a_1\theta. \end{aligned}$$

Pela Proposição 2.3.4, segue que o polinômio característico de α é dado por

$$\begin{aligned} f_\alpha(x) &= (x - \alpha_1)(x - \alpha_2) = \\ &= x^2 - x(\alpha_1 + \alpha_2) + \alpha_1\alpha_2. \end{aligned}$$

Assim, vamos calcular os coeficientes do polinômio característico

$$\begin{aligned} \alpha_1 + \alpha_2 &= (a_0 + a_1\theta) + (a_0 - a_1\theta) = 2a_0. \\ \alpha_1\alpha_2 &= (a_0 + a_1\theta)(a_0 - a_1\theta) = a_0^2 - a_1^2 d. \end{aligned}$$

Portanto, $f_\alpha(x) = x^2 - (2a_0)x + (a_0^2 - a_1^2 d)$. □

Exemplo 3.3.1. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt{7}$ e $\alpha = 1 + 2\sqrt{7} \in \mathbb{K}$. Pela Proposição 3.3.1, o polinômio característico de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 2$ e $d = 7$ e substituição direta, logo*

$$f_\alpha(x) = x^2 - (2 \times 1)x + (1^2 - 2^2 \times 7) = x^2 - 2x - 27.$$

Com este resultado, podemos enunciar e demonstrar o teorema que caracterizará o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$.

3.3.1 O anel dos inteiros de $\mathbb{Q}(\sqrt{d})$

Embora seja um resultado conhecido na literatura, nós apresentamos no teorema a seguir nossa versão da demonstração para a base integral destas extensões.

Teorema 3.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo quadrático, onde $\theta = \sqrt{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta, \text{ se } d \not\equiv 1 (mod\ 4) \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\theta}{2}\right), \text{ se } d \equiv 1 (mod\ 4). \end{cases}$$

Demonstração. Suponhamos que $\alpha \in \mathbb{K}$ é um inteiro algébrico e vamos explorar quais são as formas que α pode assumir, lembrando que $\alpha = a_0 + a_1\theta$, com $a_0, a_1 \in \mathbb{Q}$. Da Proposição 2.6.9, se α é um inteiro algébrico, então $2a_0, 2a_1 \in \mathbb{Z}$. Vamos supor $2a_i = p_i$, com $p_i \in \mathbb{Z}$ para todo $i = 0, 1$. Assim,

$$a_i = \frac{p_i}{2}, \text{ para todo } i = 0, 1.$$

Além do mais, p_i pode ser escrito da seguinte forma

$$p_i = 2q_i + r_i,$$

com $q_i, r_i \in \mathbb{Z}$ e $r_i \in \{0, 1\}$, para $i = 0, 1$. Reescrevendo α, segue que

$$\alpha = a_0 + a_1\theta = \frac{p_0}{2} + \frac{p_1}{2}\theta = \frac{2q_0 + r_0}{2} + \frac{2q_1 + r_1}{2}\theta = q_0 + q_1\theta + \frac{r_0}{2} + \frac{r_1}{2}\theta.$$

Logo,

$$\alpha = q_0 + q_1\theta + \frac{r_0}{2} + \frac{r_1}{2}\theta. \tag{3.2}$$

Agora, como $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2) e $q = q_0 + q_1\theta \in \mathcal{O}_\mathbb{K}$, segue que

$$\alpha = q_0 + q_1\theta + \frac{r_0}{2} + \frac{r_1}{2}\theta \in \mathcal{O}_\mathbb{K} \Leftrightarrow r = \frac{r_0}{2} + \frac{r_1}{2}\theta \in \mathcal{O}_\mathbb{K}.$$

Assim, α é um inteiro algébrico se, e somente se, r é um inteiro algébrico. Consequentemente,

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow r \in \mathcal{O}_\mathbb{K}. \tag{3.3}$$

Novamente por esses dois resultados (Proposição 3.3.1 e Proposição 2.3.3), segue que

$$r \in \mathcal{O}_\mathbb{K} \Leftrightarrow \begin{cases} 2\left(\frac{r_0}{2}\right) \in \mathbb{Z} \text{ e} \\ \left(\frac{r_0}{2}\right)^2 - d\left(\frac{r_1}{2}\right)^2 \in \mathbb{Z}. \end{cases} \tag{3.4}$$

Das implicações na Expressão (3.3) e na Expressão (3.4), segue que

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow \frac{(r_0)^2 - (r_1)^2 d}{4} \in \mathbb{Z}. \tag{3.5}$$

Logo,

$$\omega = \frac{(r_0)^2 - (r_1)^2 d}{4}. \tag{3.6}$$

Na Tabela (3.1), listamos todas as possibilidades para d de acordo com os parâmetros $r_0, r_1 \in \{0, 1\}$. Em seguida, faremos a análise das linhas dessa tabela que possuem solução, ou seja, que existe d tal que $\omega \in \mathbb{Z}$ (vide Equação (3.6)), para consequentemente encontrar o anel dos inteiros deste caso.

Tabela 3.1: $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, d livre de quadrados - todos os casos para análise de $\mathcal{O}_{\mathbb{K}}$.

Linhas	r_0	r_1	$\omega = \frac{(r_0)^2 - (r_1)^2 d}{4}$	$d \equiv (?)(mod\ 4)$
Linha 1	0	0	0	$\forall d$
Linha 2	0	1	$-\frac{d}{4}$	$\nexists d$
Linha 3	1	0	$\frac{1}{4}$	$\nexists d$
Linha 4	1	1	$\frac{1-d}{4}$	$d \equiv 1(mod\ 4)$

Fonte: Elaborada pela autora.

Na tabela (3.1), a célula "$\forall d$" não inclui $d \equiv 0(mod\ 4)$, uma vez que d é livre de quadrados. Para as linhas que possuem solução, faremos a análise da possível base integral de acordo com as congruências de d módulo 4. Recordamos da Equação (3.2) que será importante para essa análise, ou seja,

$$\alpha = q_0 + q_1\theta + \left(\frac{r_0 + r_1\theta}{2}\right).$$

1. Quando $d \not\equiv 1(mod\ 4)$, faremos a investigação da linha que identifica esse caso. Para a Linha 1, os restos são $r_0 = 0$ e $r_1 = 0$. Assim, substituindo os restos na Equação (3.2), segue que
$$\alpha = q_0 + q_1\theta.$$
Como $q_0, q_1 \in \mathbb{Z}$, segue que $\alpha \in \mathbb{Z} + \mathbb{Z}\theta$. Desse modo, para $d \not\equiv 1(mod\ 4)$ o anel dos inteiros é $\mathbb{Z} + \mathbb{Z}\theta$.

2. Quando $d \equiv 1(mod\ 4)$, faremos a investigação da linha que identifica esse caso. Para a Linha 4, os restos são $r_0 = 1$ e $r_1 = 1$. Assim, substituindo os restos na Equação (3.2), segue que
$$\alpha = q_0 + q_1\theta + \left(\frac{1+\theta}{2}\right) = \left(q_0 + \frac{1}{2}\right) + \left(q_1 + \frac{1}{2}\right)\theta.$$
Confirmaremos que para este caso a base integral é $\left\{1, \frac{1+\theta}{2}\right\}$. Assim, suponhamos que para algum z_0 e z_1 podemos escrever
$$\alpha = z_0 + z_1\left(\frac{1+\theta}{2}\right) = \left(z_0 + \frac{z_1}{2}\right) + \left(\frac{z_1}{2}\right)\theta.$$
Assim, comparando as formas que α pode ser escrito, montamos o seguinte sistema:
$$\begin{cases} z_0 + \frac{z_1}{2} = q_0 + \frac{1}{2} \\ \frac{z_1}{2} = q_1 + \frac{1}{2}. \end{cases}$$
Resolvendo o sistema, segue que $z_0 = q_0 - q_1$ e $z_1 = 2q_1 + 1$. Como $q_0, q_1 \in \mathbb{Z}$, segue que $z_0, z_1 \in \mathbb{Z}$, e assim, $\alpha \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\theta}{2}\right)$. Desse modo, para $d \equiv 1(mod\ 4)$ o anel dos inteiros é $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\theta}{2}\right)$.

Portanto, concluímos que o anel dos inteiros algébricos é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta, \text{ se } d \not\equiv 1(mod\ 4) \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\theta}{2}\right), \text{ se } d \equiv 1(mod\ 4), \end{cases}$$

o que prova o teorema. □

Exemplo 3.3.2. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt{7}$. Como $d = 7$ e $7 \equiv 3(mod\ 4)$, então pelo Teorema 3.3.1 o anel dos inteiros algébricos desse caso é*

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\theta.$$

3.3.2 Norma, traço e discriminante em $\mathbb{Q}(\sqrt{d})$

Nesta seção, apresentamos a norma, o traço e o discriminante em $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados.

Proposição 3.3.2. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta \in \mathbb{K}$, com $a_0, a_1 \in \mathbb{Q}$. O traço de α é calculado por*

$$\mathcal{T}r(\alpha) = 2a_0.$$

Demonstração. Pela Proposição 2.3.4, calculamos o traço de α com os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$ e $\sigma_2(\theta) = -\theta$. Assim,

$$\mathcal{T}r(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (a_0 + a_1\theta) + (a_0 - a_1\theta) = 2a_0.$$

Portanto, $\mathcal{T}r(\alpha) = 2a_0$. □

Proposição 3.3.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta \in \mathbb{K}$, com $a_0, a_1 \in \mathbb{Q}$. A norma de α é calculada por*

$$\mathcal{N}(\alpha) = a_0^2 - a_1^2 d.$$

Demonstração. Pela Proposição 2.3.4, calculamos a norma de α com os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$ e $\sigma_2(\theta) = -\theta$. Assim,

$$\mathcal{N}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (a_0 + a_1\theta)(a_0 - a_1\theta) = a_0^2 - a_1^2 d.$$

Portanto, $\mathcal{N}(\alpha) = a_0^2 - a_1^2 d$. □

Exemplo 3.3.3. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt{7}$ e $\alpha = 1 + 2\sqrt{7} \in \mathbb{K}$.*

a) Pela Proposição 3.3.2, segue que o traço de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 2$ e $d = 7$ e substituição direta. Logo, $\mathcal{T}r(\alpha) = 2 \times (1) = 2$.

b) Pela Proposição 3.3.3, segue que a norma de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 2$ e $d = 7$ e substituição direta. Logo, $\mathcal{N}(\alpha) = (1)^2 - (2)^2 \times (7) = -27$.

Proposição 3.3.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O discriminante do anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por*

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 4d, \text{ se } d \not\equiv 1(mod\ 4) \\ d, \text{ se } d \equiv 1(mod\ 4). \end{cases}$$

Demonstração. Pelo Teorema 3.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta, \text{ se } d \not\equiv 1(mod\ 4) \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\theta}{2}\right), \text{ se } d \equiv 1(mod\ 4). \end{cases}$$

Assim, a base integral (base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$) admite as possibilidades:

1. Se $d \not\equiv 1(mod\ 4)$, então a base integral é $\{1, \theta\}$.
2. Se $d \equiv 1(mod\ 4)$, então a base é integral $\left\{1, \dfrac{1+\theta}{2}\right\}$.

Pela Proposição 2.6.8, segue que

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, \\ 2d^s, \text{ se } k = 2s, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > 2 \text{ e } k \not\equiv 0(mod\ 2). \end{cases} \tag{3.7}$$

Logo, $\mathcal{T}r(1) = 2$, $\mathcal{T}r(\theta) = 0$ e $\mathcal{T}r(d) = 2d$. Agora, analisaremos o discriminante para cada possibilidade da base integral.

1. Se $d \not\equiv 1(mod\ 4)$, então a base é $\{1, \theta\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (3.7), segue que

$$\mathcal{D}(1, \theta) = \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) \\ \mathcal{T}r(\theta) & \mathcal{T}r(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

2. Se $d \equiv 1(mod\ 4)$, então a base é $\left\{1, \dfrac{1+\theta}{2}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (3.7), segue que

$$\mathcal{D}\left(1, \frac{1+\theta}{2}\right) = \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r\left(\frac{1+\theta}{2}\right) \\ \mathcal{T}r\left(\frac{1+\theta}{2}\right) & \mathcal{T}r\left(\frac{1+2\theta+\theta^2}{4}\right) \end{pmatrix} = \det \begin{pmatrix} \mathcal{T}r(1) & \frac{\mathcal{T}r(1)}{2} \\ \frac{\mathcal{T}r(1)}{2} & \frac{\mathcal{T}r(1+d)}{4} \end{pmatrix},$$

ou seja,

$$\mathcal{D}\left(1, \frac{1+\theta}{2}\right) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Logo, da análise dos itens (1) e (2), segue que

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 4d, \text{ se } d \not\equiv 1(mod\ 4) \\ d, \text{ se } d \equiv 1(mod\ 4), \end{cases}$$

o que prova a proposição. □

Exemplo 3.3.4. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt{7}$. Como $d = 7$ e $7 \equiv 3(mod\ 4)$, pela Proposição 3.3.4, segue que o discriminante é dado por $\mathcal{D}(\mathbb{K}) = 4 \times 7 = 28$.*

Observação 3.3.1. *Para $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt{d}$, com $d \in \mathbb{Z}$ livre de quadrados, podemos calcular o discriminante da base potente $\{1, \theta\}$ através do polinômio minimal $p(x) = x^2 - d$, e assim, utilizando o Corolário 2.5.4, segue*

$$\mathcal{D}(1, \theta) = (-1)^{\frac{2^2+2+2}{2}}[2^2 d^{2-1}] = 4d.$$

4 Extensões Cúbicas

Os corpos cúbicos $\mathbb{K}$ são corpos de números providos de uma extensão cúbica, ou seja, $[\mathbb{K} : \mathbb{Q}] = 3$. Neste capítulo, exploramos alguns corpos cúbicos, pois diferentemente do capítulo anterior onde estudamos os corpos quadráticos, não é tão simples identificar o elemento primitivo dos corpos cúbicos, uma vez que o caminho para encontrar as soluções de uma equação de terceiro grau é árduo. Dessa forma, a complexidade do caso geral nos leva a focar em casos particulares. Por isso, chamamos a atenção para os corpos cúbicos nos quais o elemento primitivo tem como polinômio minimal $p(x) = x^3 - d$, com d um inteiro livre de quadrados. O nosso objetivo é descobrir o anel dos inteiros algébricos desses corpos cúbicos, neste caso, a base integral que encontramos é sutilmente diferente da apresentada na referência [7]. Como aplicação direta, apresentamos, também, a norma e traço de um elemento desses corpos cúbicos e o discriminante da base integral. Este capítulo foi inspirado pelas referências [7], [8] e [9].

4.1 Corpos cúbicos

Nesta seção, apresentamos as extensões cúbicas e alguns conceitos básicos e propriedades.

Definição 4.1.1. *Seja $\mathbb{K}$ um corpo de números, com o grau da extensão $[\mathbb{K} : \mathbb{Q}] = 3$.*

1. *O corpo de números $\mathbb{K}$ é chamado de **corpo cúbico**.*
2. *A extensão de corpos $\mathbb{Q} \subseteq \mathbb{K}$ é chamada de **extensão cúbica**.*
3. *O polinômio $p(x) \in \mathbb{Q}[x]$, cujo grau é $\partial(p) = 3$, é chamado de **cúbica**.*

Consideramos $\mathbb{K}$ um corpo cúbico, ou seja, o grau da extensão é $[\mathbb{K} : \mathbb{Q}] = 3$. Pelo Teorema do Elemento Primitivo, segue que existe $\theta \in \mathbb{C}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$, ou seja, θ é o elemento primitivo de $\mathbb{K}$. Seja $p(y) = y^3 + a_2y^2 + a_1y + a_0$ o polinômio minimal de θ sobre $\mathbb{Q}$. A ideia é melhorar $p(y)$ reduzindo algum coeficiente, por isso faremos a seguinte mudança de variável $y = x - l$, e assim,

$$\begin{aligned} p(x-l) &= (x-l)^3 + a_2(x-l)^2 + a_1(x-l) + a_0 = \\ &= x^3 - 3lx^2 + 3l^2x - l^3 + a_2x^2 - 2a_2lx + a_2l^2 + a_1x - a_1l + a_0 = \\ &= x^3 + x^2(-3l + a_2) + x(3l^2 - 2a_2l + a_1) + (-l^3 + a_2l^2 - a_1l + a_0). \end{aligned}$$

Agora, para cancelar o coeficiente $-3l + a_2$, devemos tomar $l = \dfrac{a_2}{3} \in \mathbb{Q}$. Fazendo as substituições, segue que os coeficientes restantes são

$$b_1 = -\frac{(a_2)^2}{3} + a_1 \quad \text{e} \quad b_0 = \frac{2(a_2)^3}{27} - \frac{a_1a_2}{3} + a_0,$$

com $b_0, b_1 \in \mathbb{Q}$. Portanto, sem perda de generalidade, consideramos $p(x) = x^3 + b_1x + b_0 \in \mathbb{Q}[x]$. Um fato interessante é que $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\theta - l)$, desde que $l \in \mathbb{Q}$, e assim, podemos considerar $p(x) = x^3 + b_1x + b_0$.

4.2 A cúbica $p(x) = x^3 + ax + b$

Seja $\mathbb{K}$ um corpo cúbico e $\theta \in \mathbb{C}$ o seu elemento primitivo, e assim, $\mathbb{K} = \mathbb{Q}(\theta)$. Consideramos θ um inteiro algébrico e pelas considerações anteriores, segue que o seu polinômio minimal pode ser escrito da forma $p(x) = x^3 + ax + b$, com $a, b \in \mathbb{Z}$. Pelo Teorema 2.3.2, podemos considerar σ_i os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \beta$ e $\sigma_3(\theta) = \gamma$, onde θ, β e γ são as raízes de $p(x)$. Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim, podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta + a_2\theta^2$, para $a_0, a_1, a_2 \in \mathbb{Q}$ quaisquer. Nesta seção, apresentamos resultados nossos, não conhecidos na literatura.

A seguir, apresentamos alguns resultados preliminares para o polinômio $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$ e suas raízes θ, β e γ.

Lema 4.2.1. *Sejam o polinômio $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$ e suas raízes θ, β e γ.*

1. $\theta^2 + \beta^2 + \gamma^2 = -2a$.
2. $\theta^2\beta^2 + \theta^2\gamma^2 + \beta^2\gamma^2 = a^2$.
3. $\theta^2\beta + \theta^2\gamma + \theta\beta^2 + \beta^2\gamma + \theta\gamma^2 + \beta\gamma^2 = 3b$.

Demonstração. Sejam θ, β e γ as raízes de $p(x)$. Usando as relações de Girard para o polinômio $p(x) = x^3 + ax + b$, segue que

$$\begin{aligned} \theta + \beta + \gamma &= 0 \ (1) \\ \theta\beta + \theta\gamma + \beta\gamma &= a \ (2) \\ \theta\beta\gamma &= -b \ (3). \end{aligned}$$

Vamos mostrar cada item separadamente.

1. Primeiro, faremos a seguinte manipulação.

$$\begin{aligned} (\theta + \beta + \gamma)^2 &= \theta^2 + \theta\beta + \theta\gamma + \theta\beta + \beta^2 + \beta\gamma + \theta\gamma + \beta\gamma + \gamma^2 = \\ &= (\theta^2 + \beta^2 + \gamma^2) + 2(\theta\beta + \theta\gamma + \beta\gamma). \end{aligned}$$

   Assim, segue o resultado usando as Relações de Girard

$$\theta^2 + \beta^2 + \gamma^2 = (\theta + \beta + \gamma)^2 - 2(\theta\beta + \theta\gamma + \beta\gamma) \overset{(1) \text{ e } (2)}{=} 0^2 - 2a = -2a.$$

2. Agora,

$$\begin{aligned} &(\theta\beta + \theta\gamma + \beta\gamma)^2 = \theta^2\beta^2 + \theta^2\beta\gamma + \theta\beta^2\gamma + \theta^2\beta\gamma + \theta^2\gamma^2 + \theta\beta\gamma^2 + \theta\beta^2\gamma + \theta\beta\gamma^2 + \beta^2\gamma^2 = \\ &= (\theta^2\beta^2 + \theta^2\gamma^2 + \beta^2\gamma^2) + \theta\beta\gamma(\theta + \beta + \gamma). \end{aligned}$$

   Logo, usando as Relações de Girard, segue que

$$\theta^2\beta^2 + \theta^2\gamma^2 + \beta^2\gamma^2 = (\theta\beta + \theta\gamma + \beta\gamma)^2 - \theta\beta\gamma(\theta + \beta + \gamma) \overset{(1), (2) \text{ e } (3)}{=} a^2 - (-b)(0) = a^2.$$

3. Consideramos a seguinte manipulação:

$$\theta^2\beta + \theta^2\gamma + \theta\beta^2 + \beta^2\gamma + \theta\gamma^2 + \beta\gamma^2 = \theta(\theta\beta + \theta\gamma) + \beta(\theta\beta + \beta\gamma) + \gamma(\theta\gamma + \beta\gamma) =$$
$$= \theta((\theta\beta + \theta\gamma + \beta\gamma) - \beta\gamma) + \beta((\theta\beta + \theta\gamma + \beta\gamma) - \theta\gamma) + \gamma((\theta\beta + \theta\gamma + \beta\gamma) - \theta\beta) =$$
$$= (\theta + \beta + \gamma)(\theta\beta + \theta\gamma + \beta\gamma) - 3\theta\beta\gamma.$$

Dessa forma, usando as Relações de Girard, segue que

$$\theta^2\beta + \theta^2\gamma + \theta\beta^2 + \beta^2\gamma + \theta\gamma^2 + \beta\gamma^2 = (\theta + \beta + \gamma)(\theta\beta + \theta\gamma + \beta\gamma) - 3\theta\beta\gamma \overset{(1),\ (2)\ \text{e}\ (3)}{=}$$
$$= (a)(0) - 3(-b) = 3b,$$

o que prova o lema. □

Para o caso geral das cúbicas, apresentamos nas proposições seguintes as funções traço, norma e polinômio característico.

Proposição 4.2.1. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico e $\theta \in \mathbb{C}$ é um inteiro algébrico cujo polinômio minimal é o $p(x) = x^3+ax+b \in \mathbb{Z}[x]$. O traço do elemento $\alpha = a_0+a_1\theta+a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$, é dado por*

$$\mathcal{T}r(\alpha) = 3a_0 - 2a_2a. \tag{4.1}$$

Demonstração. Sejam θ, β e γ as raízes de $p(x)$. Usando as relações de Girard para o polinômio $p(x) = x^3 + ax + b$, segue que

$$\theta + \beta + \gamma = 0 \ (1)$$
$$\theta\beta + \theta\gamma + \beta\gamma = a \ (2)$$
$$\theta\beta\gamma = -b \ (3).$$

Agora, consideramos σ_i os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \beta$ e $\sigma_3(\theta) = \gamma$. Com isso, calculamos o traço de α usando a Proposição 2.3.4, as Relações de Girard e o Lema 4.2.1, ou seja,

$$\begin{aligned}
\mathcal{T}r(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha) = \\
&= \sigma_1(a_0 + a_1\theta + a_2\theta^2) + \sigma_2(a_0 + a_1\theta + a_2\theta^2) + \sigma_3(a_0 + a_1\theta + a_2\theta^2) = \\
&= (a_0 + a_1\theta + a_2\theta^2) + (a_0 + a_1\beta + a_2\beta^2) + (a_0 + a_1\gamma + a_2\gamma^2) = \\
&= 3a_0 + a_1(\theta + \beta + \gamma) + a_2(\theta^2 + \beta^2 + \gamma^2) \overset{(1)\ \text{e Lema 4.2.1}}{=} \\
&= 3a_0 + a_1(0) + a_2(-2a) = \\
&= 3a_0 - 2a_2a.
\end{aligned}$$

Portanto, $\mathcal{T}r(\alpha) = 3a_0 - 2a_2a$. □

Proposição 4.2.2. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico e $\theta \in \mathbb{C}$ é um inteiro algébrico cujo polinômio minimal é o $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$. A norma do elemento $\alpha = a_0 + a_1\theta + a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$, é dada por*

$$\mathcal{N}(\alpha) = a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2. \tag{4.2}$$

Demonstração. Sejam θ, β e γ as raízes de $p(x)$. Usando as relações de Girard para o polinômio $p(x) = x^3 + ax + b$, segue que

$$\begin{aligned} \theta + \beta + \gamma &= 0 \ (1) \\ \theta\beta + \theta\gamma + \beta\gamma &= a \ (2) \\ \theta\beta\gamma &= -b \ (3). \end{aligned}$$

Consideramos σ_i os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \beta$ e $\sigma_3(\theta) = \gamma$. Com isso, calculamos a norma de α usando a Proposição 2.3.4, as Relações de Girard (1), (2) e (3) e o Lema 4.2.1 $(*)$, ou seja,

$$\begin{aligned} \mathcal{N}(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha)\sigma_3(\alpha) = \\ &= \sigma_1(a_0 + a_1\theta + a_2\theta^2)\sigma_2(a_0 + a_1\theta + a_2\theta^2)\sigma_3(a_0 + a_1\theta + a_2\theta^2) = \\ &= (a_0 + a_1\theta + a_2\theta^2)(a_0 + a_1\beta + a_2\beta^2)(a_0 + a_1\gamma + a_2\gamma^2) = \\ &= (a_0^2 + a_0a_1\beta + a_0a_1\beta^2 + a_0a_1\theta + a_1^2\theta\beta + a_1a_2\theta\beta^2 + a_0a_2\theta^2 + a_1a_2\theta^2\beta + a_2^2\theta^2\beta^2)\times \\ &\times (a_0 + a_1\gamma + a_2\gamma^2) = \\ &= a_0^3 + a_0^2a_1\beta + a_0^2a_2\beta^2 + a_0^2a_1\theta + a_0a_1^2\theta\beta + a_0a_1a_2\theta\beta^2 + a_0^2a_2\theta^2 + a_0a_1a_2\theta^2\beta + \\ &+ a_0a_2^2\theta^2\beta^2 + a^2a_1\gamma + a_0a_1^2\beta\gamma + a_0a_1a_2\beta^2\gamma + a_0a_1^2\theta\gamma + a_1^3\theta\beta\gamma + a_1^2a_2\theta\beta^2\gamma + \\ &+ a_0a_1a_2\theta^2\gamma + a_1^2a_2\theta^2\beta\gamma + a_1^2a_2\theta^2\beta^2\gamma + a_0^2a_2\gamma^2 + a_0a_1a_2\beta\gamma^2 + a_0a_2^2\beta^2\gamma^2 + \\ &+ a_0a_1a_2\theta\gamma^2 + a_1^2a_2\theta\beta\gamma^2 + a_1a_2^2\theta\beta^2\gamma^2 + a_0a_2^2\theta^2\gamma^2 + a_1a_2^2\theta^2\beta\gamma^2 + a_2^3\theta^2\beta^2\gamma^2 = \\ &= a_0^3 + a_0^2a_1(\theta + \beta + \gamma) + a_0^2a_2(\theta^2 + \beta^2 + \gamma^2) + a_0a_1^2(\theta\beta + \theta\gamma + \beta\gamma) + \\ &+ a_0a_1a_2(\theta\beta^2 + \theta^2\beta + \beta^2\gamma + \theta^2\gamma + \beta\gamma^2 + \theta\gamma^2) + a_0a_2^2(\theta^2\beta^2 + \beta^2\gamma^2 + \theta^2\gamma^2) + \\ &+ a_1^3(\theta\beta\gamma) + a_1^2a_2(\theta\beta\gamma)(\theta + \beta + \gamma) + a_1a_2^2(\theta\beta\gamma)(\theta\beta + \theta\gamma + \beta\gamma) + a_2^3(\theta\beta\gamma)^2 \overset{(*)}{=} \\ &= a_0^3 + a_0^2a_1(0) + a_0^2a_2(-2a) + a_0a_1^2(a) + a_0a_1a_2(3b) + a_0a_2^2(a^2) + a_1^3(-b) + \\ &+ a_1^2a_2(-b)(0) + a_1a_2^2(-b)(a) + a_2^3(-b)^2 = \\ &= a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2. \end{aligned}$$

Portanto, $\mathcal{N}(\alpha) = a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2$. □

Proposição 4.2.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico e $\theta \in \mathbb{C}$ é um inteiro algébrico cujo polinômio minimal é o $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$. O polinômio característico do elemento $\alpha = a_0 + a_1\theta + a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$, é dado por*

$$\begin{aligned} f_\alpha(x) = x^3 &- x^2(3a_0 - 2a_2a) + x(3a_0^2 - 4a_0a_2a + a_1^2a + 3a_1a_2b + a_2^2a^2) - \\ &- (a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2). \end{aligned} \tag{4.3}$$

Demonstração. Sejam θ, β e γ as raízes de $p(x)$. Usando as relações de Girard para o polinômio $p(x) = x^3 + ax + b$, segue que

$$\begin{aligned} \theta + \beta + \gamma &= 0 \ (1) \\ \theta\beta + \theta\gamma + \beta\gamma &= a \ (2) \\ \theta\beta\gamma &= -b \ (3). \end{aligned}$$

Consideramos σ_i os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \beta$ e $\sigma_3(\theta) = \gamma$. Para facilitar a escrita, seja $\alpha_i = \sigma_i(\alpha)$, com $i = 1, 2, 3$.

Assim,

$$\begin{aligned}\alpha_1 &= a_0 + a_1\theta + a_2\theta^2\\ \alpha_2 &= a_0 + a_1\beta + a_2\beta^2\\ \alpha_3 &= a_0 + a_1\gamma + a_2\gamma^2.\end{aligned}$$

Pela Proposição 2.3.4, segue que o polinômio característico de α é dado por

$$\begin{aligned}f_\alpha(x) &= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) =\\ &= (x^2 - x(\alpha_1+\alpha_2) + \alpha_1\alpha_2)(x-\alpha_3) =\\ &= x^3 - x^2(\alpha_1+\alpha_2+\alpha_3) + x(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - \alpha_1\alpha_2\alpha_3.\end{aligned}$$

Agora, vamos calcular os coeficientes do polinômio característico. Pela Proposição 4.2.1, segue que

$$\alpha_1 + \alpha_2 + \alpha_3 = \mathcal{T}r(\alpha) \overset{\text{Prop. } 4.2.1}{=} 3a_0 - 2a_2a.$$

No cálculo do próximo coeficiente, para facilitar as contas, vamos separar os termos,

$$\begin{aligned}\alpha_1\alpha_2 &= (a_0 + a_1\theta + a_2\theta^2)(a_0 + a_1\beta + a_2\beta^2) =\\ &= a_0^2 + a_0a_1\beta + a_0a_2\beta^2 + a_0a_1\theta + a_1^2\theta\beta + a_1a_2\theta\beta^2 + a_0a_2\theta^2 + a_1a_2\theta^2\beta + a_2^2\theta^2\beta^2.\\ \alpha_1\alpha_3 &= (a_0 + a_1\theta + a_2\theta^2)(a_0 + a_1\gamma + a_2\gamma^2) =\\ &= a_0^2 + a_0a_1\gamma + a_0a_2\gamma^2 + a_0a_1\theta + a_1^2\theta\gamma + a_1a_2\theta\gamma^2 + a_0a_2\theta^2 + a_1a_2\theta^2\gamma + a_2^2\theta^2\gamma^2.\\ \alpha_2\alpha_3 &= (a_0 + a_1\beta + a_2\beta^2)(a_0 + a_1\gamma + a_2\gamma^2)\\ &= a_0^2 + a_0a_1\gamma + a_0a_2\gamma^2 + a_0a_1\beta + a_1^2\beta\gamma + a_1a_2\beta\gamma^2 + a_0a_2\beta^2 + a_1a_2\beta^2\gamma + a_2^2\beta^2\gamma^2.\end{aligned}$$

Assim, juntando o que adquirimos anteriormente, usando o Lema 4.2.1 e as Relações de Girard, segue que

$$\begin{aligned}\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= 3a_0^2 + 2a_0a_1(\theta+\beta+\gamma) + 2a_0a_2(\theta^2+\beta^2+\gamma^2) +\\ &+ a_1^2(\theta\beta + \theta\gamma + \beta\gamma) + a_1a_2(\theta^2\beta + \theta^2\gamma + \theta\beta^2 + \beta^2\gamma + \theta\gamma^2 + \beta\gamma^2) +\\ &+ a_2^2(\theta^2\beta^2 + \theta^2\gamma^2 + \beta^2\gamma^2) =\\ &= 3a_0^2 + 2a_0a_1(0) + 2a_0a_2(-2a) + a_1^2(a) + a_1a_2(3b) + a_2^2(a^2) =\\ &= 3a_0^2 - 4a_0a_2a + a_1^2a + 3a_1a_2b + a_2^2a^2.\end{aligned}$$

Pela Proposição 4.2.2, segue que

$$\alpha_1\alpha_2\alpha_3 = \mathcal{N}(\alpha) \overset{\text{Prop. } 4.2.2}{=} a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2.$$

Logo,

$$\begin{aligned}f_\alpha(x) = x^3 &- x^2(3a_0 - 2a_2a) + x(3a_0^2 - 4a_0a_2a + a_1^2a + 3a_1a_2b + a_2^2a^2) -\\ &- (a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2).\end{aligned}$$

Portanto, encontramos o polinômio característico $f_\alpha(x)$. □

4.2.1 Discriminante da cúbica $p(x) = x^3 + ax + b$

Nesta seção, consideramos $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 3, onde a cúbica $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, é o polinômio minimal do elemento

primitivo θ. O objetivo é descobrir o anel dos inteiros desses corpos de números através do discriminante.

Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_\mathbb{K}$. E mais, pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2) = (-1)^{\frac{3(3-1)}{2}}[3^3 b^{3-1} + (-1)^{3+1}(3-1)^{3-1}a^3] = -(4a^3 + 27b^2).$$

Assim $\mathcal{D}(1, \theta, \theta^2) = -(4a^3 + 27b^2)$. Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 | a_0, a_1, a_2 \in \mathbb{Z}\}.$$

Exemplo 4.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 3 tal que $p(x) = x^3 - x - 1$ é o polinômio minimal do elemento primitivo θ. Como*

$$\mathcal{D}(1, \theta, \theta^2) = -(4(-1)^3 + 27(-1)^2) = -23 \text{ e}$$

$\mathcal{D}(1, \theta, \theta^2) = -23$ é livre de quadrados, segue que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$.

4.3 A cúbica $p(x) = x^3 - d$, com d livre de quadrados

Nessa seção, sejam $\mathbb{K}$ um corpo de números e $p(x) = x^3 - d$ uma cúbica, com $d \in \mathbb{Z}$ livre de quadrados. O elemento $\sqrt[3]{d}$ é um inteiro algébrico, pois $p(x)$ é o seu polinômio minimal em $\mathbb{Z}$. Pela Teoria de Corpos, segue que $[\mathbb{Q}(\sqrt[3]{d}) : \mathbb{Q}] = \partial(p) = 3$, e assim, $\mathbb{Q}(\sqrt[3]{d})$ é um corpo cúbico. Para este estudo, trabalhamos com os corpos cúbicos da forma $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$ cujo elemento primitivo é o próprio $\sqrt[3]{d}$. Salvo menção, chamamos $\theta = \sqrt[3]{d}$ o elemento primitivo, com $d \in \mathbb{Z}$ livre de quadrados e o corpo cúbico em questão é o $\mathbb{K} = Q(\theta)$.

Retomando as Proposições 2.6.4 e 2.6.5, sejam θ, $\theta\xi_3$ e $\theta\xi_3^2$ as raízes do polinômio $p(x)$, onde ξ_3^k são as raízes primitivas das unidade para $i = 0, 1, 2$. Assim,

$$\xi_3^k = e^{\frac{2\pi i}{3}k} = \cos\left(\frac{2k\pi}{3}\right) + i\,\text{sen}\left(\frac{2k\pi}{3}\right).$$

Logo, $\xi_3^0 = 1$, $\xi_3^1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e $\xi_3^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, onde $\xi_3^1 + \xi_3^2 = -1$.

Pelo Teorema 2.3.2, podemos considerar σ_k os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_k(\theta) = \theta\xi_3^{k-1}$, com $k = 1, 2, 3$. Portanto, os $\mathbb{Q}$-monomorfismos em θ são definidos por $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \theta\xi_3$ e $\sigma_3(\theta) = \theta\xi_3^2$. Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim, podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta + a_2\theta^2$, onde $a_0, a_1, a_2 \in \mathbb{Q}$.

4.3.1 O anel dos inteiros de $\mathbb{Q}(\sqrt[3]{d})$

Seguindo as notações da seção, vamos encontrar o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K} = \mathbb{Q}(\theta)$ (sobre $\mathbb{Z}$). Para isso, inicialmente, faremos uma preparação através do próximo resultado, para identificar o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$.

Proposição 4.3.1. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[3]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$. O polinômio característico de α é dado por*

$$f_\alpha(x) = x^3 - x^2(3a_0) + x(3a_0^2 - 3a_1a_2d) - [a_0^3 - 3a_0a_1a_2d + d(a_1^3 + a_2^3d)]. \tag{4.4}$$

Demonstração. Na Proposição 4.2.3, calculamos o polinômio característico para o caso geral, e assim, esse resultado é uma particularidade da proposição e apenas precisamos substituir os coeficientes do polinômio $p(x) = x^3 - d$. □

Exemplo 4.3.1. *Seja* $\mathbb{K} = Q(\theta)$, *com* $\theta = \sqrt[3]{7}$ *e* $\alpha = 1 + \sqrt[3]{7} + 2(\sqrt[3]{7})^2 \in \mathbb{K}$. *Pela Proposição 4.3.1, o polinômio característico de* α *é calculado através da identificação dos valores* $a_0 = 1$, $a_1 = 1$, $a_2 = 2$ *e* $d = 7$ *e substituição direta. Logo,*

$$f_\alpha(x) = x^3 - 3x^2 - 39x - 358.$$

Com este resultado, podemos enunciar e demonstrar o teorema que caracterizará o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$. No teorema a seguir, a base integral que encontramos é sutilmente diferente da base integral apresentada na literatura.

Teorema 4.3.1. *Seja* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números, onde* $\theta = \sqrt[3]{d}$ *com* $d \in \mathbb{Z}$ *livre de quadrados. O anel dos inteiros algébricos* $\mathcal{O}_\mathbb{K}$ *de* $\mathbb{K}$ *é dado por*

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-2\theta+\theta^2}{3}\right), \text{ se } d \equiv 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-\theta+\theta^2}{3}\right), \text{ se } d \equiv -1 (mod\ 9). \end{cases}$$

Demonstração. Suponhamos $\alpha \in \mathbb{K}$ um inteiro algébrico e vamos explorar quais são as formas que α pode assumir, onde $\alpha = a_0 + a_1\theta + a_2\theta^2$, com $a_0, a_1, a_2 \in \mathbb{Q}$. Pela Proposição 2.6.9, se α é um inteiro algébrico, então $3a_0, 3a_1, 3a_2 \in \mathbb{Z}$. Vamos supor $3a_i = p_i$, com $p_i \in \mathbb{Z}$ para todo $i = 0, 1, 2$. Assim,

$$a_i = \frac{p_i}{3}, \text{ para todo } i = 0, 1, 2.$$

Além do mais, p_i pode ser escrito da seguinte forma

$$p_i = 3q_i + r_i,$$

com $q_i, r_i \in \mathbb{Z}$ e $r_i \in \{-1, 0, 1\}$, para $i = 0, 1, 2$. Reescrevendo α, segue que

$$\begin{aligned} \alpha = a_0 + a_1\theta + a_2\theta^2 = \frac{p_0}{3} + \frac{p_1}{3}\theta + \frac{p_2}{3}\theta^2 = \frac{3q_0 + r_0}{3} + \frac{3q_1 + r_1}{3}\theta + \frac{3q_2 + r_2}{3}\theta^2 = \\ = q_0 + q_1\theta + q_2\theta^2 + \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2. \end{aligned}$$

Logo,

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2. \tag{4.5}$$

Agora, como $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2) e $q = q_0 + q_1\theta + q_2\theta^2 \in \mathcal{O}_\mathbb{K}$, segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2 \in \mathcal{O}_\mathbb{K} \Leftrightarrow r = \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2 \in \mathcal{O}_\mathbb{K}.$$

Ou seja, α é um inteiro algébrico se, e somente se, r é um inteiro algébrico. Consequentemente,

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow r \in \mathcal{O}_\mathbb{K}. \tag{4.6}$$

Novamente por esses dois resultados (Proposição 4.3.1 e Proposição 2.3.3), segue que

$$r \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \begin{cases} 3\left(\frac{r_0}{3}\right) \in \mathbb{Z}, \\ 3\left(\frac{r_0}{3}\right)^2 - 3\left(\frac{r_1}{3}\right)\left(\frac{r_2}{3}\right) d \in \mathbb{Z} \text{ e} \\ \left(\frac{r_0}{3}\right)^3 - 3\left(\frac{r_0}{3}\right)\left(\frac{r_1}{3}\right)\left(\frac{r_2}{3}\right) d + d\left[\left(\frac{r_1}{3}\right)^3 + \left(\frac{r_2}{3}\right)^3 d\right] \in \mathbb{Z}. \end{cases} \tag{4.7}$$

Pelas implicações na Expressão (4.6) e na Expressão (4.7), segue que

$$\alpha \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \begin{cases} \frac{(r_0)^2 - r_1 r_2}{3} \in \mathbb{Z} \text{ e} \\ \frac{(r_0)^3 - 3r_0 r_1 r_2 d + d[(r_1)^3 + d(r_2)^3]}{27} \in \mathbb{Z}. \end{cases} \tag{4.8}$$

Agora, listamos todas as possibilidades para d de acordo com os parâmetros $r_0, r_1, r_2 \in \{0, 1, 2\}$. Para isso, renomeramos as equações obtidas na Expressão (4.8) da seguinte forma

$$\omega_1 = \frac{(r_0)^2 - r_1 r_2}{3}. \tag{4.9}$$

$$\omega_2 = \frac{(r_0)^3 - 3r_0 r_1 r_2 d + d[(r_1)^3 + d(r_2)^3]}{27}. \tag{4.10}$$

Na Tabela (4.3.1), apresentamos uma análise das linhas que possuem solução, ou seja, que existe d tal que $\omega_1, \omega_2 \in \mathbb{Z}$ (vide Equação (4.9) e Equação (4.10)), para consequentemente encontrar o anel dos inteiros algébricos. De imediato observamos que este caso se trata da análise de 27 possibilidades. Agora,

1. Se $r_0 \neq 0$, $r_1 = 0$ ou $r_2 = 0$, então $\omega_1 \notin \mathbb{Z}$.
2. Se $r_0 = 0$, $r_1 = 0$ ou (exclusivo) $r_2 = 0$, então $\omega_1 = 0$ e ω_2 é um número inteiro precisamente se $d \equiv 0 (mod\ 9)$, mas como d é livre de quadrados estes casos não possuem solução.

Afim de melhorar a quantidade de linhas para análise excluiremos as possibilidades em questão e vamos examinar as linhas decorrentes expressar pela Tabela (4.3.1).

Tabela 4.1: $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$, d livre de quadrados - casos para análise de $\mathcal{O}_{\mathbb{K}}$.

Linhas	r_0	r_1	r_2	ω_1	ω_2	$d \equiv (?) (mod\ 9)$
Linha 1	0	0	0	0	0	$\forall d$
Linha 2	0	1	1	$\frac{-d}{3}$	$\frac{d + d^2}{27}$	$\nexists d$
Linha 3	0	1	2	$\frac{-2d}{3}$	$\frac{d + 8d^2}{27}$	$\nexists d$
Linha 4	0	2	1	$\frac{-2d}{3}$	$\frac{8d + d^2}{27}$	$\nexists d$
Linha 5	0	2	2	$\frac{-4d}{3}$	$\frac{8(d + d^2)}{27}$	$\nexists d$

Linha 6	1	1	1	$\frac{1-d}{3}$	$\frac{(1-d)^2}{27}$	$d \equiv 1(mod\ 9)$
Linha 7	0	1	2	$\frac{1-2d}{3}$	$\frac{1-5d+8d^2}{27}$	$\nexists d$
Linha 8	1	2	1	$\frac{1-2d}{3}$	$\frac{(1+d)^2}{27}$	$d \equiv -1(mod\ 9)$
Linha 9	1	2	2	$\frac{1-4d}{3}$	$\frac{1-4d+8d^2}{27}$	$\nexists d$
Linha 10	2	1	1	$\frac{4-d}{3}$	$\frac{8-d+d^2}{27}$	$\nexists d$
Linha 11	2	1	2	$\frac{4-2d}{3}$	$\frac{8-11d+8d^2}{27}$	$d \equiv -1(mod\ 9)$
Linha 12	2	2	1	$\frac{4-2d}{3}$	$\frac{8-4d+d^2}{27}$	$\nexists d$
Linha 13	2	2	2	$\frac{4-4d}{3}$	$\frac{8(1-d)^2}{27}$	$d \equiv 1(mod\ 9)$

Fonte: Elaborada pela autora.

Na Tabela (4.3.1), a célula "$\forall d$" não inclui as equivalências não livre de quadrados, uma vez que d é livre de quadrados. Para as linhas que possuem solução, apresentamos uma análise da possível base integral de acordo com as congruências de d módulo 9. Recordamos que a Equação (4.5) que será importante para essa análise, ou seja,

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \left(\frac{r_0 + r_1\theta + r_2\theta^2}{3}\right).$$

1. Quando $d \not\equiv \pm 1(mod\ 9)$, faremos a investigação da linha que identifica esse caso. Para a Linha 1, os restos são $r_0 = 0$, $r_1 = 0$ e $r_2 = 0$. Assim, substituindo os restos na Equação (4.5), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2.$$

   Mas, $q_0, q_1, q_2 \in \mathbb{Z}$, e dessa forma, $\alpha \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$. Assim, para $d \not\equiv \pm 1(mod\ 9)$, segue que o anel dos inteiros é $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$.

2. Quando $d \equiv 1(mod\ 9)$, faremos a investigação das linhas que identificam esse caso.

   (a) Para a Linha 6, os restos são $r_0 = 1$, $r_1 = 1$ e $r_2 = 1$. Assim, substituindo os restos na Equação (4.5), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \left(\frac{1 + \theta + \theta^2}{3}\right) = \left(q_0 + \frac{1}{3}\right) + \left(q_1 + \frac{1}{3}\right)\theta + \left(q_2 + \frac{1}{3}\right)\theta^2.$$

   Agora, vamos mostrar que para este caso a base integral é $\left\{1, \theta, \frac{-2 - 2\theta + \theta^2}{3}\right\}$. Assim, suponhamos que para algum z_0, z_1 e z_2 podemos escrever

$$\alpha = z_0 + z_1\theta + z_2\left(\frac{-2 - 2\theta + \theta^2}{3}\right) = \left(z_0 - \frac{2z_2}{3}\right) + \left(z_1 - \frac{2z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.$$

Comparando as formas que α pode ser escrito, montamos o seguinte sistema

$$\begin{cases} z_0 - \dfrac{2z_2}{3} = q_0 + \dfrac{1}{3} \\ z_1 - \dfrac{2z_2}{3} = q_1 + \dfrac{1}{3} \\ \dfrac{z_2}{3} = q_2 + \dfrac{1}{3} \end{cases}$$

Resolvendo o sistema, segue que $z_0 = q_0+2q_2+1$, $z_1 = q_1+2q_2+1$ e $z_2 = 3q_2+1$. Como $q_0, q_1, q_2 \in \mathbb{Z}$, segue que $z_0, z_1, z_2 \in \mathbb{Z}$. Deste modo, $\alpha \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\dfrac{-2-2\theta+\theta^2}{3}\right)$.

(b) Para a Linha 13, os restos são $r_0 = 2$, $r_1 = 2$ e $r_2 = 2$. Assim, substituindo os restos na Equação (4.5), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \left(\frac{2+2\theta+2\theta^2}{3}\right) = \left(q_0 + \frac{2}{3}\right) + \left(q_1 + \frac{2}{3}\right)\theta + \left(q_2 + \frac{2}{3}\right)\theta^2.$$

Agora, vamos mostrar que para este caso a base integral é $\left\{1, \theta, \dfrac{-2-2\theta+\theta^2}{3}\right\}$. Assim, suponhamos que para algum z_0, z_1 e z_2 podemos escrever

$$\alpha = z_0 + z_1\theta + z_2\left(\frac{-2-2\theta+\theta^2}{3}\right) = \left(z_0 - \frac{2z_2}{3}\right) + \left(z_1 - \frac{2z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.$$

Assim, comparando as formas que α pode ser escrito, montamos o seguinte sistema

$$\begin{cases} z_0 - \dfrac{2z_2}{3} = q_0 + \dfrac{2}{3} \\ z_1 - \dfrac{2z_2}{3} = q_1 + \dfrac{2}{3} \\ \dfrac{z_2}{3} = q_2 + \dfrac{2}{3} \end{cases}$$

Resolvendo o sistema, segue que $z_0 = q_0+2q_2+2$, $z_1 = q_1+2q_2+2$ e $z_2 = 3q_2+2$. Como $q_0, q_1, q_2 \in \mathbb{Z}$, segue que $z_0, z_1, z_2 \in \mathbb{Z}$. Deste modo, $\alpha \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\dfrac{-2-2\theta+\theta^2}{3}\right)$.

Assim, para $d \equiv 1(mod\ 9)$ o anel dos inteiros é $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\dfrac{-2-2\theta+\theta^2}{3}\right)$.

3. Quando $d \equiv -1(mod\ 9)$, faremos a investigação das linhas que identificam esse caso.

(a) Para a Linha 8, os restos são $r_0 = 1$, $r_1 = 2$ e $r_2 = 1$. Assim, substituindo os restos na Equação (4.5), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \left(\frac{1+2\theta+\theta^2}{3}\right) = \left(q_0 + \frac{1}{3}\right) + \left(q_1 + \frac{2}{3}\right)\theta + \left(q_2 + \frac{1}{3}\right)\theta^2.$$

Agora, vamos mostrar que para este caso a base integral é $\left\{1, \theta, \dfrac{-2-\theta+\theta^2}{3}\right\}$. Assim, suponhamos que para algum z_0, z_1 e z_2 podemos escrever

$$\alpha = z_0 + z_1\theta + z_2\left(\frac{-2-\theta+\theta^2}{3}\right) = \left(z_0 - \frac{2z_2}{3}\right) + \left(z_1 - \frac{z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.$$

Assim, comparando as formas que α pode ser escrito, montamos o seguinte sistema

$$\begin{cases} z_0 - \dfrac{2z_2}{3} = q_0 + \dfrac{1}{3} \\ z_1 - \dfrac{z_2}{3} = q_1 + \dfrac{2}{3} \\ \dfrac{z_2}{3} = q_2 + \dfrac{1}{3} \end{cases}$$

Resolvendo o sistema, segue que $z_0 = q_0 + 2q_2 + 1$, $z_1 = q_1 + q_2 + 1$ e $z_2 = 3q_2 + 1$. Como $q_0, q_1, q_2 \in \mathbb{Z}$, segue que $z_0, z_1, z_2 \in \mathbb{Z}$. Deste modo, $\alpha \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\dfrac{-2 - \theta + \theta^2}{3}\right)$.

(b) Para a Linha 11, os restos são $r_0 = 2$, $r_1 = 1$ e $r_2 = 2$. Assim, substituindo os restos na Equação (4.5), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \left(\frac{2 + \theta + 2\theta^2}{3}\right) = \left(q_0 + \frac{2}{3}\right) + \left(q_1 + \frac{1}{3}\right)\theta + \left(q_2 + \frac{2}{3}\right)\theta^2.$$

Agora, vamos mostrar que para este caso a base integral é $\left\{1, \theta, \dfrac{-2 - \theta + \theta^2}{3}\right\}$. Assim, suponhamos que para algum z_0, z_1 e z_2 podemos escrever

$$\alpha = z_0 + z_1\theta + z_2\left(\frac{-2 - \theta + \theta^2}{3}\right) = \left(z_0 - \frac{2z_2}{3}\right) + \left(z_1 - \frac{z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.$$

Assim, comparando as formas que α pode ser escrito, montamos o seguinte sistema

$$\begin{cases} z_0 - \dfrac{2z_2}{3} = q_0 + \dfrac{2}{3} \\ z_1 - \dfrac{z_2}{3} = q_1 + \dfrac{1}{3} \\ \dfrac{z_2}{3} = q_2 + \dfrac{2}{3} \end{cases}$$

Resolvendo o sistema,segue que $z_0 = q_0 + 2q_2 + 2$, $z_1 = q_1 + q_2 + 1$ e $z_2 = 3q_2 + 2$. Como $q_0, q_1, q_2 \in \mathbb{Z}$, segue que $z_0, z_1, z_2 \in \mathbb{Z}$. Deste modo, $\alpha \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\dfrac{-2 - \theta + \theta^2}{3}\right)$.

Logo, para $d \equiv -1 (mod\ 9)$ o anel dos inteiros é dado por $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\dfrac{-2 - \theta + \theta^2}{3}\right)$.

Portanto, o anel dos inteiros algébricos é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - 2\theta + \theta^2}{3}\right), \text{ se } d \equiv 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - \theta + \theta^2}{3}\right), \text{ se } d \equiv -1 (mod\ 9), \end{cases}$$

o que prova o teorema. □

Exemplo 4.3.2. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[3]{7}$. Como $d = 7$ e $7 \equiv 7 (mod\ 9)$, pelo Teorema 4.3.1, segue que o anel dos inteiros algébricos desse caso é dado por*

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2.$$

4.3.2 Norma, traço e discriminante em $\mathbb{Q}(\sqrt[3]{d})$

Nesta seção, apresentamos a norma, o traço e o discriminante em $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$, com d um inteiro livre de quadrados. Para isso, lembramos que o polinômio minimal de θ sobre os inteiros é o $p(x) = x^3 - d$, cuja as raízes são θ, $\theta\xi_3$ e $\theta\xi_3^2$, com ξ_3^{i-1} raízes da unidade para $i = 1, 2, 3$.

Proposição 4.3.2. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[3]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$. O traço de α é calculado por*

$$\mathcal{T}r(\alpha) = 3a_0.$$

Demonstração. Na Proposição 4.2.1, calculamos o traço para o caso geral, assim esses resultado é uma particularidade da proposição e apenas precisamos substituir os coeficientes do polinômio $p(x) = x^3 - d$. Portanto, $\mathcal{T}r(\alpha) = 3a_0$. □

Proposição 4.3.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[3]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$. A norma de α é calculada por:*

$$\mathcal{N}(\alpha) = a_0^3 - 3a_0a_1a_2d + a_1^3d + a_2^3d^2.$$

Demonstração. Na Proposição 4.2.2, calculamos a norma para o caso geral, assim esses resultado é uma particularidade da proposição e apenas precisamos substituir os coeficientes do polinômio $p(x) = x^3 - d$. Portanto, $\mathcal{N}(\alpha) = a_0^3 - 3a_0a_1a_2d + a_1^3d + a_2^3d^2$. □

Exemplo 4.3.3. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[3]{7}$ e $\alpha = 1 + \sqrt[3]{7} + 2(\sqrt[3]{7})^2 \in \mathbb{K}$.*

a) Pela Proposição 4.3.2, segue que o traço de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 1$, $a_2 = 2$ e $d = 7$ e substituição direta. Logo, $\mathcal{T}r(\alpha) = 3$.

b) Pela Proposição 4.3.3, segue que a norma de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 1$, $a_2 = 2$ e $d = 7$ e substituição direta. Logo, $\mathcal{N}(\alpha) = 358$.

Proposição 4.3.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[3]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O discriminante do anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -27d^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ -3d^2, \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

Demonstração. Pelo Teorema 4.3.1, segue que o anel dos inteiros $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-2\theta+\theta^2}{3}\right), \text{ se } d \equiv 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-\theta+\theta^2}{3}\right), \text{ se } d \equiv -1 (mod\ 9). \end{cases}$$

Assim, a base integral (base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$) admite as possibilidades.

1. Se $d \not\equiv \pm 1 (mod\ 9)$, então a base integral é $\{1, \theta, \theta^2\}$.
2. Se $d \equiv 1 (mod\ 9)$, então a base integral é $\left\{1, \theta, \dfrac{-2 - 2\theta + \theta^2}{3}\right\}$.

3. Se $d \equiv -1(mod\ 9)$, então a base integral é $\left\{1, \theta, \dfrac{-2-\theta+\theta^2}{3}\right\}$.

Pela Proposição 2.6.8, segue que

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, \\ 3d^s, \text{ se } k = 3s, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > 3 \text{ e } k \not\equiv 0(mod\ 3). \end{cases} \tag{4.11}$$

Logo, $\mathcal{T}r(1) = 3$, $\mathcal{T}r(\theta) = 0$, $\mathcal{T}r(\theta^2) = 0$, $\mathcal{T}r(d) = 3d$ e $\mathcal{T}r(\theta^4) = 0$. Agora, analisamos o discriminante para cada possibilidade da base integral.

1. Se $d \not\equiv 1(mod\ 9)$, então a base é $\{1, \theta, \theta^2\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (4.11), segue que

$$\mathcal{D}(1, \theta, \theta^2) = \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(d) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(d) & \mathcal{T}r(\theta^4) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3d \\ 0 & 3d & 0 \end{pmatrix} = -27d^2.$$

2. Se $d \equiv 1(mod\ 9)$, então a base é $\left\{1, \theta, \dfrac{-2-2\theta+\theta^2}{3}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (4.11), segue que

$$\begin{aligned} \mathcal{D}\left(1, \theta, \frac{-2-2\theta+\theta^2}{3}\right) &= \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r\left(\frac{-2-2\theta+\theta^2}{3}\right) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r\left(\frac{-2\theta-2\theta^2+d}{3}\right) \\ \mathcal{T}r\left(\frac{-2-2\theta+\theta^2}{3}\right) & \mathcal{T}r\left(\frac{-2\theta-2\theta^2+d}{3}\right) & \mathcal{T}r\left(\frac{4+8\theta+4\theta^2-4d+\theta^4}{9}\right) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & 0 & -2 \\ 0 & 0 & d \\ -2 & d & \frac{4-4d}{3} \end{pmatrix} = -3d^2. \end{aligned}$$

3. Se $d \equiv -1(mod\ 9)$, então a base é $\left\{1, \theta, \dfrac{-2-\theta+\theta^2}{3}\right\}$. Assim, usando as propriedades de traço e (1), (2), (3), (4) e (5), segue que

$$\begin{aligned} \mathcal{D}\left(1, \theta, \frac{-2-\theta+\theta^2}{3}\right) &= \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r\left(\frac{-2-\theta+\theta^2}{3}\right) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r\left(\frac{-2\theta-\theta^2+d}{3}\right) \\ \mathcal{T}r\left(\frac{-2-\theta+\theta^2}{3}\right) & \mathcal{T}r\left(\frac{-2\theta-\theta^2+d}{3}\right) & \mathcal{T}r\left(\frac{4+4\theta-3\theta^2-2d+\theta^4}{9}\right) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & 0 & -2 \\ 0 & 0 & d \\ -2 & d & \frac{4-2d}{3} \end{pmatrix} = -3d^2. \end{aligned}$$

Logo, da análise dos itens (1), (2) e (3), segue que

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -27d^2, \text{ se } d \not\equiv \pm 1(mod\ 9) \\ -3d^2, \text{ se } d \equiv \pm 1(mod\ 9), \end{cases}$$

o que prova a proposição. □

Exemplo 4.3.4. *Seja* $\mathbb{K} = Q(\theta)$*, com* $\theta = \sqrt[3]{7}$*. Como* $d = 7$ *e* $7 \equiv 7(mod\ 9)$*, pela Proposição 4.3.4, segue que o discriminante é dado por* $\mathcal{D}(\mathbb{K}) = -27 \times 7^2 = -1323$*.*

Observação 4.3.1. *Para* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números, onde* $\theta = \sqrt[3]{d}$*, com* $d \in \mathbb{Z}$ *livre de quadrados, podemos calcular o discriminante da base potente* $\{1, \theta, \theta^2\}$ *através do polinômio minimal* $p(x) = x^3 - d$*, e assim, utilizando o Corolário 2.5.4, segue que*

$$\mathcal{D}(1, \theta, \theta^2) = (-1)^{\frac{3^2+3+2}{2}}[3^3 d^{3-1}] = -27d^2.$$

5 Extensões Quárticas

Os corpos quárticos $\mathbb{K}$ são corpos de números providos de uma extensão quártica, ou seja, $[\mathbb{K} : \mathbb{Q}] = 4$. Neste capítulo, apresentamos alguns corpos quárticos, pois diferentemente do Capítulo 3 onde apresentamos os corpos quadráticos, não é tão simples identificar o elemento primitivo dos corpos quárticos. Dessa forma, a complexidade do caso geral nos leva a focar em casos particulares. Por isso, chamamos a atenção para os corpos quárticos nos quais o elemento primitivo tem como polinômio minimal $p(x) = x^4 - d$, com d um inteiro livre de quadrados. O nosso objetivo é determinar o anel dos inteiros algébricos desses corpos quárticos. Observamos que a base integral encontrada na referência [8] não está completa, ou seja, não é válida quando $d \equiv 1(mod\ 8)$. Assim, neste capítulo, apresentamos uma nova versão (de nossa autoria) do resultado apresentado em [8], onde determinamos completamente o anel dos inteiros algébricos para qualquer inteiro $d \neq 1$ e livre de quadrados. Como aplicação direta, apresentamos também a norma e traço de um elemento desses corpos quárticos e o discriminante da base integral. Este capítulo foi inspirado pelas referências [7], [8] e [9].

5.1 Corpos quárticos

Nesta seção, apresentamos as extensões quárticas e alguns conceitos básicos e propriedades.

Definição 5.1.1. *Seja $\mathbb{K}$ um corpo de números, com o grau da extensão $[\mathbb{K} : \mathbb{Q}] = 4$.*

1. *O corpo de números $\mathbb{K}$ é chamado de **corpo quártico**.*

2. *A extensão de corpos $\mathbb{Q} \subseteq \mathbb{K}$ é chamada de **extensão quártica**.*

3. *O polinômio $p(x) \in \mathbb{Q}[x]$, cujo grau é $\partial(p) = 4$, é chamado de **quártica**.*

Consideramos $\mathbb{K}$ um corpo quártico, ou seja, o grau da extensão é $[\mathbb{K} : \mathbb{Q}] = 4$. Pelo Teorema do Elemento Primitivo, segue que existe $\theta \in \mathbb{C}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$, ou seja, θ é o elemento primitivo de $\mathbb{K}$. Seja $p(y) = y^4 + a_3y^3 + a_2y^2 + a_1y + a_0$ o polinômio minimal de θ sobre $\mathbb{Q}$. A ideia é melhorar $p(y)$ reduzindo algum coeficiente, por isso faremos a seguinte mudança de variável $y = x - l$, ou seja,

$$\begin{aligned} p(x-l) &= (x-l)^4 + a_3(x-l)^3 + a_2(x-l)^2 + a_1(x-l) + a_0 = \\ &= x^4 + (-4l + a_3)x^3 + (6l^2 - 3a_3l + a_2)x^2 + (-4l^3 + 3a_3l^2 - 2a_2l + a_1)x + \\ &+ (l^4 - a_3l^3 + a_2l^2 - a_1l + a_0) \end{aligned}$$

O objetivo é cancelar o coeficiente $-4l+a_3$, e para isso, tomamos $l = \frac{a_3}{4} \in \mathbb{Q}$. Fazendo as substituições, segue que os coeficientes restantes são $b_2 = -\frac{3a_3^2}{8} + a_2$, $b_1 = \frac{a_3^3}{8} - \frac{a_2 a_3}{2} + a_1$ e $b_0 = -\frac{3a_3^4}{256} + \frac{a_2 a_3^2}{16} - \frac{a_1 a_3}{4} + a_0$ com $b_0, b_1, b_2 \in \mathbb{Q}$. Portanto, sem perda de generalidade, consideramos $p(x) = x^4 + b_2 x^2 + b_1 x + b_0 \in \mathbb{Q}[x]$. Um fato interessante é que $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\theta - l)$, e assim, não temos problema em usar esses parâmetros. Com isso, o ambiente desenvolvido expressa o seguinte campo para trabalho. Sejam $\mathbb{K}$ um corpo quártico e $\theta \in \mathbb{C}$ o seu elemento primitivo, e assim, $\mathbb{K} = \mathbb{Q}(\theta)$. Consideramos θ um inteiro algébrico e pelas considerações anteriores, segue que o seu polinômio minimal pode ser escrito da forma $p(x) = x^4 + b_2 x^2 + b_1 x + b_0$, com $b_0, b_1, b_2 \in \mathbb{Z}$.

5.2 A quártica $p(x) = x^4 + ax + b$

Nesta seção, consideramos $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 4, onde a quártica $p(x) = x^4 + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, é o polinômio minimal do elemento primitivo θ. O objetivo é descobrir o anel dos inteiros desses corpos de números através do discriminante. Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2, \theta^3\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_\mathbb{K}$. E mais, pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3) = (-1)^{\frac{4(4-1)}{2}}[4^4 b^{4-1} + (-1)^{4+1}(4-1)^{4-1} a^4] = -27a^4 + 256b^3.$$

Assim, $\mathcal{D}(1, \theta, \theta^2, \theta^3) = -27a^4 + 256b^3$. Pela Proposição 2.5.5, se o discriminante denotado por $\mathcal{D}(1, \theta, \theta^2, \theta^3)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 | a_0, a_1, a_2, a_3 \in \mathbb{Z}\}.$$

Exemplo 5.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 4 tal que $p(x) = x^4 - x - 1$ é o polinômio minimal do elemento primitivo θ. Como*

$$\mathcal{D}(1, \theta, \theta^2, \theta^3) = -27(-1)^4 + 256(-1)^3 = -283 \text{ e}$$

$\mathcal{D}(1, \theta, \theta^2, \theta^3) = -283$ *é livre de quadrados (283 é primo), segue que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$.*

5.3 A quártica $p(x) = x^4 - d$, com d livre de quadrados

Nessa seção, sejam $\mathbb{K}$ um corpo de números e $p(x) = x^4 - d$ uma quártica, com $d \in \mathbb{Z}$ livre de quadrados. O elemento $\sqrt[4]{d}$ é um inteiro algébrico, pois $p(x)$ é o seu polinômio minimal em $\mathbb{Z}$. Pela Teoria de Corpos, segue que $[\mathbb{Q}(\sqrt[4]{d}) : \mathbb{Q}] = \partial(p) = 4$, e assim, $\mathbb{Q}(\sqrt[4]{d})$ é um corpo quártico. Para este estudo, trabalhamos com os corpos quárticos da forma $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$ cujo elemento primitivo é o próprio $\sqrt[4]{d}$. Salvo menção contrária, tomamos $\theta = \sqrt[4]{d}$ o elemento primitivo, com $d \in \mathbb{Z}$ livre de quadrados e o corpo quártico em questão é o $\mathbb{K} = Q(\theta)$.

Retomando as Proposições 2.6.4 e 2.6.5, sejam θ, $\theta\xi_4$ e $\theta\xi_4^2$ e $\theta\xi_4^3$ as raízes do polinômio $p(x)$, onde ξ_4^k são as raízes primitivas das unidade para $i = 0, 1, 2, 3$. Como

$$\xi_4^k = e^{\frac{2\pi i}{4}k} = \cos\left(\frac{2k\pi}{4}\right) + i\,\text{sen}\left(\frac{2k\pi}{4}\right),$$

segue que $\xi_4^0 = 1$, $\xi_4^1 = i$, $\xi_4^2 = -1$, $\xi_4^3 = -i$, vale ressaltar que $\xi_4^1 + \xi_4^2 + \xi_4^3 = -1$.

Pelo Teorema 2.3.2, podemos considerar σ_k os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_k(\theta) = \theta\xi_4^{k-1}$, com $k = 1, 2, 3, 4$. Portanto, os $\mathbb{Q}$-monomorfismos em θ são definidos por $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \theta\xi_4$, $\sigma_3(\theta) = \theta\xi_4^2$ e $\sigma_4(\theta) = \theta\xi_4^3$. Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2, \theta^3\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim, podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$, onde $a_i \in \mathbb{Q}$ para $i = 0, 1, 2, 3, 4$.

5.3.1 O anel dos inteiros de $\mathbb{Q}(\sqrt[4]{d})$

Seguindo as notações da seção, vamos encontrar o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K} = \mathbb{Q}(\theta)$ (sobre $\mathbb{Z}$). Desse modo, inicialmente, faremos uma preparação através do próximo resultado, para identificar o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$.

Proposição 5.3.1. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[4]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. O polinômio característico de α é dado por:*

$$\begin{aligned} f_\alpha(x) = x^4 - x^3[4a_0] + x^2[6a_0^2 - (2a_2^2 + 4a_1a_3)d] - x[4a_0^3 + (4a_1^2a_2 - 4a_0a_2^2 - \\ - 8a_0a_1a_3)d + (4a_2a_3^2)d^2] + [a_0^4 - (a_1^4 - 4a_0a_1^2a_2 + 2a_0^2a_2^2 + 4a_0^2a_1a_3)d + \\ + (a_2^4 - 4a_1a_2^2a_3 + 2a_1^2a_3^2 + 4a_0a_2a_3^2)d^2 - a_3^4d^3]. \end{aligned} \tag{5.1}$$

Demonstração. Consideramos $\alpha_i = \sigma_i(\alpha)$, com $i = 1, 2, 3, 4$. Assim,

$$\begin{aligned} \alpha_1 &= a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3, \\ \alpha_2 &= a_0 + a_1\theta\xi_4 + a_2\theta^2\xi_4^2 + a_3\theta^3\xi_4^3, \\ \alpha_3 &= a_0 + a_1\theta\xi_4^2 + a_2\theta^2 + a_3\theta^3\xi_4^2 \text{ e} \\ \alpha_4 &= a_0 + a_1\theta\xi_4^3 + a_2\theta^2\xi_4^2 + a_3\theta^3\xi_4. \end{aligned}$$

Pela Proposição 2.3.4, segue que o polinômio característico de α é dado por

$$\begin{aligned} f_\alpha(x) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) = \\ &= x^4 - x^3(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) + x^2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4) - \\ &- x(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) + (\alpha_1\alpha_2\alpha_3\alpha_4). \end{aligned}$$

Lembramos que $\xi_4 + \xi_4^2 + \xi_4^3 = -1$. Com o auxílio do programa Wolfram Mathematica 11.3, para desenvolvermos os coeficientes, segue que

$\to$ $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 4a_0$.

$\to$ $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4 = 6a_0^2 - (2a_2^2 + 4a_1a_3)d$.

$\to$ $\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 = 4a_0^3 + (4a_1^2a_2 - 4a_0a_2^2 - 8a_0a_1a_3)d + (4a_2a_3^2)d^2$.

$\to$ $\alpha_1\alpha_2\alpha_3\alpha_4 = a_0^4 - (a_1^4 - 4a_0a_1^2a_2 + 2a_0^2a_2^2 + 4a_0^2a_1a_3)d + (a_2^4 - 4a_1a_2^2a_3 + 2a_1^2a_3^2 + 4a_0a_2a_3^2)d^2 - a_3^4d^3$.

Assim,

$$\begin{aligned} f_\alpha(x) = x^4 - x^3[4a_0] + x^2[6a_0^2 - (2a_2^2 + 4a_1a_3)d] - x[4a_0^3 + (4a_1^2a_2 - 4a_0a_2^2 - \\ - 8a_0a_1a_3)d + (4a_2a_3^2)d^2] + [a_0^4 - (a_1^4 - 4a_0a_1^2a_2 + 2a_0^2a_2^2 + 4a_0^2a_1a_3)d + \\ + (a_2^4 - 4a_1a_2^2a_3 + 2a_1^2a_3^2 + 4a_0a_2a_3^2)d^2 - a_3^4d^3]. \end{aligned}$$

o que prova a proposição. □

Exemplo 5.3.1. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[4]{7}$ e $\alpha = 1 + 2(\sqrt[4]{7})^3 \in \mathbb{K}$. Pela Proposição 5.3.1, segue que o polinômio característico de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 2$ e $d = 7$ e substituição direta. Logo,*

$$f_\alpha(x) = x^4 - 4x^3 + 6x^2 - 4x - 5487.$$

Com este resultado, podemos enunciar e demonstrar o teorema que caracterizará o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$. O próximo teorema foi inspirado na determinação da base integral desses corpos da referência [8] que não está completa, uma vez que o caso onde $d \equiv 1(mod\ 8)$ e livre de quadrados, não foi analisado. Assim, o Teorema 5.3.1 é uma das nossas contribuições deste trabalho, onde apresentamos a determinação completa do anel de inteiros desses corpos.

Teorema 5.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[4]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3, \text{ se } d \not\equiv 1, 5(mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right), \text{ se } d \equiv 5(mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{ se } d \equiv 1(mod\ 8). \end{cases}$$

Demonstração. Suponhamos que $\alpha \in \mathbb{K}$ um inteiro algébrico e vamos explorar quais são as formas que α pode assumir. Lembramos que $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$, com $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. Pela Proposição 2.6.9, se α é um inteiro algébrico, então $4a_0, 4a_1, 4a_2, 4a_3 \in \mathbb{Z}$. Vamos supor $4a_i = p_i$, com $p_i \in \mathbb{Z}$ para todo $i = 0, 1, 2, 3$. Assim,

$$a_i = \frac{p_i}{4}, \text{para todo } i = 0, 1, 2, 3.$$

Além do mais, p_i pode ser escrito da seguinte forma

$$p_i = 4q_i + r_i,$$

com $q_i, r_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3\}$, para $i = 0, 1, 2, 3$. Reescrevendo α, segue que

$$\begin{aligned} \alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 = \frac{p_0}{4} + \frac{p_1}{4}\theta + \frac{p_2}{4}\theta^2 + \frac{p_3}{4}\theta^3 = \\ = \frac{4q_0 + r_0}{4} + \frac{4q_1 + r_1}{4}\theta + \frac{4q_2 + r_2}{4}\theta^2 + \frac{4q_3 + r_3}{4}\theta^3 = \\ = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3. \end{aligned}$$

Logo,

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3. \tag{5.2}$$

Agora, como $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2) e $q = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 \in \mathcal{O}_\mathbb{K}$, segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3 \in \mathcal{O}_\mathbb{K} \Leftrightarrow$$
$$r = \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3 \in \mathcal{O}_\mathbb{K}.$$

Assim, α é um inteiro algébrico se, e somente se, r é um inteiro algébrico. Consequentemente,

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow r \in \mathcal{O}_\mathbb{K}. \tag{5.3}$$

Novamente por esses dois resultados (Proposição 5.3.1 e Proposição 2.3.3), segue que

$$r \in \mathcal{O}_\mathbb{K} \Leftrightarrow \begin{cases} \dfrac{4r_0}{4} \in \mathbb{Z}, \\ \dfrac{6r_0^2}{16} - \left(\dfrac{2r_2^2}{16} + \dfrac{4r_1r_3}{16}\right) d \in \mathbb{Z}, \\ \dfrac{4r_0^3}{64} + \left(\dfrac{4r_1^2r_2}{64} - \dfrac{4r_0r_2^2}{64} - \dfrac{8r_0r_1r_3}{64}\right) d + \left(\dfrac{4r_2r_3^2}{64}\right) d^2 \in \mathbb{Z} \text{ e} \\ \dfrac{r_0^4}{256} - \left(\dfrac{r_1^4}{256} - \dfrac{4r_0r_1^2r_2}{256} + \dfrac{2r_0^2r_2^2}{256} + \dfrac{4r_0^2r_1r_3}{256}\right) d + \\ + \left(\dfrac{r_2^4}{256} - \dfrac{4r_1r_2^2r_3}{256} + \dfrac{2r_1^2r_3^2}{256} + \dfrac{4r_0r_2r_3^2}{256}\right) d^2 - \left(\dfrac{a_3^4}{256}\right) d^3 \in \mathbb{Z}. \end{cases} \tag{5.4}$$

Renomeando as expressões obtidas, segue

$$\omega_1 = \frac{3r_0^2 - (r_2^2 + 2r_1r_3)d}{8}. \tag{5.5}$$

$$\omega_2 = \frac{r_0^3 + (r_1^2r_2 - r_0r_2^2 - 2r_0r_1r_3)d + (r_2r_3^2)d^2}{16}. \tag{5.6}$$

$$\omega_3 = \frac{r_0^4 - (r_1^4 - 4r_0r_1^2r_2 + 2r_0^2r_2^2 + 4r_0^2r_1r_3)d + (r_2^4 - 4r_1r_2^2r_3 + 2r_1^2r_3^2)d^2}{256} + \\ + \frac{(4r_0r_2r_3^2)d^2 - (a_3^4)d^3}{256}. \tag{5.7}$$

Das implicações na Expressão (5.3) e na Expressão (5.4), segue que

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow \omega_1, \omega_2, \omega_3 \in \mathbb{Z}. \tag{5.8}$$

De acordo com os parâmetros $r_0, r_1, r_2, r_3 \in \{0, 1, 2, 3\}$, segue que este caso se trata da análise de 256 possibilidades. Mas, por este resultado se tratar de uma equivalência biunívoca, vamos encontrar somente as possibilidades que são soluções da forma (r_0, r_1, r_2, r_3). Para isso, vamos confirmar que a base integral pode ser $\{1, \theta, \theta^2, \theta^3\}$ ou $\left\{1, \theta, \dfrac{\theta^2 - 1}{2}, \dfrac{1 + \theta + \theta^2 + \theta^3}{2}\right\}$ e para quais valores de r_i's isso é verídico, com $i = 0, 1, 2, 3$.

1. Valores de r_i's para que a base integral seja $\{1, \theta, \theta^2, \theta^3\}$. Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (5.2), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3 = \\ = \left(q_0 + \frac{r_0}{4}\right) + \left(q_1 + \frac{r_1}{4}\right)\theta + \left(q_2 + \frac{r_2}{4}\right)\theta^2 + \left(q_3 + \frac{r_3}{3}\right)\theta^3.$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3\}$ para $i = 0,1,2,3$. Suponhamos que para $z_0, z_1, z_2, z_3 \in \mathbb{Z}$, α pode ser escrito como

$$\alpha = z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3.$$

Comparando as maneiras de escrever α obtemos as seguintes relações:

$$\begin{aligned} z_0 &= q_0 + \frac{r_0}{4} \ (1), \\ z_1 &= q_1 + \frac{r_1}{4} \ (2), \\ z_2 &= q_2 + \frac{r_2}{4} \ (3) \text{ e} \\ z_3 &= q_3 + \frac{r_3}{4} \ (4). \end{aligned}$$

Logo, o conjunto $\{1, \theta, \theta^2, \theta^3\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3\}$, para $i = 0,1,2,3$, segue que o conjunto citado é base integral se tivermos

(a) De (1), então $r_0 = 0$,

(b) De (2), então $r_1 = 0$,

(c) De (3), então $r_2 = 0$ e

(d) De (4), então $r_3 = 0$.

Assim, a solução possível é $(0,0,0,0)$.

2. Valores de r_i's para que a base integral seja $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{2}\right\}$. Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (5.2), segue que

$$\begin{aligned} \alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3 = \\ &= \left(q_0 + \frac{r_0}{4}\right) + \left(q_1 + \frac{r_1}{4}\right)\theta + \left(q_2 + \frac{r_2}{4}\right)\theta^2 + \left(q_3 + \frac{r_3}{3}\right)\theta^3. \end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3\}$ para $i = 0,1,2,3$. Suponhamos que para $z_0, z_1, z_2, z_3 \in \mathbb{Z}$, α pode ser escrito como

$$\begin{aligned} \alpha &= z_0 + z_1\theta + z_2\left(\frac{\theta^2-1}{2}\right) + z_3\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right) \\ &= \left(z_0 - \frac{z_2}{2} + \frac{z_3}{2}\right) + \left(z_1 + \frac{z_3}{2}\right)\theta + \left(\frac{z_2}{2} + \frac{z_3}{2}\right)\theta^2 + \left(\frac{z_3}{2}\right)\theta^3. \end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 - \frac{z_2}{2} + \frac{z_3}{2} &= q_0 + \frac{r_0}{4} \ (1), \\ z_1 + \frac{z_3}{2} &= q_1 + \frac{r_1}{4} \ (2), \\ \frac{z_2}{2} + \frac{z_3}{2} &= q_2 + \frac{r_2}{4} \ (3) \text{ e} \\ \frac{z_3}{2} &= q_3 + \frac{r_3}{4} \ (4). \end{aligned}$$

Logo, conjunto $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{2}\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3\}$, para $i = 0,1,2,3$, segue que o conjunto citado é base integral se tivermos

(a) De (4), segue que $z_3 = 2q_3 + \frac{r_3}{2}$. Assim,

$$\boxed{r_3 = 0 \text{ ou } r_3 = 2.}$$

(b) De (3) e (4), segue que $z_2 = 2q_2 - 2q_3 + \frac{r_2 - r_3}{2}$. Assim,

$$\boxed{r_2 \equiv r_3 (mod\ 2).}$$

(c) De (2) e (4), segue que $z_1 = q_1 - q_3 + \frac{r_1 - r_3}{4}$. Assim,

$$\boxed{r_1 = r_3.}$$

(d) De (1), (3) e (4), segue que $r_0 = q_0 + q_2 - 4q_3 + \frac{r_2 - 2r_3 + r_0}{4}$. Assim,

$$\boxed{r_0 \equiv 2r_3 - r_2 (mod\ 4).}$$

Assim, as soluções possíveis são $(0,0,0,0)$, $(0,2,0,2)$, $(2,0,2,0)$ e $(2,2,2,2)$.

3. Valores de r_i's para que a base integral seja $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}\right\}$. Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (5.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + \frac{r_0}{4} + \frac{r_1}{4}\theta + \frac{r_2}{4}\theta^2 + \frac{r_3}{4}\theta^3 = \\ &= \left(q_0 + \frac{r_0}{4}\right) + \left(q_1 + \frac{r_1}{4}\right)\theta + \left(q_2 + \frac{r_2}{4}\right)\theta^2 + \left(q_3 + \frac{r_3}{3}\right)\theta^3.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3\}$ para $i = 0,1,2,3$. Suponhamos que para $z_0, z_1, z_2, z_3 \in \mathbb{Z}$, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\left(\frac{\theta^2-1}{2}\right) + z_3\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right) \\ &= \left(z_0 - \frac{z_2}{2} + \frac{z_3}{4}\right) + \left(z_1 + \frac{z_3}{4}\right)\theta + \left(\frac{z_2}{2} + \frac{z_3}{4}\right)\theta^2 + \left(\frac{z_3}{4}\right)\theta^3.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 - \frac{z_2}{2} + \frac{z_3}{4} &= q_0 + \frac{r_0}{4}\ (1), \\ z_1 + \frac{z_3}{4} &= q_1 + \frac{r_1}{4}\ (2), \\ \frac{z_2}{2} + \frac{z_3}{4} &= q_2 + \frac{r_2}{4}\ (3) \text{ e} \\ \frac{z_3}{4} &= q_3 + \frac{r_3}{4}\ (4). \end{aligned}$$

Logo, conjunto $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3\}$, para $i = 0,1,2,3$, segue que o conjunto citado é base integral se tivermos

(a) De (4), segue que $z_3 = 4q_3 + r_3$. Assim,

$$\boxed{r_3 = 0, 1, 2 \text{ ou } 3.}$$

(b) De (3) e (4), segue que $z_2 = 2q_2 - 2q_3 + \frac{r_2 - r_3}{2}$. Assim,

$$\boxed{r_2 \equiv r_3 (mod\ 2).}$$

(c) De (2) e (4), segue que $z_1 = q_1 - q_3 + \frac{r_1 - r_3}{4}$. Assim,

$$\boxed{r_1 = r_3.}$$

(d) De (1), (3) e (4), segue que $r_0 = q_0 + q_2 - 2q_3 + \frac{r_0 - 2r_3 + r_2}{4}$. Assim,

$$\boxed{r_0 \equiv 2r_3 - r_2 (mod\ 4).}$$

Assim, as soluções possíveis são $(0,0,0,0)$, $(0,2,0,2)$, $(2,0,2,0)$, $(2,2,2,2)$, $(1,1,1,1)$, $(3,1,3,1)$, $(1,3,1,3)$ e $(3,3,3,3)$.

Nos itens (1), (2) e (3) encontramos 8 soluções. Ao substituir essas soluções nas Equações (5.5), (5.6) e (5.7) encontramos as equivalências de d módulo 4 de modo que $\omega_1, \omega_2, \omega_3 \in \mathbb{Z}$. Essa análise será descrita na seguinte Tabela (5.1).

Tabela 5.1: $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$, d livre de quadrados - casos para análise de $\mathcal{O}_\mathbb{K}$.

r_0	r_1	r_2	r_3	ω_1	ω_2	ω_3	$d \equiv (?)(mod\ 8)$
0	0	0	0	0	0	0	$\forall d$
0	2	0	2	$-d$	0	$\frac{-d(1-d)^2}{16}$	$d \equiv 1, 5 (mod\ 8)$
2	0	2	0	$\frac{3-d}{2}$	$\frac{1-d}{2}$	$\frac{(1-d)^2}{16}$	$d \equiv 1, 5 (mod\ 8)$
2	2	2	2	$\frac{3(1-d)}{2}$	$\frac{(1-d)^2}{2}$	$\frac{(1-d)^3}{16}$	$d \equiv 1, 5 (mod\ 8)$
1	1	1	1	$\frac{3(1-d)}{8}$	$\frac{(1-d)^2}{16}$	$\frac{(1-d)^3}{256}$	$d \equiv 1 (mod\ 8)$
3	1	3	1	$\frac{27-11d}{8}$	$\frac{3(9-10d+d^2)}{16}$	$\frac{81-163d+83d^2-d^3}{16}$	$d \equiv 1 (mod\ 8)$
1	3	1	3	$\frac{3-19d}{8}$	$\frac{1-10d+9d^2}{16}$	$\frac{1-83d+163d^2-81d^3}{256}$	$d \equiv 1 (mod\ 8)$
3	3	3	3	$\frac{27(1-d)}{8}$	$\frac{27(1-d)^2}{16}$	$\frac{81(1-d)^3}{256}$	$d \equiv 1 (mod\ 8)$

Fonte: Elaborada pela autora.

Na Tabela (5.1), a célula "$\forall d$" não inclui as equivalências não livre de quadrados, uma vez que d é livre de quadrados. Para estabelecer o anel dos inteiros algébricos, relacionamos as informações obtidas das possíveis bases integrais nos itens (1), (2) e (3) com as informações da Tabela (5.1). Logo, seguem as observações

1. Para $d \not\equiv 1, 5(mod\ 8)$ exclusivamente, a solução é $(0, 0, 0, 0)$. Para esta solução a base integral é
$$\left\{1, \theta, \theta^2, \theta^3\right\}.$$

2. Para $d \equiv 5(mod\ 8)$ exclusivamente, as soluções são $(0, 2, 0, 2)$, $(2, 2, 0, 2)$ e $(2, 2, 2, 2)$. Para estas soluções a base integral é dada por
$$\left\{1, \theta, \frac{\theta^2 - 1}{2}, \frac{1 + \theta + \theta^2 + \theta^3}{2}\right\}.$$

3. Para $d \equiv 1(mod\ 8)$ exclusivamente, as soluções são $(1, 1, 1, 1)$, $(1, 3, 1, 3)$ e $(3, 3, 3, 3)$. Para estas soluções a base integral é dada por
$$\left\{1, \theta, \frac{\theta^2 - 1}{2}, \frac{1 + \theta + \theta^2 + \theta^3}{4}\right\}.$$

Portanto, o anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3, \text{ se } d \not\equiv 1, 5(mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right), \text{ se } d \equiv 5(mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{ se } d \equiv 1(mod\ 8). \end{cases}$$

o que prova o teorema. □

Exemplo 5.3.2. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[4]{7}$. Como $d = 7$ e $7 \not\equiv 1, 5(mod\ 8)$, pelo Teorema 5.3.1, segue que o anel dos inteiros algébricos desse caso é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3$.*

5.3.2 Norma, traço e discriminante em $\mathbb{Q}(\sqrt[4]{d})$

Nesta seção, apresentamos a norma, o traço e o discriminante em $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$, com d um inteiro livre de quadrados.

Proposição 5.3.2. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[4]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. O traço de α é calculado por*
$$\mathcal{T}r(\alpha) = 4a_0.$$

Demonstração. Na Proposição 5.3.1, calculamos o polinômio característico de α e assim pela Observação 2.3.6, segue que
$$\mathcal{T}r(\alpha) = 4a_0,$$
o que prova a proposição. □

Proposição 5.3.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[4]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. A norma de α é calculada por*

$$\mathcal{N}(\alpha) = a_0^4 - (a_1^4 - 4a_0a_1^2a_2 + 2a_0^2a_2^2 + 4a_0^2a_1a_3)d + (a_2^4 - 4a_1a_2^2a_3 + 2a_1^2a_3^2 + 4a_0a_2a_3^2)d^2 - a_3^4d^3.$$

Demonstração. Na Proposição 5.3.1, calculamos o polinômio característico de α e assim pela Observação 2.3.6, segue que:

$$\mathcal{N}(\alpha) = a_0^4 - (a_1^4 - 4a_0a_1^2a_2 + 2a_0^2a_2^2 + 4a_0^2a_1a_3)d + (a_2^4 - 4a_1a_2^2a_3 + 2a_1^2a_3^2 + 4a_0a_2a_3^2)d^2 - a_3^4d^3$$

o que prova a proposição. □

Exemplo 5.3.3. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[4]{7}$ e $\alpha = 1 + 2(\sqrt[4]{7})^3 \in \mathbb{K}$.*

a) Pela Proposição 5.3.2, segue que o traço de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 2$ e $d = 7$ e substituição direta. Logo, $\mathcal{T}r(\alpha) = 4$.

b) Pela Proposição 5.3.3, segue que a norma de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 0$, $a_2 = 0$ e $d = 7$ e substituição direta. Logo, $\mathcal{N}(\alpha) = -5487$.

Proposição 5.3.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[4]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O discriminante do anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -256d^3, \text{ se } d \not\equiv 1, 5 (mod\ 8) \\ -16d^3, \text{ se } d \equiv 5 (mod\ 8) \\ -4d^3, \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Demonstração. Pelo Teorema 5.3.1, segue que o anel dos inteiros $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3, \text{ se } d \not\equiv 1, 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right), \text{ se } d \equiv 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Assim, a base integral (base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$) admite as possibilidades:

1. Se $d \not\equiv 1, 5 (mod\ 8)$, então uma base integral é $\{1, \theta, \theta^2, \theta^3\}$.
2. Se $d \equiv 5 (mod\ 8)$, então uma base integral é $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{2}\right\}$.
3. Se $d \equiv 1 (mod\ 8)$, então uma base integral é $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}\right\}$.

Pela Proposição 2.6.8, segue que

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, 3, \\ 4d^s, \text{ se } k = 4s, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > 4 \text{ e } k \not\equiv 0 (mod\ 4). \end{cases} \tag{5.9}$$

Logo, $\mathcal{T}r(1) = 4$, $\mathcal{T}r(\theta) = 0$, $\mathcal{T}r(\theta^2) = 0$, $\mathcal{T}r(\theta^3) = 0$, $\mathcal{T}r(d) = 4d$, $\mathcal{T}r(\theta^5) = 0$ e $\mathcal{T}r(\theta^6) = 0$. Agora, analisamos o discriminante para cada possibilidade da base integral.

1. Se $d \not\equiv 1, 5(mod\ 8)$, então uma base é $\{1, \theta, \theta^2, \theta^3\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (5.9), segue que

$$\mathcal{D}(1,\theta,\theta^2,\theta^3) = \det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(d) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(d) & \mathcal{T}r(\theta^5) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(d) & \mathcal{T}r(\theta^5) & \mathcal{T}r(\theta^6) \end{pmatrix} = \det\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4d \\ 0 & 0 & 4d & 0 \\ 0 & 4d & 0 & 0 \end{pmatrix}$$
$$= (-1)^{1+1}.4.\det\begin{pmatrix} 0 & 0 & 4d \\ 0 & 4d & 0 \\ 4d & 0 & 0 \end{pmatrix} = -256d^3.$$

2. Se $d \equiv 5(mod\ 8)$, então uma base é $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{2}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (5.9), segue que
$\mathcal{D}\left(1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{2}\right) =$

$$\det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r\left(\frac{\theta^2-1}{2}\right) & \mathcal{T}r\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \left(\frac{\theta^3-\theta}{2}\right) & \mathcal{T}r\left(\frac{\theta+\theta^2+\theta^3+d}{2}\right) \\ \mathcal{T}r\left(\frac{\theta^2-1}{2}\right) & \mathcal{T}r\left(\frac{\theta^3-\theta}{2}\right) & \mathcal{T}r\left(\frac{d-2\theta^2+1}{4}\right) & \mathcal{T}r\left(\frac{-1-\theta+d+\theta^5}{4}\right) \\ \mathcal{T}r\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right) & \mathcal{T}r\left(\frac{\theta+\theta^2+\theta^3+d}{2}\right) & \mathcal{T}r\left(\frac{-1-\theta+d+\theta^5}{4}\right) & \mathcal{T}r\left(\frac{1+2\theta+3\theta^2+4\theta^3+3d+2\theta^5+\theta^6}{4}\right) \end{pmatrix}$$
$$= \det\begin{pmatrix} 4 & 0 & -2 & 2 \\ 0 & 0 & 0 & 2d \\ -2 & 0 & d+1 & d-1 \\ 2 & 2d & d-1 & 1+3d \end{pmatrix} = (-1)^{2+4}.2d.\det\begin{pmatrix} 4 & 0 & -2 \\ -2 & 0 & d+1 \\ 2 & 2d & d-1 \end{pmatrix} = -16d^3.$$

3. Se $d \equiv 1(mod\ 8)$, então uma base é $\left\{1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (5.9), segue que
$\mathcal{D}\left(1, \theta, \frac{\theta^2-1}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}\right) =$

$$\det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r\left(\frac{\theta^2-1}{2}\right) & \mathcal{T}r\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \left(\frac{\theta^3-\theta}{2}\right) & \mathcal{T}r\left(\frac{\theta+\theta^2+\theta^3+d}{4}\right) \\ \mathcal{T}r\left(\frac{\theta^2-1}{2}\right) & \mathcal{T}r\left(\frac{\theta^3-\theta}{2}\right) & \mathcal{T}r\left(\frac{d-2\theta^2+1}{4}\right) & \mathcal{T}r\left(\frac{-1-\theta+d+\theta^5}{8}\right) \\ \mathcal{T}r\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right) & \mathcal{T}r\left(\frac{\theta+\theta^2+\theta^3+d}{4}\right) & \mathcal{T}r\left(\frac{-1-\theta+d+\theta^5}{8}\right) & \mathcal{T}r\left(\frac{1+2\theta+3\theta^2+4\theta^3+3d+2\theta^5+\theta^6}{16}\right) \end{pmatrix}$$
$$= \det\begin{pmatrix} 4 & 0 & -2 & 1 \\ 0 & 0 & 0 & d \\ -2 & 0 & d+1 & \frac{d-1}{2} \\ 1 & d & \frac{d-1}{2} & \frac{1+3d}{4} \end{pmatrix} = (-1)^{2+4}.d.\det\begin{pmatrix} 4 & 0 & -2 \\ -2 & 0 & d+1 \\ 1 & d & \frac{d-1}{2} \end{pmatrix} = -4d^3.$$

Logo, da análise dos itens (1) e (2), segue que

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -256d^3, \text{ se } d \not\equiv 1, 5(mod\ 8) \\ -16d^3, \text{ se } d \equiv 5(mod\ 8) \\ -4d^3, \text{ se } d \equiv 1(mod\ 8). \end{cases}$$

o que prova a proposição. □

Exemplo 5.3.4. *Seja* $\mathbb{K} = Q(\theta)$*, com* $\theta = \sqrt[4]{7}$*. Como* $d = 7$ *e* $7 \not\equiv 1, 5(mod\ 8)$*, pela Proposição 5.3.4, segue que o discriminante é dado por* $\mathcal{D}(\mathbb{K}) = -256 \times 7^3 = -87808$*.*

Observação 5.3.1. *Para* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números, onde* $\theta = \sqrt[4]{d}$*, com* $d \in \mathbb{Z}$ *livre de quadrados, podemos calcular o discriminante da base potente* $\{1, \theta, \theta^2, \theta^3\}$ *através do polinômio minimal* $p(x) = x^4 - d$*, e assim, utilizando o Corolário 2.5.4, segue que*

$$\mathcal{D}(1, \theta, \theta^2, \theta^3) = (-1)^{\frac{4^2+4+2}{2}}[4^4 d^{4-1}] = -256d^3.$$

6 Extensões Quínticas

Os corpos quínticos $\mathbb{K}$ são corpos de números providos de uma extensão quíntica, ou seja, $[\mathbb{K} : \mathbb{Q}] = 5$. Neste capítulo, exploramos alguns corpos quínticos, pois diferentemente do Capítulo 3 onde estudamos os corpos quadráticos, não é tão simples identificar o elemento primitivo dos corpos quínticos. Dessa forma, a complexidade do caso geral nos leva a focar em casos particulares. Por isso, chamamos a atenção para os corpos quínticos nos quais o elemento primitivo tem como polinômio minimal $p(x) = x^5 - d$, com d um inteiro livre de quadrados. O nosso objetivo é descobrir o anel dos inteiros algébricos desses corpos quínticos, neste caso, a referência [9] apresenta apenas o polinômio característico e estimula trabalho futuros, então o teorema que contém a base integral descrito neste capítulo é de nossa autoria, não conhecido na literatura. Como aplicação direta, apresentamos também a norma e traço de um elemento desses corpos quínticos e o discriminante da base integral. Este capítulo foi inspirado pelas referências [7], [8] e [9].

6.1 Corpos quínticos

Nesta seção, apresentamos as extensões quintas e alguns conceitos básicos e propriedades.

Definição 6.1.1. *Seja $\mathbb{K}$ um corpo de números, com o grau da extensão $[\mathbb{K} : \mathbb{Q}] = 5$.*

1. *O corpo de números $\mathbb{K}$ é chamado de **corpo quíntico**.*
2. *A extensão de corpos $\mathbb{Q} \subseteq \mathbb{K}$ é chamada de **extensão quinta**.*
3. *O polinômio $p(x) \in \mathbb{Q}[x]$, cujo grau é $\partial(p) = 5$, é chamado de **quinta**.*

Consideramos $\mathbb{K}$ um corpo quíntico, e assim, o grau da extensão é $[\mathbb{K} : \mathbb{Q}] = 5$. Pelo Teorema do Elemento Primitivo, segue que existe $\theta \in \mathbb{C}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$, ou seja, θ é o elemento primitivo de $\mathbb{K}$. Seja $p(y) = y^5 + a_4y^4 + a_3y^3 + a_2y^2 + a_1y + a_0$ o polinômio minimal de θ sobre $\mathbb{Q}$. A ideia é melhorar $p(y)$ reduzindo algum coeficiente, por isso faremos a seguinte mudança de variável $y = x - l$, ou seja,

$$\begin{aligned} p(x-l) &= (x-l)^5 + a_4(x-l)^4 + a_3(x-l)^3 + a_2(x-l)^2 + a_1(x-l) + a_0 = \\ &= x^5 + (-5l + a_4)x^4 + (10l^2 - 4a_4l + a_3)x^3 + (-10l^3 + 6a_4l^2 - 3a_3l + a_2)x^2 + \\ &+ (5l^4 - 4a_4l^3 + 3a_3l^2 - 2a_2l + a_1)x + (-l^5 + a_4l^4 - a_3l^3 + a_2l^2 - a_1l + a_0). \end{aligned}$$

Vamos cancelar o coeficiente $-5l + a_4$, e para isso, tomamos $l = \dfrac{a_4}{5} \in \mathbb{Q}$. Fazendo as substituições, segue que os coeficientes restantes são $b_3 = -\dfrac{2a_4^2}{5} + a_3$, $b_2 = \dfrac{4a_4^3}{25} - \dfrac{3a_3a_4}{5} + a_2$,

$b_1 = -\frac{3a_4^4}{125} + \frac{3a_3a_4^2}{25} - \frac{2a_2a_4}{5} + a_1$ e $b_0 = \frac{4a_4^5}{3125} - \frac{a_3a_4^2}{125} + \frac{a_2a_4^2}{25} - \frac{a_1a_4}{5} + a_0$ com $b_0, b_1, b_2, b_3 \in \mathbb{Q}$. Portanto, sem perda de generalidade, consideramos $p(x) = x^5 + b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{Q}[x]$. Um fato interessante é que $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\theta - l)$, uma vez que que $l \in \mathbb{Q}$.

O ambiente desenvolvido expressa o seguinte campo para trabalho: Seja $\mathbb{K}$ um corpo quíntico e $\theta \in \mathbb{C}$ o seu elemento primitivo, e assim, $\mathbb{K} = \mathbb{Q}(\theta)$. Consideramos θ um inteiro algébrico e pelas considerações anteriores o seu polinômio minimal pode ser escrito da forma $p(x) = x^5 + b_3x^3 + b_2x^2 + b_1x + b_0$, com $b_0, b_1, b_2, b_3 \in \mathbb{Z}$.

6.2 A quinta $p(x) = x^5 + ax + b$

Nesta seção, consideramos $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 5, onde a quinta $p(x) = x^5 + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, é o polinômio minimal do elemento primitivo θ. O objetivo é descobrir o anel dos inteiros desses corpos de números através do discriminante.

Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_\mathbb{K}$. E mais, pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4) = (-1)^{\frac{5(5-1)}{2}}[5^5b^{5-1} + (-1)^{5+1}(5-1)^{5-1}a^5] = 256a^5 + 3125b^4.$$

Assim, $\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4) = 256a^5 + 3125b^4$. Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 | a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}\}.$$

Exemplo 6.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 5 tal que $p(x) = x^5 - x - 1$ é o polinômio minimal do elemento primitivo θ. Como*

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4) = 256(-1)^5 + 3125(-1)^4 = 2869 \text{ e}$$

$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4) = 2869 = 19 \times 151$ *é livre de quadrados (19 e 151 são primos), segue que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$.*

6.3 A quinta $p(x) = x^5 - d$, com d livre de quadrados

Nessa seção, sejam $\mathbb{K}$ um corpo de números e $p(x) = x^5 - d$ uma quinta, com $d \in \mathbb{Z}$ livre de quadrados. O elemento $\sqrt[5]{d}$ é um inteiro algébrico, pois $p(x)$ é o seu polinômio minimal em $\mathbb{Z}$. Pela Teoria de Corpos, segue que $[\mathbb{Q}(\sqrt[5]{d}) : \mathbb{Q}] = \partial(p) = 5$, e assim, $\mathbb{Q}(\sqrt[5]{d})$ é um corpo quíntico. Para este estudo, trabalhamos com os corpos quínticos da forma $\mathbb{K} = \mathbb{Q}(\sqrt[5]{d})$ cujo elemento primitivo é o próprio $\sqrt[5]{d}$. Salvo menção contrária, chamamos $\theta = \sqrt[5]{d}$ o elemento primitivo, com $d \in \mathbb{Z}$ livre de quadrados e o corpo quíntico em questão é o $\mathbb{K} = Q(\theta)$.

Retomando as Proposições 2.6.4 e 2.6.5, sejam θ, $\theta\xi_5$ e $\theta\xi_5^2$, $\theta\xi_5^3$ e $\theta\xi_5^4$ as raízes do polinômio $p(x)$, onde ξ_5^k são as raízes primitivas das unidade para $i = 0, 1, 2, 3, 4$. Como

$$\xi_5^k = e^{\frac{2\pi i}{5}k} = \cos\left(\frac{2k\pi}{5}\right) + i\,\text{sen}\left(\frac{2k\pi}{5}\right)$$

segue que $\xi_5^0 = 1$, $\xi_5^1 = \frac{-1+\sqrt{5}}{4} + i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}$, $\xi_5^2 = \frac{-1-\sqrt{5}}{4} + i\sqrt{\frac{5}{8}-\frac{\sqrt{5}}{8}}$, $\xi_5^3 = \frac{-1-\sqrt{5}}{4} - i\sqrt{\frac{5}{8}-\frac{\sqrt{5}}{8}}$ e $\xi_5^4 = \frac{-1+\sqrt{5}}{4} - i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}$, onde $\xi_5^1 + \xi_5^2 + \xi_5^3 + \xi_5^4 = -1$.

Pelo Teorema 2.3.2, podemos considerar σ_k os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_k(\theta) = \theta\xi_5^{k-1}$, com $i = 1, 2, 3, 4, 5$. Portanto, os $\mathbb{Q}$-monomorfismos em θ são definidos por $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \theta\xi_5$, $\sigma_3(\theta) = \theta\xi_5^2$, $\sigma_4(\theta) = \theta\xi_5^3$ e $\sigma_5(\theta) = \theta\xi_5^4$. Pela Teoria do Corpos, segue que o conjunto $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim, podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4$, onde $a_i \in \mathbb{Q}$ para $i = 0, 1, 2, 3, 4$.

6.3.1 O anel dos inteiros de $\mathbb{Q}(\sqrt[5]{d})$

Seguindo as notações anteriores, vamos encontrar o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K} = \mathbb{Q}(\theta)$ (sobre $\mathbb{Z}$). Desse modo, inicialmente, faremos uma preparação através do próximo resultado, para identificar o anel dos inteiros algébricos de $\mathcal{O}_\mathbb{K}$.

Proposição 6.3.1. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[5]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}$. O polinômio característico de α é dado por:*

$$\begin{aligned} f_\alpha(x) = x^5 &- x^4[5a_0] + x^3[5(2a_0^2 - (a_2a_3 + a_1a_4)d)] - x^2[5(2a_0^3 + (-3a_0a_2a_3 - \\ &- 3a_0a_1a_4 + a_1a_2^2 + a_1^2a_3)d + (a_3^2a_4 + a_2a_4^2)d^2)] + x[5(a_0^4 + (-3a_0^2a_2a_3 - \\ &- 3a_0^2a_1a_4 + 2a_0a_1a_2^2 + 2a_0a_1^2a_3 - a_1^3a_2)d + (2a_0a_3^2a_4 + 2a_0a_2a_4^2 + a_1^2a_4^2 - \\ &- a_1a_3^3 - a_1a_2a_3a_4 + a_2^2a_3^2 - a_2^3a_4)d^2 + (-a_3a_4^3)d^3)] - [a_0^5 + (-5a_0^3a_2a_3 - \\ &- 5a_0^3a_1a_4 + 5a_0^2a_1a_2^2 + 5a_0^2a_1^2a_3 - 5a_0a_1^3a_2 + a_1^5)d + (5a_0^2a_3^2a_4 + 5a_0^2a_2a_4^2 + \\ &+ 5a_0a_1^2a_4^2 - 5a_0a_1a_3^3 - 5a_0a_1a_2a_3a_4 + 5a_0a_2^2a_3^2 - 5a_0a_2^3a_4 - 5a_1^3a_3a_4 + \\ &+ 5a_1^2a_2a_3^2 + 5a_1^2a_2^2a_4 - 5a_1a_2^3a_3 + a_2^5)d^2 + (-5a_0a_3a_4^3 + 5a_1a_3^2a_4^2 - \\ &- 5a_1a_2a_4^3 + a_3^5 - 5a_2a_3^3a_4 + 5a_2^2a_3a_4^2)d^3 + (a_4^5)d^4]. \end{aligned} \tag{6.1}$$

Demonstração. Consideramos $\alpha_i = \sigma_i(\alpha)$, com $i = 1, 2, 3, 4, 5$. Assim,

$$\begin{aligned} \alpha_1 &= a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4, \\ \alpha_2 &= a_0 + a_1\theta\xi_5 + a_2\theta^2\xi_5^2 + a_3\theta^3\xi_5^3 + a_4\theta^4\xi_5^4, \\ \alpha_3 &= a_0 + a_1\theta\xi_5^2 + a_2\theta^2\xi_5^4 + a_3\theta^3\xi_5 + a_4\theta^4\xi_5^3, \\ \alpha_4 &= a_0 + a_1\theta\xi_5^3 + a_2\theta^2\xi_5 + a_3\theta^3\xi_5^4 + a_4\theta^4\xi_5^2 \text{ e} \\ \alpha_5 &= a_0 + a_1\theta\xi_5^4 + a_2\theta^2\xi_5^3 + a_3\theta^3\xi_5^2 + a_4\theta^4\xi_5. \end{aligned}$$

Pela Proposição 2.3.4, segue que o polinômio característico de α é dado por

$$\begin{aligned} f_\alpha(x) &= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5) = \\ &= x^5 - x^4(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5) + x^3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \\ &+ \alpha_3\alpha_4 + \alpha_1\alpha_5 + \alpha_2\alpha_5 + \alpha_3\alpha_5 + \alpha_4\alpha_5) - x^2(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_2\alpha_5 + \alpha_1\alpha_3\alpha_4 + \\ &+ \alpha_1\alpha_3\alpha_5 + \alpha_1\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_5 + \alpha_2\alpha_4\alpha_5 + \alpha_3\alpha_4\alpha_5) + x(\alpha_1\alpha_2\alpha_3\alpha_4 + \\ &+ \alpha_1\alpha_2\alpha_3\alpha_5 + \alpha_1\alpha_2\alpha_4\alpha_5 + \alpha_1\alpha_3\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4\alpha_5) - (\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5). \end{aligned}$$

Lembramos que $\xi_5+\xi_5^2+\xi_5^3+\xi_5^4=-1$. Com o auxílio do programa Wolfram Mathematica 11.3, ao desenvolvermos os coeficientes, obtemos

$\rightarrow\ \alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5=5a_0.$

$\rightarrow\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4+\alpha_3\alpha_4+\alpha_1\alpha_5+\alpha_2\alpha_5+\alpha_3\alpha_5+\alpha_4\alpha_5=$
$=5(2a_0^2-(a_2a_3+a_1a_4)d).$

$\rightarrow\ \alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_2\alpha_5+\alpha_1\alpha_3\alpha_4+\alpha_1\alpha_3\alpha_5+\alpha_1\alpha_4\alpha_5+\alpha_2\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_5+$
$+\alpha_2\alpha_4\alpha_5+\alpha_3\alpha_4\alpha_5=5(2a_0^3+(-3a_0a_2a_3-3a_0a_1a_4+a_1a_2^2+a_1^2a_3)d+(a_3^2a_4+$
$+a_2a_4^2)d^2).$

$\rightarrow\ \alpha_1\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_3\alpha_5+\alpha_1\alpha_2\alpha_4\alpha_5+\alpha_1\alpha_3\alpha_4\alpha_5+\alpha_2\alpha_3\alpha_4\alpha_5=5(a_0^4+(-3a_0^2a_2a_3-$
$-3a_0^2a_1a_4+2a_0a_1a_2^2+2a_0a_1^2a_3-a_1^3a_2)d+(2a_0a_3^2a_4+2a_0a_2a_4^2+a_1^2a_4^2-a_1a_3^3-$
$-a_1a_2a_3a_4+a_2^2a_3^2-a_2^3a_4)d^2+(-a_3a_4^3)d^3).$

$\rightarrow\ \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5=a_0^5+(-5a_0^3a_2a_3-5a_0^3a_1a_4+5a_0^2a_1a_2^2+5a_0^2a_1^2a_3-5a_0a_1^3a_2+a_1^5)d+$
$+(5a_0^2a_3^2a_4+5a_0^2a_2a_4^2+5a_0a_1^2a_4^2-5a_0a_1a_3^3-5a_0a_1a_2a_3a_4+5a_0a_2^2a_3^2-5a_0a_2^3a_4-$
$-5a_1^3a_3a_4+5a_1^2a_2a_3^2+5a_1^2a_2^2a_4-5a_1a_2^3a_3+a_2^5)d^2+(-5a_0a_3a_4^3+5a_1a_3^2a_4^2-$
$-5a_1a_2a_4^3+a_3^5-5a_2a_3^3a_4+5a_2^2a_3a_4^2)d^3+(a_4^5)d^4.$

Assim,

$$\begin{aligned}f_\alpha(x)=x^5-x^4[5a_0]+x^3[5(2a_0^2-(a_2a_3+a_1a_4)d)]-x^2[5(2a_0^3+(-3a_0a_2a_3-\\-3a_0a_1a_4+a_1a_2^2+a_1^2a_3)d+(a_3^2a_4+a_2a_4^2)d^2)]+x[5(a_0^4+(-3a_0^2a_2a_3-\\-3a_0^2a_1a_4+2a_0a_1a_2^2+2a_0a_1^2a_3-a_1^3a_2)d+(2a_0a_3^2a_4+2a_0a_2a_4^2+a_1^2a_4^2-\\-a_1a_3^3-a_1a_2a_3a_4+a_2^2a_3^2-a_2^3a_4)d^2+(-a_3a_4^3)d^3)]-[a_0^5+(-5a_0^3a_2a_3-\\-5a_0^3a_1a_4+5a_0^2a_1a_2^2+5a_0^2a_1^2a_3-5a_0a_1^3a_2+a_1^5)d+(5a_0^2a_3^2a_4+5a_0^2a_2a_4^2+\\+5a_0a_1^2a_4^2-5a_0a_1a_3^3-5a_0a_1a_2a_3a_4+5a_0a_2^2a_3^2-5a_0a_2^3a_4-5a_1^3a_3a_4+\\+5a_1^2a_2a_3^2+5a_1^2a_2^2a_4-5a_1a_2^3a_3+a_2^5)d^2+(-5a_0a_3a_4^3+5a_1a_3^2a_4^2-\\-5a_1a_2a_4^3+a_3^5-5a_2a_3^3a_4+5a_2^2a_3a_4^2)d^3+(a_4^5)d^4],\end{aligned}$$

o que prova a proposição. □

Exemplo 6.3.1. *Seja $\mathbb{K}=Q(\theta)$, com $\theta=\sqrt[5]{7}$ e $\alpha=2+3(\sqrt[5]{7})^3\in\mathbb{K}$. Pela Proposição 6.3.1, segue que o polinômio característico de α é calculado através da identificação dos valores $a_0=2$, $a_1=0$, $a_2=0$, $a_3=3$, $a_4=0$ e $d=7$ e substituição direta. Logo,*

$$f_\alpha(x)=x^5-10x^4+40x^3-80x^2+160x-83381.$$

Com este resultado, podemos enunciar e demonstrar o teorema que caracterizará o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$. O teorema a seguir, é uma das nossas contribuições deste trabalho e apresenta um resultado novo de nossa autoria, não conhecido na literatura.

Teorema 6.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[5]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -7 (mod\ 25). \end{cases}$$

Demonstração. Suponhamos que $\alpha \in \mathbb{K}$ um inteiro algébrico e vamos explorar quais são as formas que α pode assumir. Para isso, lembramos que $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4$, com $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}$. Pela Proposição 2.6.9, se α é um inteiro algébrico, então $5a_0, 5a_1, 5a_2, 5a_3, 5a_4 \in \mathbb{Z}$. Vamos supor $5a_i = p_i$, com $p_i \in \mathbb{Z}$ para todo $i = 0, 1, 2, 3, 4$. Assim,

$$a_i = \frac{p_i}{5}, \text{ para todo } i = 0, 1, 2, 3, 4.$$

Além do mais, p_i pode ser escrito da seguinte forma

$$p_i = 5q_i + r_i,$$

com $q_i, r_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4\}$, para $i = 0, 1, 2, 3, 4$. Reescrevendo α, segue que

$$\begin{aligned} \alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 &= \frac{p_0}{5} + \frac{p_1}{5}\theta + \frac{p_2}{5}\theta^2 + \frac{p_3}{5}\theta^3 + \frac{p_4}{5}\theta^4 = \\ &= \frac{5q_0 + r_0}{5} + \frac{5q_1 + r_1}{5}\theta + \frac{5q_2 + r_2}{5}\theta^2 + \frac{5q_3 + r_3}{5}\theta^3 + \frac{5q_4 + r_4}{5}\theta^4 = \\ &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4. \end{aligned}$$

Logo,

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4. \tag{6.2}$$

Agora, como $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2) e $q = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 \in \mathcal{O}_\mathbb{K}$, segue que

$$\begin{aligned} &\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 \in \mathcal{O}_\mathbb{K} \Leftrightarrow \\ &\Leftrightarrow r = \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 \in \mathcal{O}_\mathbb{K}. \end{aligned}$$

Assim, α é um inteiro algébrico se, e somente se, r é um inteiro algébrico. Consequentemente,

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow r \in \mathcal{O}_\mathbb{K}. \tag{6.3}$$

Novamente por esses dois resultados (Proposição 6.3.1 e Proposição 2.3.3), segue que

$r \in \mathcal{O}_{\mathbb{K}}$ se, e somente se,

$$\begin{cases} 5[\frac{r_0}{5}] \in \mathbb{Z} \\ 5[\frac{2r_0^2}{25} - (\frac{r_2r_3}{25} + \frac{r_1r_4}{25})d] \in \mathbb{Z}, \\ 5[\frac{2r_0^3}{125} + (-\frac{3r_0r_2r_3}{125} - \frac{3r_0r_1r_4}{125} + \frac{r_1r_2^2}{125} + \frac{r_1^2r_3}{125})d + (\frac{r_3^2r_4}{125} + \frac{r_2r_4^2}{125})d^2] \in \mathbb{Z}, \\ 5[\frac{r_0^4}{625} + (-\frac{3r_0^2r_2r_3}{625} - \frac{3r_0^2r_1r_4}{625} + \frac{2r_0r_1r_2^2}{625} + \frac{2r_0r_1^2r_3}{625} - \frac{r_1^3r_2}{625})d + (\frac{2r_0r_3^2r_4}{625} + \\ +\frac{2r_0r_2r_4^2}{625} + \frac{r_1^2r_4^2}{625} - \frac{r_1r_3^3}{625} - \frac{r_1r_2r_3r_4}{625} + \frac{r_2^2r_3^2}{625} - \frac{r_2^3r_4}{625})d^2 + (-\frac{r_3r_4^3}{625})d^3] \in \mathbb{Z} \text{ e} \\ \frac{r_0^5}{3125} + (-\frac{5r_0^3r_2r_3}{3125} - \frac{5r_0^3r_1r_4}{3125} + \frac{5r_0^2r_1r_2^2}{3125} + \frac{5r_0^2r_1^2r_3}{3125} - \frac{5r_0r_1^3r_2}{3125} + \frac{r_1^5}{3125})d + \\ +(\frac{5r_0^2r_3^2r_4}{3125} + \frac{5r_0^2r_2r_4^2}{3125} + \frac{5r_0r_1^2r_4^2}{3125} - \frac{5r_0r_1r_3^3}{3125} - \frac{5r_0r_1r_2r_3r_4}{3125} + \frac{5r_0r_2^2r_3^2}{3125} - \frac{5r_0r_2^3r_4}{3125} - \\ -\frac{5r_1^3r_3r_4}{3125} + \frac{5r_1^2r_2r_3^2}{3125} + \frac{5r_1^2r_2^2r_4}{3125} - \frac{5r_1r_2^3r_3}{3125} + \frac{r_2^5}{3125})d^2 + (-\frac{5r_0r_3r_4^3}{3125} + \frac{5r_1r_3^2r_4^2}{3125} - \\ -\frac{5r_1r_2r_4^3}{3125} + \frac{r_3^5}{3125} - \frac{5r_2r_3^3r_4}{3125} + \frac{5r_2^2r_3r_4^2}{3125})d^3 + (\frac{r_4^5}{3125})d^4 \in \mathbb{Z}. \end{cases} \tag{6.4}$$

Renomeando as expressões obtidas, segue

$$\omega_1 = \frac{2r_0^2 - (r_2r_3 + r_1r_4)d}{5}. \tag{6.5}$$

$$\omega_2 = \frac{2r_0^3 + (-3r_0r_2r_3 - 3r_0r_1r_4 + r_1r_2^2 + r_1^2r_3)d + (r_3^2r_4 + r_2r_4^2)d^2}{25}. \tag{6.6}$$

$$\begin{aligned} \omega_3 = &\frac{r_0^4 + (-3r_0^2r_2r_3 - 3r_0^2r_1r_4 + 2r_0r_1r_2^2 + 2r_0r_1^2r_3 - r_1^3r_2)d + (2r_0r_3^2r_4)d^2}{125} + \\ &+ \frac{(2r_0r_2r_4^2 + r_1^2r_4^2 - r_1r_3^3 - r_1r_2r_3r_4 + r_2^2r_3^2 - r_2^3r_4)d^2 + (-r_3r_4^3)d^3}{125}. \end{aligned} \tag{6.7}$$

$$\begin{aligned} \omega_4 = &\frac{r_0^5 + (-5r_0^3r_2r_3 - 5r_0^3r_1r_4 + 5r_0^2r_1r_2^2 + 5r_0^2r_1^2r_3 - 5r_0r_1^3r_2 + r_1^5)d}{3125} + \\ &+ \frac{(5r_0^2r_3^2r_4 + 5r_0^2r_2r_4^2 + 5r_0r_1^2r_4^2 - 5r_0r_1r_3^3 - 5r_0r_1r_2r_3r_4 + 5r_0r_2^2r_3^2)d^2}{3125} + \\ &+ \frac{(-5r_0r_2^3r_4 - 5r_1^3r_3r_4 + 5r_1^2r_2r_3^2 + 5r_1^2r_2^2r_4 - 5r_1r_2^3r_3 + r_2^5)d^2}{3125} + \\ &+ \frac{(-5r_0r_3r_4^3 + 5r_1r_3^2r_4^2 - 5r_1r_2r_4^3 + r_3^5 - 5r_2r_3^3r_4 + 5r_2^2r_3r_4^2)d^3 + (r_4^5)d^4}{3125}. \end{aligned} \tag{6.8}$$

Das implicações na Expressão (6.3) e na Expressão (6.4), segue que

$$\alpha \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \omega_1, \omega_2, \omega_3, \omega_4 \in \mathbb{Z}. \tag{6.9}$$

De acordo com os parâmetros $r_0, r_1, r_2, r_3, r_4 \in \{0, 1, 2, 3, 4\}$, segue que este caso se trata da análise de 3125 possibilidades. Mas, por este resultado se tratar de uma equivalência biunívoca, vamos encontrar somente as possibilidades que são soluções da forma $s_j = (r_0, r_1, r_2, r_3, r_4)$, para algum j. Agora, vamos mostrar que a base integral é dada por $\{1, \theta, \theta^2, \theta^3, \theta^4\}$, $\left\{1, \theta, \theta^2, \theta^3, \frac{1 + \theta + \theta^2 + \theta^3 + \theta^4}{5}\right\}$, $\left\{1, \theta, \theta^2, \theta^3, \frac{1 + 4\theta + \theta^2 + 4\theta^3 + \theta^4}{5}\right\}$, $\left\{1, \theta, \theta^2, \theta^3, \frac{1 + 3\theta + 4\theta^2 + 2\theta^3 + \theta^4}{5}\right\}$ ou $\left\{1, \theta, \theta^2, \theta^3, \frac{1 + 2\theta + 4\theta^2 + 3\theta^3 + \theta^4}{5}\right\}$ e também para quais valores de r_i's isso é verídico, com $i = 0, 1, 2, 3, 4$.

1. Valores de r_i's para que a base integral seja $\{1, \theta, \theta^2, \theta^3, \theta^4\}$. Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (6.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 = \\ &= \left(q_0 + \frac{r_0}{5}\right) + \left(q_1 + \frac{r_1}{5}\right)\theta + \left(q_2 + \frac{r_2}{5}\right)\theta^2 + \left(q_3 + \frac{r_3}{5}\right)\theta^3 + \left(q_4 + \frac{r_4}{5}\right)\theta^4.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4\}$ para $i = 0, 1, 2, 3, 4$. Agora, suponhamos que para z_0, z_1, z_2, z_3, z_4 quaisquer, α pode ser escrito como

$$\alpha = z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\theta^4.$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned}z_0 &= q_0 + \frac{r_0}{5}\ (1),\\ z_1 &= q_1 + \frac{r_1}{5}\ (2),\\ z_2 &= q_2 + \frac{r_2}{5}\ (3),\\ z_3 &= q_3 + \frac{r_3}{5}\ (4)\text{ e}\\ z_4 &= q_4 + \frac{r_4}{5}\ (5).\end{aligned}$$

Logo, o conjunto $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0, 1, 2, 3, 4\}$, para $i = 0, 1, 2, 3, 4$, segue que o conjunto citado é base integral se tivermos

   (a) De (1), então $r_0 = 0$,
   (b) De (2), então $r_1 = 0$,
   (c) De (3), então $r_2 = 0$,
   (d) De (4), então $r_3 = 0$ e
   (e) De (5), então $r_4 = 0$.

Assim, a solução possível é $s_1 = (0, 0, 0, 0, 0)$.

2. Valores de r_i's para que a base integral seja $\left\{1, \theta, \theta^2, \theta^3, \dfrac{1 + \theta + \theta^2 + \theta^3 + \theta^4}{5}\right\}$. Neste caso, consideramos α que o elemento genérico que escolhemos inicialmente. Pela Equação (6.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 = \\ &= \left(q_0 + \frac{r_0}{5}\right) + \left(q_1 + \frac{r_1}{5}\right)\theta + \left(q_2 + \frac{r_2}{5}\right)\theta^2 + \left(q_3 + \frac{r_3}{5}\right)\theta^3 + \left(q_4 + \frac{r_4}{5}\right)\theta^4.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4\}$ para $i = 0, 1, 2, 3, 4$. Suponhamos que para z_0, z_1, z_2, z_3, z_4 quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\left(\frac{1 + \theta + \theta^2 + \theta^3 + \theta^4}{5}\right)\\ &= \left(z_0 + \frac{z_4}{5}\right) + \left(z_1 + \frac{z_4}{5}\right)\theta + \left(z_2 + \frac{z_4}{5}\right)\theta^2 + \left(z_3 + \frac{z_4}{5}\right)\theta^3 + \left(\frac{z_4}{5}\right)\theta^4.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_4}{5} &= q_0 + \frac{r_0}{5} \ (1), \\ z_1 + \frac{z_4}{5} &= q_1 + \frac{r_1}{5} \ (2), \\ z_2 + \frac{z_4}{5} &= q_2 + \frac{r_2}{5} \ (3), \\ z_3 + \frac{z_4}{5} &= q_3 + \frac{r_3}{5} \ (4) \text{ e} \\ \frac{z_4}{5} &= q_4 + \frac{r_4}{5} \ (5), \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \theta^3, \dfrac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3,4\}$, para $i = 0,1,2,3,4$, segue que o conjunto citado é base integral se tivermos

(a) De (5), segue que $z_4 = 5q_4 + r_4$. Assim,

$$\boxed{r_4 = 0, 1, 2, 3 \text{ ou } 4.}$$

(b) De (4) e (5), segue que $z_3 = q_3 - q_4 + \dfrac{r_3 - r_4}{5}$. Assim,

$$\boxed{r_3 = r_4.}$$

(c) De (3) e (5), segue que $z_2 = q_2 - q_4 + \dfrac{r_2 - r_4}{5}$. Assim,

$$\boxed{r_2 = r_4.}$$

(d) De (2) e (5), segue que $z_1 = q_1 - q_4 + \dfrac{r_1 - r_4}{5}$. Assim,

$$\boxed{r_1 = r_4.}$$

(e) De (1) e (5), segue que $z_0 = q_0 - q_4 + \dfrac{r_0 - r_4}{5}$. Assim,

$$\boxed{r_0 = r_4.}$$

Assim, as soluções possíveis são $s_1 = (0,0,0,0,0)$, $s_2 = (1,1,1,1,1)$, $s_3 = (2,2,2,2,2)$, $s_4 = (3,3,3,3,3)$ e $s_5 = (4,4,4,4,4)$.

3. Valores de r_i's para que a base integral seja $\left\{1, \theta, \theta^2, \theta^3, \dfrac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right\}$.
Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (6.2), segue que

$$\begin{aligned} \alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 = \\ &= \left(q_0 + \frac{r_0}{5}\right) + \left(q_1 + \frac{r_1}{5}\right)\theta + \left(q_2 + \frac{r_2}{5}\right)\theta^2 + \left(q_3 + \frac{r_3}{5}\right)\theta^3 + \left(q_4 + \frac{r_4}{5}\right)\theta^4. \end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4\}$ para $i = 0, 1, 2, 3, 4$. Suponhamos que para z_0, z_1, z_2, z_3, z_4 quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\left(\frac{1 + 4\theta + \theta^2 + 4\theta^3 + \theta^4}{5}\right) \\ &= \left(z_0 + \frac{z_4}{5}\right) + \left(z_1 + \frac{4z_4}{5}\right)\theta + \left(z_2 + \frac{z_4}{5}\right)\theta^2 + \left(z_3 + \frac{4z_4}{5}\right)\theta^3 + \left(\frac{z_4}{5}\right)\theta^4.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_4}{5} &= q_0 + \frac{r_0}{5}\ (1), \\ z_1 + \frac{4z_4}{5} &= q_1 + \frac{r_1}{5}\ (2), \\ z_2 + \frac{z_4}{5} &= q_2 + \frac{r_2}{5}\ (3), \\ z_3 + \frac{4z_4}{5} &= q_3 + \frac{r_3}{5}\ (4) \text{ e} \\ \frac{z_4}{5} &= q_4 + \frac{r_4}{5}\ (5), \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \theta^3, \dfrac{1 + 4\theta + \theta^2 + 4\theta^3 + \theta^4}{5}\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0, 1, 2, 3, 4\}$, para $i = 0, 1, 2, 3, 4$, analisamos para quais condições o conjunto citado é uma base integral.

(a) De (5), segue que $z_4 = 5q_4 + r_4$. Assim,

$$\boxed{r_4 = 0, 1, 2, 3 \text{ ou } 4.}$$

(b) De (4) e (5), segue que $z_3 = q_3 - 4q_4 + \dfrac{r_3 - 4r_4}{5}$. Assim,

$$\boxed{r_3 \equiv 4r_4 (mod\ 5).}$$

(c) De (3) e (5), segue que $z_2 = q_2 - q_4 + \dfrac{r_2 - r_4}{5}$. Assim,

$$\boxed{r_2 = r_4.}$$

(d) De (2) e (5), segue que $z_1 = q_1 - 4q_4 + \dfrac{r_1 - 4r_4}{5}$. Assim,

$$\boxed{r_1 \equiv 4r_4 (mod\ 5).}$$

(e) De (1) e (5), segue que $z_0 = q_0 - q_4 + \dfrac{r_0 - r_4}{5}$. Assim,

$$\boxed{r_0 = r_4.}$$

Assim, as soluções possíveis são $s_1 = (0, 0, 0, 0, 0)$, $s_6 = (1, 4, 1, 4, 1)$, $s_7 = (2, 3, 2, 3, 2)$, $s_8 = (3, 2, 3, 2, 3)$ e $s_9 = (4, 1, 4, 1, 4)$.

4. Valores de r_i's para que a base integral seja $\left\{1, \theta, \theta^2, \theta^3, \frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right\}$.
Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (6.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 = \\ &= \left(q_0 + \frac{r_0}{5}\right) + \left(q_1 + \frac{r_1}{5}\right)\theta + \left(q_2 + \frac{r_2}{5}\right)\theta^2 + \left(q_3 + \frac{r_3}{5}\right)\theta^3 + \left(q_4 + \frac{r_4}{5}\right)\theta^4.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3,4\}$ para $i = 0,1,2,3,4$. Suponhamos que para z_0, z_1, z_2, z_3, z_4 quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\left(\frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right) \\ &= \left(z_0 + \frac{z_4}{5}\right) + \left(z_1 + \frac{3z_4}{5}\right)\theta + \left(z_2 + \frac{4z_4}{5}\right)\theta^2 + \left(z_3 + \frac{2z_4}{5}\right)\theta^3 + \left(\frac{z_4}{5}\right)\theta^4.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_4}{5} &= q_0 + \frac{r_0}{5}\ (1), \\ z_1 + \frac{3z_4}{5} &= q_1 + \frac{r_1}{5}\ (2), \\ z_2 + \frac{4z_4}{5} &= q_2 + \frac{r_2}{5}\ (3), \\ z_3 + \frac{2z_4}{5} &= q_3 + \frac{r_3}{5}\ (4) \text{ e} \\ \frac{z_4}{5} &= q_4 + \frac{r_4}{5}\ (5), \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \theta^3, \frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3,4\}$, para $i = 0,1,2,3,4$, segue que o conjunto citado é base integral se tivermos

(a) De (5), segue que $z_4 = 5q_4 + r_4$. Assim,

$$\boxed{r_4 = 0, 1, 2, 3 \text{ ou } 4.}$$

(b) De (4) e (5), segue que $z_3 = q_3 - 2q_4 + \frac{r_3 - 2r_4}{5}$. Assim,

$$\boxed{r_3 \equiv 2r_4 (mod\ 5).}$$

(c) De (3) e (5), segue que $z_2 = q_2 - 4q_4 + \frac{r_2 - 4r_4}{5}$. Assim,

$$\boxed{r_2 \equiv 4r_4 (mod\ 5).}$$

(d) De (2) e (5), segue que $z_1 = q_1 - 3q_4 + \frac{r_1 - 3r_4}{5}$. Assim,

$$\boxed{r_1 \equiv 3r_4 (mod\ 5).}$$

(e) De (1) e (5), segue que $z_0 = q_0 - q_4 + \dfrac{r_0 - r_4}{5}$. Assim,

$$\boxed{r_0 = r_4.}$$

Assim, as soluções possíveis são dadas por $s_1 = (0,0,0,0,0)$, $s_{10} = (1,3,4,2,1)$, $s_{11} = (2,1,3,4,2)$, $s_{12} = (3,4,2,1,3)$ e $s_{13} = (4,2,1,3,4)$.

5. Valores de r_i's para que a base integral seja $\left\{1, \theta, \theta^2, \theta^3, \dfrac{1 + 2\theta + 4\theta^2 + 3\theta^3 + \theta^4}{5}\right\}$.

Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (6.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4 = \\ &= \left(q_0 + \frac{r_0}{5}\right) + \left(q_1 + \frac{r_1}{5}\right)\theta + \left(q_2 + \frac{r_2}{5}\right)\theta^2 + \left(q_3 + \frac{r_3}{5}\right)\theta^3 + \left(q_4 + \frac{r_4}{5}\right)\theta^4.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3,4\}$ para $i = 0,1,2,3,4$. Suponhamos que para z_0, z_1, z_2, z_3, z_4 quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\left(\frac{1 + 2\theta + 4\theta^2 + 3\theta^3 + \theta^4}{5}\right) \\ &= \left(z_0 + \frac{z_4}{5}\right) + \left(z_1 + \frac{2z_4}{5}\right)\theta + \left(z_2 + \frac{4z_4}{5}\right)\theta^2 + \left(z_3 + \frac{3z_4}{5}\right)\theta^3 + \left(\frac{z_4}{5}\right)\theta^4.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_4}{5} &= q_0 + \frac{r_0}{5}\ (1), \\ z_1 + \frac{2z_4}{5} &= q_1 + \frac{r_1}{5}\ (2), \\ z_2 + \frac{4z_4}{5} &= q_2 + \frac{r_2}{5}\ (3), \\ z_3 + \frac{3z_4}{5} &= q_3 + \frac{r_3}{5}\ (4) \text{ e} \\ \frac{z_4}{5} &= q_4 + \frac{r_4}{5}\ (5), \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \theta^3, \dfrac{1 + 2\theta + 4\theta^2 + 3\theta^3 + \theta^4}{5}\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3,4\}$, para $i = 0,1,2,3,4$, segue que o conjunto citado é base integral se tivermos

(a) De (5), segue que $z_4 = 5q_4 + r_4$. Assim,

$$\boxed{r_4 = 0, 1, 2, 3 \text{ ou } 4.}$$

(b) De (4) e (5), segue que $z_3 = q_3 - 3q_4 + \dfrac{r_3 - 3r_4}{5}$. Assim,

$$\boxed{r_3 \equiv 3r_4 (mod\ 5).}$$

(c) De (3) e (5), segue que $z_2 = q_2 - 4q_4 + \dfrac{r_2 - 4r_4}{5}$. Assim,

$$\boxed{r_2 \equiv 4r_4 \mod 5.}$$

(d) De (2) e (5), segue que $z_1 = q_1 - 2q_4 + \dfrac{r_1 - 2r_4}{5}$. Assim,

$$\boxed{r_1 \equiv 2r_4 (mod\ 5).}$$

(e) De (1) e (5), segue que $z_0 = q_0 - q_4 + \dfrac{r_0 - r_4}{5}$. Assim,

$$\boxed{r_0 = r_4.}$$

Assim, as soluções possíveis são dadas por $s_1 = (0,0,0,0,0)$, $s_{14} = (1,2,4,3,1)$, $s_{15} = (2,4,3,1,2)$, $s_{16} = (3,1,2,4,3)$ e $s_{17} = (4,3,1,2,4)$.

Nos itens (1), (2), (3), (4) e (5) encontramos 17 soluções da forma $s_j = (r_0, r_1, r_2, r_3, r_4)$, com $j = 1, 2, \ldots, 17$. Ao substituir essas soluções nas Equações (6.5), (6.6), (6.7) e (6.8) encontraremos as equivalências de d módulo 25 de modo que $\omega_1, \omega_2, \omega_3, \omega_4 \in \mathbb{Z}$. Essa análise será descrita na Tabela (6.1).

Tabela 6.1: $\mathbb{K} = \mathbb{Q}(\sqrt[5]{d})$, d livre de quadrados - casos para análise de $\mathcal{O}_{\mathbb{K}}$.

s_j	ω_1	ω_2	ω_3	ω_4	$d \equiv (?)$
s_1	0	0	0	0	$\forall d$
s_2	$\frac{2(1-d)}{5}$	$\frac{2(1-d)^2}{25}$	$\frac{(1-d)^3}{125}$	$\frac{(1-d)^4}{3125}$	$d \equiv 1$
s_3	$\frac{8(1-d)}{5}$	$\frac{16(1-d)^2}{25}$	$\frac{16(1-d)^3}{125}$	$\frac{32(1-d)^4}{3215}$	$d \equiv 1$
s_4	$\frac{18(1-d)}{5}$	$\frac{54(1-d)^2}{25}$	$\frac{81(1-d)^3}{125}$	$\frac{243(1-d)^4}{3125}$	$d \equiv 1$
s_5	$\frac{32(1-d)}{5}$	$\frac{128(1-d)^2}{25}$	$\frac{256(1-d)^3}{125}$	$\frac{1024(1-d)^4}{3125}$	$d \equiv 1$
s_6	$\frac{2(1-4d)}{5}$	$\frac{2+44d+17d^2}{25}$	$\frac{1+48d-207d^2-4d^3}{125}$	$\frac{1+1004d-1119d^2+1004d^3+d^4}{3125}$	$d \equiv -1$
s_7	$\frac{4(2-3d)}{5}$	$\frac{16-33d+26d^2}{25}$	$\frac{16-42d+43d^2-24d^3}{125}$	$\frac{32+3d-58d^2+3d^3+32d^4}{3125}$	$d \equiv -1$
s_8	$\frac{6(3-2d)}{5}$	$\frac{54-82d+39d^2}{25}$	$\frac{81-192d+173d^2-54d^3}{125}$	$\frac{243-778d+1083d^2-778d^3+243d^4}{3125}$	$d \equiv -1$
s_9	$\frac{8(4-d)}{5}$	$\frac{128-79d+68d^2}{25}$	$\frac{256-252d+303d^2-64d^3}{125}$	$\frac{1024-1279d+1644d^2-1279d^3+1024d^4}{3125}$	$d \equiv -1$
s_{10}	$\frac{2-11d}{5}$	$\frac{2+33d+8d^2}{25}$	$\frac{1-9d-23d^2-2d^3}{125}$	$\frac{1-22d+119d^2+22d^3+d^4}{3125}$	$d \equiv 7$
s_{11}	$\frac{2(4-7d)}{5}$	$\frac{16-71d+44d^2}{25}$	$\frac{16-119d+182d^2-32d^3}{125}$	$\frac{32-329d+933d^2-296d^3+32d^4}{3125}$	$d \equiv 7$
s_{12}	$\frac{2(9-7d)}{5}$	$\frac{54-94d+21d^2}{25}$	$\frac{81-314d+222d^2-27d^3}{125}$	$\frac{243-1346d+2417d^2-1154d^3+243d^4}{3125}$	$d \equiv 7$
s_{13}	$\frac{32-11d}{5}$	$\frac{2(64-59d+26d^2)}{25}$	$\frac{256-424d+407d^2-192d^3}{125}$	$\frac{1024-2528d+3731d^2-3097d^3+1024d^4}{3125}$	$d \equiv 7$
s_{14}	$\frac{2(1-7d)}{5}$	$\frac{2+2d+13d^2}{25}$	$\frac{1+14d+32d^2-3d^3}{125}$	$\frac{1+22d+119d^2-22d^3+d^4}{3125}$	$d \equiv -7$
s_{15}	$\frac{8-11d}{5}$	$\frac{2(8-7d+7d^2)}{25}$	$\frac{16-116d+47d^2-8d^3}{125}$	$\frac{32-296d+933d^2-329d^3+32d^4}{3125}$	$d \equiv -7$
s_{16}	$\frac{18-11d}{5}$	$\frac{54-91d+66d^2}{25}$	$\frac{81-251d+357d^2-108d^3}{125}$	$\frac{243-1154d+2417d^2-1346d^3+243d^4}{3125})$	$d \equiv -7$
s_{17}	$\frac{2(16-7d)}{5}$	$\frac{128-147d+32d^2}{25}$	$\frac{256-531d+352d^2-128d^3}{125}$	$\frac{1024-3097d+3731d^2-2528d^3+1024d^4}{3125}$	$d \equiv -7$

Fonte: Elaborada pela autora.

Na Tabela (6.1), a célula "$\forall d$" não inclui as equivalências não livre de quadrados, uma vez que d é livre de quadrados. Para estabelecer o anel dos inteiros algébricos, relacionaremos as informações obtidas das possíveis bases integrais nos itens (1), (2), (3), (4) e (5) com as informações da Tabela (6.1). Logo,

1. Para $d \not\equiv \pm 1, \pm 7 (mod\ 25)$ exclusivamente, a solução é s_1. Para esta solução a base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \theta^4\right\}.$$

2. Para $d \equiv 1 (mod\ 25)$ exclusivamente, as soluções são s_2, s_3, s_4 e s_5. Para estas soluções a base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right\}.$$

3. Para $d \equiv -1 (mod\ 25)$ exclusivamente, as soluções são s_6, s_7, s_8 e s_9. Para estas soluções a base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \frac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right\}.$$

4. Para $d \equiv 7 (mod\ 25)$ exclusivamente, as soluções são s_{10}, s_{11}, s_{12} e s_{13}. Para estas soluções a base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right\}.$$

5. Para $d \equiv -7 (mod\ 25)$ exclusivamente, as soluções são s_{14}, s_{15}, s_{16} e s_{17}. Para estas soluções a base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \frac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}\right\}.$$

Portanto, o anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -7 (mod\ 25), \end{cases}$$

o que prova o teorema. □

Exemplo 6.3.2. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[5]{7}$. Como $d = 7$ e $7 \equiv 7 (mod\ 25)$, pelo Teorema 6.3.1, segue que o anel dos inteiros algébricos desse caso é dada por*

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right).$$

6.3.2 Norma, traço e discriminante em $\mathbb{Q}(\sqrt[5]{d})$

Nesta seção, apresentamos a norma, o traço e o discriminante em $\mathbb{K} = \mathbb{Q}(\sqrt[5]{d})$, com d um inteiro livre de quadrados.

Proposição 6.3.2. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[5]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}$. O traço de α é calculado por*

$$\mathcal{T}r(\alpha) = 5a_0.$$

Demonstração. Na Proposição 6.3.1, calculamos o polinômio característico de α e assim pela Observação 2.3.6, segue que

$$\mathcal{T}r(\alpha) = 5a_0,$$

o que prova a proposição. □

Proposição 6.3.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[5]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}$. A norma de α é calculada por*

$$\begin{aligned}\mathcal{N}(\alpha) = {} & a_0^5 + (-5a_0^3a_2a_3 - 5a_0^3a_1a_4 + 5a_0^2a_1a_2^2 + 5a_0^2a_1^2a_3 - 5a_0a_1^3a_2 + a_1^5)d + \\ & + (5a_0^2a_3^2a_4 + 5a_0^2a_2a_4^2 + 5a_0a_1^2a_4^2 - 5a_0a_1a_3^3 - 5a_0a_1a_2a_3a_4 + 5a_0a_2^2a_3^2 - 5a_0a_2^3a_4 - \\ & - 5a_1^3a_3a_4 + 5a_1^2a_2a_3^2 + 5a_1^2a_2^2a_4 - 5a_1a_2^3a_3 + a_2^5)d^2 + (-5a_0a_3a_4^3 + 5a_1a_3^2a_4^2 - \\ & - 5a_1a_2a_4^3 + a_3^5 - 5a_2a_3^3a_4 + 5a_2^2a_3a_4^2)d^3 + (a_4^5)d^4.\end{aligned}$$

Demonstração. Na proposição 6.3.1, calculamos o polinômio característico de α e assim pela Observação 2.3.6, segue que

$$\begin{aligned}\mathcal{N}(\alpha) = {} & a_0^5 + (-5a_0^3a_2a_3 - 5a_0^3a_1a_4 + 5a_0^2a_1a_2^2 + 5a_0^2a_1^2a_3 - 5a_0a_1^3a_2 + a_1^5)d + \\ & + (5a_0^2a_3^2a_4 + 5a_0^2a_2a_4^2 + 5a_0a_1^2a_4^2 - 5a_0a_1a_3^3 - 5a_0a_1a_2a_3a_4 + 5a_0a_2^2a_3^2 - 5a_0a_2^3a_4 - \\ & - 5a_1^3a_3a_4 + 5a_1^2a_2a_3^2 + 5a_1^2a_2^2a_4 - 5a_1a_2^3a_3 + a_2^5)d^2 + (-5a_0a_3a_4^3 + 5a_1a_3^2a_4^2 - \\ & - 5a_1a_2a_4^3 + a_3^5 - 5a_2a_3^3a_4 + 5a_2^2a_3a_4^2)d^3 + (a_4^5)d^4,\end{aligned}$$

o que prova a proposição. □

Exemplo 6.3.3. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[5]{7}$ e $\alpha = 2 + 3(\sqrt[5]{7})^3 \in \mathbb{K}$.*

a) Pela Proposição 6.3.2, segue que o traço de α é calculado através da identificação dos valores $a_0 = 2$, $a_1 = 0$, $a_2 = 0$, $a_3 = 3$, $a_4 = 0$ e $d = 7$ e substituição direta. Logo, $\mathcal{T}r(\alpha) = 10$.

b) Pela Proposição 6.3.3, segue que a norma de α é calculado através da identificação dos valores $a_0 = 2$, $a_1 = 0$, $a_2 = 0$, $a_3 = 3$, $a_4 = 0$ e $d = 7$ e substituição direta. Logo, $\mathcal{N}(\alpha) = 83381$.

Proposição 6.3.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[5]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O discriminante do anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 3125d^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ 125d^4, \text{ se } d \equiv \pm 1, \pm 7 (mod\ 25). \end{cases}$$

Demonstração. Pelo Teorema 6.3.1, segue que o anel dos inteiros $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -7 (mod\ 25). \end{cases}$$

Assim, uma base integral (base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$) admite as possibilidades.

1. Se $d \not\equiv \pm 1, \pm 7 (mod\ 25)$, então uma base integral é $\{1, \theta, \theta^2, \theta^3, \theta^4\}$.
2. Se $d \equiv 1 (mod\ 25)$, então uma base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right\}$.
3. Se $d \equiv -1 (mod\ 25)$, então uma base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right\}$.
4. Se $d \equiv 7 (mod\ 25)$, então uma base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right\}$.
5. Se $d \equiv -7 (mod\ 25)$, então uma base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}\right\}$.

Pela Proposição 2.6.8, segue que

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, 3, 4 \\ 5d^s, \text{ se } k = 5s, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > 5 \text{ e } k \not\equiv 0 (mod\ 5). \end{cases} \tag{6.10}$$

Logo, $\mathcal{T}r(1) = 5$, $\mathcal{T}r(\theta) = 0$, $\mathcal{T}r(\theta^2) = 0$, $\mathcal{T}r(\theta^3) = 0$, $\mathcal{T}r(\theta^4) = 0$, $\mathcal{T}r(d) = 5d$, $\mathcal{T}r(\theta^6) = 0$, $\mathcal{T}r(\theta^7) = 0$ e $\mathcal{T}r(\theta^8) = 0$. Agora, analisamos o discriminante para cada possibilidade da base integral.

1. Se $d \not\equiv \pm 1, \pm 7 (mod\ 25)$, então uma base é $\{1, \theta, \theta^2, \theta^3, \theta^4\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (6.10), segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4) = \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) & \mathcal{T}r(\theta^7) \\ \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) & \mathcal{T}r(\theta^7) & \mathcal{T}r(\theta^8) \end{pmatrix}$$

$$= \det \begin{pmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5d \\ 0 & 0 & 0 & 5d & 0 \\ 0 & 0 & 5d & 0 & 0 \\ 0 & 5d & 0 & 0 & 0 \end{pmatrix} = (-1)^{1+1}.5.\det \begin{pmatrix} 0 & 0 & 0 & 5d \\ 0 & 0 & 5d & 0 \\ 0 & 5d & 0 & 0 \\ 5d & 0 & 0 & 0 \end{pmatrix}$$

$$= 5.(-1)^{1+4}.5d \det \begin{pmatrix} 0 & 0 & 5d \\ 0 & 5d & 0 \\ 5d & 0 & 0 \end{pmatrix} = 3125d^4.$$

2. Se $d \equiv 1, (mod\ 25)$, então uma base é $\{1, \theta, \theta^2, \theta^3, \beta_1\}$, onde $\beta_1 = \frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (6.10), segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \beta_1) = \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\beta_1) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta\beta_1) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^2\beta_1) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) & \mathcal{T}r(\theta^3\beta_1) \\ \mathcal{T}r(\beta_1) & \mathcal{T}r(\theta\beta_1) & \mathcal{T}r(\theta^2\beta_1) & \mathcal{T}r(\theta^3\beta_1) & \mathcal{T}r(\beta_1^2) \end{pmatrix}$$

$$= \det\begin{pmatrix} 5 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & d \\ 0 & 0 & 0 & 5d & d \\ 0 & 0 & 5d & 0 & d \\ 1 & d & d & d & 1+4d \end{pmatrix} = (-1)^{2+5}.d.\det\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5d \\ 0 & 0 & 5d & 0 \\ 1 & d & d & d \end{pmatrix}$$

$$= (-d).(-1)^{1+1}.5.\det\begin{pmatrix} 0 & 0 & 5d \\ 0 & 5d & 0 \\ d & d & d \end{pmatrix} = 125d^4.$$

3. Se $d \equiv -1, (mod\, 25)$, então uma base é $\{1, \theta, \theta^2, \theta^3, \beta_2\}$, onde $\beta_2 = \dfrac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (6.10), segue que

$$\mathcal{D}(1,\theta,\theta^2,\theta^3,\beta_2) = \det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\beta_2) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta\beta_2) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^2\beta_2) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) & \mathcal{T}r(\theta^3\beta_2) \\ \mathcal{T}r(\beta_2) & \mathcal{T}r(\theta\beta_2) & \mathcal{T}r(\theta^2\beta_2) & \mathcal{T}r(\theta^3\beta_2) & \mathcal{T}r(\beta_2^2) \end{pmatrix}$$

$$= \det\begin{pmatrix} 5 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & d \\ 0 & 0 & 0 & 5d & 4d \\ 0 & 0 & 5d & 0 & d \\ 1 & d & 4d & d & 1+16d \end{pmatrix} = (-1)^{2+5}.d.\det\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5d \\ 0 & 0 & 5d & 0 \\ 1 & d & 4d & d \end{pmatrix}$$

$$= (-d).(-1)^{1+1}.5.\det\begin{pmatrix} 0 & 0 & 5d \\ 0 & 5d & 0 \\ d & 4d & d \end{pmatrix} = 125d^4.$$

4. Se $d \equiv 7, (mod\, 25)$, então uma base é $\{1, \theta, \theta^2, \theta^3, \beta_3\}$, onde $\beta_3 = \dfrac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (6.10), segue que

$$\mathcal{D}(1,\theta,\theta^2,\theta^3,\beta_3) = \det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\beta_3) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta\beta_3) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^2\beta_3) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) & \mathcal{T}r(\theta^3\beta_3) \\ \mathcal{T}r(\beta_3) & \mathcal{T}r(\theta\beta_3) & \mathcal{T}r(\theta^2\beta_3) & \mathcal{T}r(\theta^3\beta_3) & \mathcal{T}r(\beta_3^2) \end{pmatrix}$$

$$= \det\begin{pmatrix} 5 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & d \\ 0 & 0 & 0 & 5d & 2d \\ 0 & 0 & 5d & 0 & 4d \\ 1 & d & 2d & 4d & 1+22d \end{pmatrix} = (-1)^{2+5}.d.\det\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5d \\ 0 & 0 & 5d & 0 \\ 1 & d & 2d & 4d \end{pmatrix}$$

$$= (-d).(-1)^{1+1}.5.\det\begin{pmatrix} 0 & 0 & 5d \\ 0 & 5d & 0 \\ d & 2d & 4d \end{pmatrix} = 125d^4.$$

5. Se $d \equiv -7(mod\ 25)$, então uma base é dada por $\{1, \theta, \theta^2, \theta^3, \beta_4\}$, onde $\beta_4 = \dfrac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}$. Assim, usando as propriedades de traço e as informações

obtidas da Equação (6.10), segue que

$$\mathcal{D}(1,\theta,\theta^2,\theta^3,\beta_4) = \det\begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\beta_4) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta\beta_4) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^2\beta_4) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(d) & \mathcal{T}r(\theta^6) & \mathcal{T}r(\theta^3\beta_4) \\ \mathcal{T}r(\beta_4) & \mathcal{T}r(\theta\beta_4) & \mathcal{T}r(\theta^2\beta_4) & \mathcal{T}r(\theta^3\beta_4) & \mathcal{T}r(\beta_4^2) \end{pmatrix}$$

$$= \det\begin{pmatrix} 5 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & d \\ 0 & 0 & 0 & 5d & 3d \\ 0 & 0 & 5d & 0 & 4d \\ 1 & d & 3d & 4d & 1+28d \end{pmatrix} = (-1)^{2+5}.d.\det\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5d \\ 0 & 0 & 5d & 0 \\ 1 & d & 3d & 4d \end{pmatrix}$$

$$= (-d).(-1)^{1+1}.5.\det\begin{pmatrix} 0 & 0 & 5d \\ 0 & 5d & 0 \\ d & 3d & 4d \end{pmatrix} = 125d^4.$$

Logo, da análise dos itens (1), (2), (3), (4) e (5), segue que

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 3125d^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ 125d^4, \text{ se } d \equiv \pm 1, \pm 7 (mod\ 25), \end{cases}$$

o que prova a proposição. □

Exemplo 6.3.4. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[5]{7}$. Como $d = 7$ e $7 \equiv 7(mod\ 25)$, pela Proposição 6.3.4, segue que o discriminante é dado por $\mathcal{D}(\mathbb{K}) = 125 \times 7^4 = 300125$.*

Observação 6.3.1. *Para $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[5]{d}$, com $d \in \mathbb{Z}$ livre de quadrados, podemos calcular o discriminante da base potente $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ através do polinômio minimal $p(x) = x^5 - d$, e assim, utilizando o Corolário 2.5.4, segue que*

$$\mathcal{D}(1,\theta,\theta^2,\theta^3,\theta^4) = (-1)^{\frac{5^2+5+2}{2}}[5^5 d^{5-1}] = 3125d^4.$$

7 Extensões Sêxticas

Os corpos sêxticos $\mathbb{K}$ são corpos de números providos de uma extensão sêxtica, ou seja, $[\mathbb{K} : \mathbb{Q}] = 6$. Neste capítulo, apresentamos alguns corpos sêxticos, pois diferentemente do Capítulo 3 onde estudamos os corpos quadráticos, não é tão simples identificar o elemento primitivo dos corpos sêxticos. Dessa forma, a complexidade do caso geral nos leva a focar em casos particulares. Por isso, exploramos os corpos sêxticos nos quais o elemento primitivo tem como polinômio minimal $p(x) = x^6 - d$, com d um inteiro livre de quadrados. O nosso objetivo é descobrir o anel dos inteiros algébricos desses corpos sêxticos, neste caso, a proposição que descreve o polinômio característico e o teorema que contém a base integral descrito neste capítulo são de nossa autoria, não conhecidos na literaturas. Como aplicação direta, apresentamos também a norma e traço de um elemento desses corpos sêxticos e o discriminante da base integral. Este capítulo foi inspirado pelas referências [7], [8] e [9].

7.1 Corpos sêxticos

Nesta seção, apresentamos as extensões sêxticas e alguns conceitos básicos e propriedades.

Definição 7.1.1. *Seja $\mathbb{K}$ um corpo de números, com o grau da extensão $[\mathbb{K} : \mathbb{Q}] = 6$.*

1. *O corpo de números $\mathbb{K}$ é chamado de **corpo sêxtico**.*
2. *A extensão de corpos $\mathbb{Q} \subseteq \mathbb{K}$ é chamada de **extensão sêxtica**.*
3. *O polinômio $p(x) \in \mathbb{Q}[x]$, cujo grau é $\partial(p) = 6$, é chamado de **sexta**.*

Consideramos $\mathbb{K}$ um corpo sêxtico, e assim, o grau da extensão é $[\mathbb{K} : \mathbb{Q}] = 6$. Pelo Teorema do Elemento Primitivo, segue que existe $\theta \in \mathbb{C}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$, ou seja, θ é o elemento primitivo de $\mathbb{K}$. Seja $p(y) = y^6 + a_5y^5 + a_4y^4 + a_3y^3 + a_2y^2 + a_1y + a_0$ o polinômio minimal de θ sobre $\mathbb{Q}$. A ideia é melhorar $p(y)$ reduzindo algum coeficiente, e para isso faremos a seguinte mudança de variável $y = x - l$. Assim,

$$\begin{aligned} p(x-l) &= (x-l)^6 + a_5(x-l)^5 + a_4(x-l)^4 + a_3(x-l)^3 + a_2(x-l)^2 + a_1(x-l) + a_0 = \\ &= x^6 + (-6l + a_5)x^5 + (15l^2 - 5a_5l + a_4)x^4 + (-20l^3 + 10a_5l^2 - 4a_4l + a_3)x^3 + \\ &+ (15l^4 - 10a_5l^3 + 6a_4l^2 - 3a_3l + a_2)x^2 + (-6l^5 + 5a_5l^4 - 4a_4l^3 + 3a_3l^2 - \\ &- 2a_2l + a_1)x + (l^6 - a_5l^5 + a_4l^4 - a_3l^3 + a_2l^2 - a_1l + a_0). \end{aligned}$$

Vamos cancelar o coeficiente $-6l + a_5$, e para isso tomamos $l = \dfrac{a_5}{6} \in \mathbb{Q}$. Fazendo as substituições, segue que os coeficientes restantes são $b_4 = -\dfrac{5a_5^2}{12} + a_4$, $b_3 = \dfrac{5a_5^3}{27} -$

$\frac{2a_4a_5}{3} + a_3$, $b_2 = -\frac{5a_5^4}{144} + \frac{a_4a_5^2}{6} - \frac{a_3a_5}{2} + a_2$, $b_1 = \frac{a_5^5}{423} - \frac{1_4 1_5^3}{54} + \frac{a_3a_5^2}{12} - \frac{a_2a_5}{3} + a_1$ e $b_0 = -\frac{5a_5^6}{46656} + \frac{a_4a_5^4}{1296} - \frac{a_3a_5^3}{1296} - \frac{a_3a_5^3}{216} + \frac{a_2a_5^2}{36} - \frac{a_1a_5}{6} + a_0$, com $b_0, b_1, b_2, b_3, b_4 \in \mathbb{Q}$. Portanto, sem perda de generalidade, consideramos $p(x) = x^6 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{Q}[x]$. Um fato interessante é que $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\theta - l)$, desde que $l \in \mathbb{Q}$.

O ambiente desenvolvido expressa o seguinte campo para trabalho: Seja $\mathbb{K}$ um corpo sêxtico e $\theta \in \mathbb{C}$ o seu elemento primitivo, e assim, $\mathbb{K} = \mathbb{Q}(\theta)$. Consideramos θ um inteiro algébrico e pelas considerações anteriores o seu polinômio minimal pode ser escrito da forma $p(x) = x^6 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$, com $b_0, b_1, b_2, b_3, b_4 \in \mathbb{Z}$.

7.2 A sexta $p(x) = x^6 + ax + b$

Nesta seção, consideramos $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 6, onde a sêxtica $p(x) = x^6 + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, é o polinômio minimal do elemento primitivo θ. O objetivo é descobrir o anel dos inteiros desses corpos de números através do discriminante.

Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_\mathbb{K}$. E mais, pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5) = (-1)^{\frac{6(6-1)}{2}}[6^6b^{6-1} + (-1)^{6+1}(6-1)^{6-1}a^6] = 3125a^6 - 46656b^5.$$

Assim, $\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5) = 3125a^6 - 46656b^5$. Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5 | a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}\}.$$

Exemplo 7.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau 6 tal que $p(x) = x^6 - x - 1$ é o polinômio minimal do elemento primitivo θ. Como*

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5) = 3125(-1)^6 - 46656(-1)^5 = 49781 \text{ e}$$

$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5) = 49781 = 67 \times 743$ *é livre de quadrados (67 e 743 são primos), segue que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$.*

7.3 A sexta $p(x) = x^6 - d$, com d livre de quadrados

Nessa seção, sejam $\mathbb{K}$ um corpo de números e $p(x) = x^6 - d$ uma sexta, com $d \in \mathbb{Z}$ livre de quadrados. O elemento $\sqrt[6]{d}$ é um inteiro algébrico, pois $p(x)$ é o seu polinômio minimal em $\mathbb{Z}$. Pela Teoria de Corpos, segue que $[\mathbb{Q}(\sqrt[6]{d}) : \mathbb{Q}] = \partial(p) = 6$, e assim, $\mathbb{Q}(\sqrt[6]{d})$ é um corpo sêxtico. Para este estudo, trabalhamos com os corpos sêxticos da forma $\mathbb{K} = \mathbb{Q}(\sqrt[6]{d})$ cujo elemento primitivo é o próprio $\sqrt[6]{d}$. Salvo menção contrária, chamamos $\theta = \sqrt[6]{d}$ o elemento primitivo, com $d \in \mathbb{Z}$ livre de quadrados e o corpo sêxtico em questão é o $\mathbb{K} = Q(\theta)$.

Retomando as Proposições 2.6.4 e 2.6.5, sejam θ, $\theta\xi_6$ e $\theta\xi_6^2$, $\theta\xi_6^3$, $\theta\xi_6^4$ e $\theta\xi_6^5$ as raízes do polinômio $p(x)$, onde ξ_6^k são as raízes primitivas das unidade para $i = 0, 1, 2, 3, 4, 5$. Como

$$\xi_6^k = e^{\frac{2\pi i}{6}k} = \cos\left(\frac{2k\pi}{6}\right) + i\,\text{sen}\left(\frac{2k\pi}{6}\right),$$

segue que $\xi_6^0 = 1$, $\xi_6^1 = \frac{1+i\sqrt{3}}{2}$, $\xi_6^2 = \frac{-1+i\sqrt{3}}{2}$, $\xi_6^3 = -1$, $\xi_6^4 = \frac{-1-i\sqrt{3}}{2}$ e $\xi_6^5 = \frac{1-i\sqrt{3}}{2}$, e ainda, $\xi_6^1 + \xi_6^2 + \xi_6^3 + \xi_6^4 + \xi_6^5 = -1$.

Pelo Teorema 2.3.2, podemos considerar σ_k os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_k(\theta) = \theta\xi_6^{k-1}$, com $i = 1, 2, 3, 4, 5, 6$. Portanto, os $\mathbb{Q}$-monomorfismos em θ são definidos por $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \theta\xi_6$, $\sigma_3(\theta) = \theta\xi_6^2$, $\sigma_4(\theta) = \theta\xi_6^3$, $\sigma_5(\theta) = \theta\xi_6^4$ e $\sigma_6(\theta) = \theta\xi_6^5$. Pela Teoria de corpos, segue que o conjunto $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim, podemos escrever qualquer $\alpha \in \mathbb{K}$ como $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5$, onde $a_i \in \mathbb{Q}$ para $i = 0, 1, 2, 3, 4, 5$.

7.3.1 O anel dos inteiros de $\mathbb{Q}(\sqrt[6]{d})$

Seguindo as notações da seção, vamos encontrar o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K} = \mathbb{Q}(\theta)$ (sobre $\mathbb{Z}$). Para isso, inicialmente, faremos uma preparação através do próximo resultado, para identificar o anel dos inteiros algébricos de $\mathcal{O}_\mathbb{K}$. A proposição a seguir, é uma das nossas contribuições deste trabalho e apresenta um resultado novo de nossa autoria, não conhecido na literatura.

Proposição 7.3.1. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}$. O polinômio característico de α é dado por*

$$
\begin{aligned}
f_\alpha(x) = {} & x^6 - x^5[6a_0] + x^4[3(5a_0^2 - (a_3^2 + 2a_2a_4 + 2a_1a_5)d)] - x^3[2(10a_0^3 + (a_2^3 + \\
& + 6a_1a_2a_3 - 6a_0a_3^2 + 3a_1^2a_4 - 12a_0a_2a_4 - 12a_0a_1a_5)d + (a_4^3 + 6a_3a_4a_5 + \\
& + 3a_2a_5^2)d^2)] + x^2[3(5a_0^4 + (-3a_1^2a_2^2 + 2a_0a_2^3 - 2a_1^3a_3 + 12a_0a_1a_2a_3 - \\
& - 6a_0^2a_3^2 + 6a_0a_1^2a_4 - 12a_0^2a_2a_4 - 12a_0^2a_1a_5)d + (a_3^4 + 3a_2^2a_4^2 - 6a_1a_3a_4^2 + \\
& + 2a_0a_4^3 - 6a_2^2a_3a_5 + 12a_0a_3a_4a_5 + 3a_1^2a_5^2 + 6a_0a_2a_5^2)d^2 + (-3a_4^2a_5^2 - \\
& - 2a_3a_5^3)d^3)] - x[6(a_0^5 + (a_1^4a_2 - 3a_0a_1^2a_2^2 + a_0^2a_2^3 - 2a_0a_1^3a_3 + 6a_0^2a_1a_2a_3 - \\
& - 2a_0^3a_3^2 + 3a_0^2a_1^2a_4 - 4a_0^3a_2a_4 - 4a_0^3a_1a_5)d + (a_2^3a_3^2 - 2a_1a_2a_3^3 + a_0a_3^4 - \\
& - a_2^4a_4 + 3a_1^2a_3^2a_4 + 3a_0a_2^2a_4^2 - 6a_0a_1a_3a_4^2 + a_0^2a_4^3 + 2a_1a_2^3a_5 - 6a_0a_2^2a_3a_5 - \\
& - 2a_1^3a_4a_5 + 6a_0^2a_3a_4a_5 + 3a_0a_1^2a_5^2 + 3a_0^2a_2a_5^2)d^2 + (a_3^2a_4^3 - a_2a_4^4 - 2a_3^3a_4a_5 + \\
& + 2a_1a_4^3a_5 + 3a_2a_3^2a_5^2 - 3a_0a_4^2a_5^2 - 2a_1a_2a_5^3 - 2a_0a_3a_5^3)d^3 + (a_4a_5^4)d^4)] + \\
& + [a_0^6 + (-a_1^6 + 6a_0a_1^4a_2 - 9a_0^2a_1^2a_2^2 + 2a_0^3a_2^3 - 6a_0^2a_1^3a_3 + 12a_0^3a_1a_2a_3 - \\
& - 3a_0^4a_3^2 + 6a_0^3a_1^2a_4 - 6a_0^4a_2a_4 - 6a_0^4a_1a_5)d + (a_2^6 - 6a_1a_2^4a_3 + 9a_1^2a_2^2a_3^2 + \\
& + 6a_0a_2^3a_3^2 - 2a_1^3a_3^3 - 12a_0a_1a_2a_3^3 + 3a_0^2a_3^4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 - \\
& - 12a_1^3a_2a_3a_4 + 18a_0a_1^2a_3^2a_4 + 3a_1^4a_4^2 + 9a_0^2a_2^2a_4^2 - 18a_0^2a_1a_3a_4^2 + 2a_0^3a_4^3 - \\
& - 6a_1^3a_2^2a_5 + 12a_0a_1a_2^3a_5 + 6a_1^4a_3a_5 - 18a_0^2a_2^2a_3a_5 - 12a_0a_1^3a_4a_5 + \\
& + 12a_0^3a_3a_4a_5 + 9a_0^2a_1^2a_5^2 + 6a_0^3a_2a_5^2)d^2 + (-a_3^6 + 6a_2a_3^4a_4 - 9a_2^2a_3^2a_4^2 - \\
& - 6a_1a_3^3a_4^2 + 2a_2^3a_4^3 + 12a_1a_2a_3a_4^3 + 6a_0a_3^2a_4^3 - 3a_1^2a_4^4 - 6a_0a_2a_4^4 - 6a_2^2a_3^3a_5 + \\
& + 6a_1a_3^4a_5 + 12a_2^3a_3a_4a_5 - 12a_0a_3^3a_4a_5 - 18a_1a_2^2a_4^2a_5 + 12a_0a_1a_4^3a_5 - \\
& - 3a_2^4a_5^2 - 9a_1^2a_3^2a_5^2 + 18a_0a_2a_3^2a_5^2 + 18a_1^2a_2a_4a_5^2 - 9a_0^2a_4^2a_5^2 - 2a_1^3a_5^3 - \\
& - 12a_0a_1a_2a_5^3 - 6a_0^2a_3a_5^3)d^3 + (a_4^6 - 6a_3a_4^4a_5 + 9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - 2a_3^3a_5^3 - \\
& - 12a_2a_3a_4a_5^3 - 6a_1a_4^2a_5^3 + 3a_2^2a_5^4 + 6a_1a_3a_5^4 + 6a_0a_4a_5^4)d^4 + (-a_5^6)d^5].
\end{aligned} \tag{7.1}
$$

Demonstração. Consideramos $\alpha_i = \sigma_i(\alpha)$, com $i = 1, 2, 3, 4, 5, 6$. Assim,

$$\begin{aligned}
\alpha_1 &= a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5,\\
\alpha_2 &= a_0 + a_1\theta\xi_6 + a_2\theta^2\xi_6^2 + a_3\theta^3\xi_6^3 + a_4\theta^4\xi_6^4 + a_5\theta^5\xi_6^5,\\
\alpha_3 &= a_0 + a_1\theta\xi_6^2 + a_2\theta^2\xi_6^4 + a_3\theta^3 + a_4\theta^4\xi_6^2 + a_5\theta^5\xi_6^4,\\
\alpha_4 &= a_0 + a_1\theta\xi_6^3 + a_2\theta^2 + a_3\theta^3\xi_6^3 + a_4\theta^4 + a_5\theta^5\xi_6^3,\\
\alpha_5 &= a_0 + a_1\theta\xi_6^4 + a_2\theta^2\xi_6^2 + a_3\theta^3 + a_4\theta^4\xi_6^4 + a_5\theta^5\xi_6^2 \text{ e}\\
\alpha_6 &= a_0 + a_1\theta\xi_6^5 + a_2\theta^2\xi_6^4 + a_3\theta^3\xi_6^3 + a_4\theta^4\xi_6^2 + a_5\theta^5\xi_6.
\end{aligned}$$

Pela Proposição 2.3.4, segue que o polinômio característico de α é dado por

$$\begin{aligned}
f_\alpha(x) &= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6) =\\
&= x^6 - x^5(\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6) + x^4(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4+\\
&+ \alpha_3\alpha_4+\alpha_1\alpha_5+\alpha_2\alpha_5+\alpha_3\alpha_5+\alpha_4\alpha_5+\alpha_1\alpha_6+\alpha_2\alpha_6+\alpha_3\alpha_6+\alpha_4\alpha_6+\alpha_5\alpha_6)-\\
&- x^3(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_5+\alpha_1\alpha_3\alpha_5+\alpha_2\alpha_3\alpha_5+\alpha_1\alpha_4\alpha_5+\\
&+ \alpha_2\alpha_4\alpha_5+\alpha_3\alpha_4\alpha_5+\alpha_1\alpha_2\alpha_6+\alpha_1\alpha_3\alpha_6+\alpha_2\alpha_3\alpha_6+\alpha_1\alpha_4\alpha_6+\alpha_2\alpha_4\alpha_6+\alpha_3\alpha_4\alpha_6+\\
&+ \alpha_1\alpha_5\alpha_6+\alpha_2\alpha_5\alpha_6+\alpha_3\alpha_5\alpha_6+\alpha_4\alpha_5\alpha_6) + x^2(\alpha_1\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_3\alpha_5+\alpha_1\alpha_2\alpha_4\alpha_5+\\
&+ \alpha_1\alpha_3\alpha_4\alpha_5+\alpha_2\alpha_3\alpha_4\alpha_5+\alpha_1\alpha_2\alpha_3\alpha_6+\alpha_1\alpha_2\alpha_4\alpha_6+\alpha_1\alpha_3\alpha_4\alpha_6+\alpha_2\alpha_3\alpha_4\alpha_6+\\
&+ \alpha_1\alpha_2\alpha_5\alpha_6+\alpha_1\alpha_3\alpha_5\alpha_6+\alpha_2\alpha_3\alpha_5\alpha_6+\alpha_1\alpha_4\alpha_5\alpha_6+\alpha_2\alpha_4\alpha_5\alpha_6+\alpha_3\alpha_4\alpha_5\alpha_6)-\\
&- x(\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5+\alpha_1\alpha_2\alpha_3\alpha_4\alpha_6+\alpha_1\alpha_2\alpha_3\alpha_5\alpha_6+\alpha_1\alpha_2\alpha_4\alpha_5\alpha_6+\alpha_1\alpha_3\alpha_4\alpha_5\alpha_6+\\
&+ \alpha_2\alpha_3\alpha_4\alpha_5\alpha_6) + (\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6).
\end{aligned}$$

Lembramos que $\xi_6+\xi_6^2+\xi_6^3+\xi_6^4+\xi_6^5 = -1$. Com o auxílio do programa Wolfram Mathematica 11.3, para o desenvolvermos os coeficientes, obtemos

$\to\ \alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6 = 6a_0.$

$\to\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4+\alpha_3\alpha_4+\alpha_1\alpha_5+\alpha_2\alpha_5+\alpha_3\alpha_5+\alpha_4\alpha_5+\alpha_1\alpha_6+$
$+\alpha_2\alpha_6+\alpha_3\alpha_6+\alpha_4\alpha_6+\alpha_5\alpha_6 = 3(5a_0^2-(a_3^2+2a_2a_4+2a_1a_5)d).$

$\to\ \alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_5+\alpha_1\alpha_3\alpha_5+\alpha_2\alpha_3\alpha_5+\alpha_1\alpha_4\alpha_5+$
$+\alpha_2\alpha_4\alpha_5+\alpha_3\alpha_4\alpha_5+\alpha_1\alpha_2\alpha_6+\alpha_1\alpha_3\alpha_6+\alpha_2\alpha_3\alpha_6+\alpha_1\alpha_4\alpha_6+\alpha_2\alpha_4\alpha_6+\alpha_3\alpha_4\alpha_6+$
$+\alpha_1\alpha_5\alpha_6+\alpha_2\alpha_5\alpha_6+\alpha_3\alpha_5\alpha_6+\alpha_4\alpha_5\alpha_6 = 2(10a_0^3+(a_2^3+6a_1a_2a_3-6a_0a_3^2+3a_1^2a_4-$
$-12a_0a_2a_4-12a_0a_1a_5)d+(a_4^3+6a_3a_4a_5+3a_2a_5^2)d^2).$

$\to\ \alpha_1\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_3\alpha_5+\alpha_1\alpha_2\alpha_4\alpha_5+\alpha_1\alpha_3\alpha_4\alpha_5+\alpha_2\alpha_3\alpha_4\alpha_5+\alpha_1\alpha_2\alpha_3\alpha_6+\alpha_1\alpha_2\alpha_4\alpha_6+$
$+\alpha_1\alpha_3\alpha_4\alpha_6+\alpha_2\alpha_3\alpha_4\alpha_6+\alpha_1\alpha_2\alpha_5\alpha_6+\alpha_1\alpha_3\alpha_5\alpha_6+\alpha_2\alpha_3\alpha_5\alpha_6+\alpha_1\alpha_4\alpha_5\alpha_6+\alpha_2\alpha_4\alpha_5\alpha_6+$
$+\alpha_3\alpha_4\alpha_5\alpha_6 = 3(5a_0^4+(-3a_1^2a_2^2+2a_0a_2^3-2a_1^3a_3+12a_0a_1a_2a_3-6a_0^2a_3^2+6a_0a_1^2a_4-$
$-12a_0^2a_2a_4-12a_0^2a_1a_5)d+(a_3^4+3a_2^2a_4^2-6a_1a_3a_4^2+2a_0a_4^3-6a_2^2a_3a_5+12a_0a_3a_4a_5+$
$+3a_1^2a_5^2+6a_0a_2a_5^2)d^2+(-3a_4^2a_5^2-2a_3a_5^3)d^3).$

$\to\ \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5+\alpha_1\alpha_2\alpha_3\alpha_4\alpha_6+\alpha_1\alpha_2\alpha_3\alpha_5\alpha_6+\alpha_1\alpha_2\alpha_4\alpha_5\alpha_6+\alpha_1\alpha_3\alpha_4\alpha_5\alpha_6+\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6 =$
$=6(a_0^5+(a_1^4a_2-3a_0a_1^2a_2^2+a_0^2a_2^3-2a_0a_1^3a_3+6a_0^2a_1a_2a_3-2a_0^3a_3^2+3a_0^2a_1^2a_4-4a_0^3a_2a_4-$
$-4a_0^3a_1a_5)d+(a_2^3a_3^2-2a_1a_2a_3^3+a_0a_3^4-a_2^4a_4+3a_1^2a_3^2a_4+3a_0a_2^2a_4^2-6a_0a_1a_3a_4^2+a_0^2a_4^3+$
$+2a_1a_2^3a_5-6a_0a_2^2a_3a_5-2a_1^3a_4a_5+6a_0^2a_3a_4a_5+3a_0a_1^2a_5^2+3a_0^2a_2a_5^2)d^2+(a_3^2a_4^3-a_2a_4^4-$
$-2a_3^3a_4a_5+2a_1a_4^3a_5+3a_2a_3^2a_5^2-3a_0a_4^2a_5^2-2a_1a_2a_5^3-2a_0a_3a_5^3)d^3+(a_4a_5^4)d^4).$

$\to\ \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6 = a_0^6 + (-a_1^6 + 6a_0a_1^4a_2 - 9a_0^2a_1^2a_2^2 + 2a_0^3a_2^3 - 6a_0^2a_1^3a_3 + 12a_0^3a_1a_2a_3 - 3a_0^4a_3^2 + 6a_0^3a_1^2a_4 - 6a_0^4a_2a_4 - 6a_0^4a_1a_5)d + (a_2^6 - 6a_1a_2^4a_3 + 9a_1^2a_2^2a_3^2 + 6a_0a_2^3a_3^2 - 2a_1^3a_3^3 - 12a_0a_1a_2a_3^3 + 3a_0^2a_3^4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 - 12a_1^3a_2a_3a_4 + 18a_0a_1^2a_3^2a_4 + 3a_1^4a_4^2 + 9a_0^2a_2^2a_4^2 - 18a_0^2a_1a_3a_4^2 + 2a_0^3a_4^3 - 6a_1^3a_2^2a_5 + 12a_0a_1a_2^2a_5 + 6a_1^4a_3a_5 - 18a_0^2a_2^2a_3a_5 - 12a_0a_1^3a_4a_5 + 12a_0^3a_3a_4a_5 + 9a_0^2a_1^2a_5^2 + 6a_0^3a_2a_5^2)d^2 + (-a_3^6 + 6a_2a_3^4a_4 - 9a_2^2a_3^2a_4^2 - 6a_1a_3^3a_4^2 + 2a_2^3a_4^3 + 12a_1a_2a_3a_4^3 + 6a_0a_3^2a_4^3 - 3a_1^2a_4^4 - 6a_0a_2a_4^4 - 6a_2^2a_3^3a_5 + 6a_1a_3^4a_5 + 12a_2^3a_3a_4a_5 - 12a_0a_3^3a_4a_5 - 18a_1a_2^2a_4^2a_5 + 12a_0a_1a_3^2a_5 - 3a_2^4a_5^2 - 9a_1^2a_3^2a_5^2 + 18a_0a_2a_3^2a_5^2 + 18a_1^2a_2a_4a_5^2 - 9a_0^2a_4^2a_5^2 - 2a_1^3a_5^3 - 12a_0a_1a_2a_5^3 - 6a_0^2a_3a_5^3)d^3 + (a_4^6 - 6a_3a_4^4a_5 + 9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - 2a_3^3a_5^3 - 12a_2a_3a_4a_5^3 - 6a_1a_4^2a_5^3 + 3a_2^2a_5^4 + 6a_1a_3a_5^4 + 6a_0a_4a_5^4)d^4 + (-a_5^6)d^5.$

Assim,

$$\begin{aligned}
f_\alpha(x) = {} & x^6 - x^5[6a_0] + x^4[3(5a_0^2 - (a_3^2 + 2a_2a_4 + 2a_1a_5)d)] - x^3[2(10a_0^3 + (a_2^3 + \\
& + 6a_1a_2a_3 - 6a_0a_3^2 + 3a_1^2a_4 - 12a_0a_2a_4 - 12a_0a_1a_5)d + (a_4^3 + 6a_3a_4a_5 + \\
& + 3a_2a_5^2)d^2)] + x^2[3(5a_0^4 + (-3a_1^2a_2^2 + 2a_0a_2^3 - 2a_1^3a_3 + 12a_0a_1a_2a_3 - \\
& - 6a_0^2a_3^2 + 6a_0a_1^2a_4 - 12a_0^2a_2a_4 - 12a_0^2a_1a_5)d + (a_3^4 + 3a_2^2a_4^2 - 6a_1a_3a_4^2 + \\
& + 2a_0a_4^3 - 6a_2^2a_3a_5 + 12a_0a_3a_4a_5 + 3a_1^2a_5^2 + 6a_0a_2a_5^2)d^2 + (-3a_4^2a_5^2 - \\
& - 2a_3a_5^3)d^3)] - x[6(a_0^5 + (a_1^4a_2 - 3a_0a_1^2a_2^2 + a_0^2a_2^3 - 2a_0a_1^3a_3 + 6a_0^2a_1a_2a_3 - \\
& - 2a_0^3a_3^2 + 3a_0^2a_1^2a_4 - 4a_0^3a_2a_4 - 4a_0^3a_1a_5)d + (a_2^3a_3^2 - 2a_1a_2a_3^3 + a_0a_3^4 - \\
& - a_2^4a_4 + 3a_1^2a_3^2a_4 + 3a_0a_2^2a_4^2 - 6a_0a_1a_3a_4^2 + a_0^2a_4^3 + 2a_1a_2^3a_5 - 6a_0a_2^2a_3a_5 - \\
& - 2a_1^3a_4a_5 + 6a_0^2a_3a_4a_5 + 3a_0a_1^2a_5^2 + 3a_0^2a_2a_5^2)d^2 + (a_3^2a_4^3 - a_2a_4^4 - 2a_3^3a_4a_5 + \\
& + 2a_1a_4^3a_5 + 3a_2a_3^2a_5^2 - 3a_0a_4^2a_5^2 - 2a_1a_2a_5^3 - 2a_0a_3a_5^3)d^3 + (a_4a_5^4)d^4)] + \\
& + [a_0^6 + (-a_1^6 + 6a_0a_1^4a_2 - 9a_0^2a_1^2a_2^2 + 2a_0^3a_2^3 - 6a_0^2a_1^3a_3 + 12a_0^3a_1a_2a_3 - \\
& - 3a_0^4a_3^2 + 6a_0^3a_1^2a_4 - 6a_0^4a_2a_4 - 6a_0^4a_1a_5)d + (a_2^6 - 6a_1a_2^4a_3 + 9a_1^2a_2^2a_3^2 + \\
& + 6a_0a_2^3a_3^2 - 2a_1^3a_3^3 - 12a_0a_1a_2a_3^3 + 3a_0^2a_3^4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 - \\
& - 12a_1^3a_2a_3a_4 + 18a_0a_1^2a_3^2a_4 + 3a_1^4a_4^2 + 9a_0^2a_2^2a_4^2 - 18a_0^2a_1a_3a_4^2 + 2a_0^3a_4^3 - \\
& - 6a_1^3a_2^2a_5 + 12a_0a_1a_2^2a_5 + 6a_1^4a_3a_5 - 18a_0^2a_2^2a_3a_5 - 12a_0a_1^3a_4a_5 + \\
& + 12a_0^3a_3a_4a_5 + 9a_0^2a_1^2a_5^2 + 6a_0^3a_2a_5^2)d^2 + (-a_3^6 + 6a_2a_3^4a_4 - 9a_2^2a_3^2a_4^2 - \\
& - 6a_1a_3^3a_4^2 + 2a_2^3a_4^3 + 12a_1a_2a_3a_4^3 + 6a_0a_3^2a_4^3 - 3a_1^2a_4^4 - 6a_0a_2a_4^4 - 6a_2^2a_3^3a_5 + \\
& + 6a_1a_3^4a_5 + 12a_2^3a_3a_4a_5 - 12a_0a_3^3a_4a_5 - 18a_1a_2^2a_4^2a_5 + 12a_0a_1a_3^2a_5 - \\
& - 3a_2^4a_5^2 - 9a_1^2a_3^2a_5^2 + 18a_0a_2a_3^2a_5^2 + 18a_1^2a_2a_4a_5^2 - 9a_0^2a_4^2a_5^2 - 2a_1^3a_5^3 - \\
& - 12a_0a_1a_2a_5^3 - 6a_0^2a_3a_5^3)d^3 + (a_4^6 - 6a_3a_4^4a_5 + 9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - 2a_3^3a_5^3 - \\
& - 12a_2a_3a_4a_5^3 - 6a_1a_4^2a_5^3 + 3a_2^2a_5^4 + 6a_1a_3a_5^4 + 6a_0a_4a_5^4)d^4 + (-a_5^6)d^5],
\end{aligned}$$

o que prova a proposição. □

Exemplo 7.3.1. *Seja* $\mathbb{K} = Q(\theta)$, *com* $\theta = \sqrt[6]{7}$ *e* $\alpha = 1 + 2(\sqrt[6]{7})^5 \in \mathbb{K}$. *Pela Proposição 7.3.1, segue que o polinômio característico de* α *é calculado através da identificação dos valores* $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 2$ *e* $d = 7$ *e substituição direta. Logo,*

$$f_\alpha(x) = x^6 - 6x^5 + 15x^4 - 20x^3 + 15x^2 - 6x - 1075647.$$

Com este resultado, podemos enunciar e demonstrar o teorema que caracteriza o anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$. O teorema a seguir, é uma das nossas contribuições deste trabalho e apresenta um resultado novo de nossa autoria, não conhecido na literatura.

Teorema 7.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por*

$$\begin{cases} \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\theta^4+\mathbb{Z}\theta^5, \text{ se } d \not\equiv \pm1, \pm17, \pm10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 1 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+2\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+2\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -10, -1 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 17 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -17, 10 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{\theta+\theta^4}{2}\right)+\mathbb{Z}\left(\frac{\theta^2+\theta^5}{2}\right), \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Demonstração. Suponhamos que $\alpha \in \mathbb{K}$ é um inteiro algébrico e vamos explorar quais são as formas que α pode assumir, onde $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5$, com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}$. Pela Proposição 2.6.9, se α é um inteiro algébrico, então $6a_0, 6a_1, 6a_2, 6a_3, 6a_4, 6a_5 \in \mathbb{Z}$. Vamos supor que $6a_i = p_i$, com $p_i \in \mathbb{Z}$, para todo $i = 0, 1, 2, 3, 4, 5$. Assim,

$$a_i = \frac{p_i}{6}, \text{para todo } i = 0, 1, 2, 3, 4, 5.$$

Além do mais, p_i pode ser escrito da seguinte forma

$$p_i = 6q_i + r_i,$$

com $q_i, r_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4, 5\}$, para $i = 0, 1, 2, 3, 4, 5$. Reescrevendo α, segue que

$$\begin{aligned} \alpha &= a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5 = \frac{p_0}{6} + \frac{p_1}{6}\theta + \frac{p_2}{6}\theta^2 + \frac{p_3}{6}\theta^3 + \frac{p_4}{6}\theta^4 + \frac{p_5}{6}\theta^5 = \\ &= \frac{6q_0 + r_0}{6} + \frac{6q_1 + r_1}{6}\theta + \frac{6q_2 + r_2}{6}\theta^2 + \frac{6q_3 + r_3}{6}\theta^3 + \frac{6q_4 + r_4}{6}\theta^4 + \frac{6q_5 + r_5}{6}\theta^5 = \\ &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5. \end{aligned}$$

Logo,

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5. \quad (7.2)$$

Agora, como $\mathcal{O}_\mathbb{K}$ é um anel (Corolário 2.2.2) e $q = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 \in \mathcal{O}_\mathbb{K}$, segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 \in \mathcal{O}_\mathbb{K} \Leftrightarrow$$
$$r = \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_4}{6}\theta^5 \in \mathcal{O}_\mathbb{K}.$$

Assim, α é um inteiro algébrico se, e somente se, r é um inteiro algébrico. Consequentemente,

$$\alpha \in \mathcal{O}_\mathbb{K} \Leftrightarrow r \in \mathcal{O}_\mathbb{K}. \quad (7.3)$$

Novamente por esses dois resultados (Proposição 7.3.1 e Proposição 2.3.3), segue que

$r \in \mathcal{O}_{\mathbb{K}}$ se, e somente se,

$$
\begin{cases}
6[\frac{r_0}{6}] \in \mathbb{Z} \\
3[(\frac{5r_0^2}{36} - (\frac{r_3^2}{36} + \frac{2r_2r_4}{36} + \frac{2r_1r_5}{36})d)] \in \mathbb{Z}, \\
2[\frac{10r_0^3}{216} + (\frac{r_2^3}{216} + \frac{6r_1r_2r_3}{216} - \frac{6r_0r_3^2}{216} + \frac{3r_1^2r_4}{216} - \frac{12r_0r_2r_4}{216} - \frac{12r_0r_1r_5}{216})d + \\
+(\frac{r_4^3}{216} + \frac{6r_3r_4r_5}{216} + \frac{3r_2r_5^2}{216})d^2] \in \mathbb{Z}, \\
3[\frac{5r_0^4}{1296} + (-\frac{3r_1^2r_2^2}{1296} + \frac{2r_0r_2^3}{1296} - \frac{2r_1^3r_3}{1296} + \frac{12r_0r_1r_2r_3}{1296} - \frac{6r_0^2r_3^2}{1296} + \frac{6r_0r_1^2r_4}{1296} - \frac{12r_0^2r_2r_4}{1296} - \\
-\frac{12r_0^2r_1r_5}{1296})d + (\frac{r_3^4}{1296} + \frac{3r_2^2r_4^2}{1296} - \frac{6r_1r_3r_4^2}{1296} + \frac{2r_0r_4^3}{1296} - \frac{6r_2^2r_3r_5}{1296} + \frac{12r_0r_3r_4r_5}{1296} + \frac{3r_1^2r_5^2}{1296} + \\
+\frac{6r_0r_2r_5^2}{1296})d^2 + (-\frac{3r_4^2r_5^2}{1296} - \frac{2r_3r_5^3}{1296})d^3] \in \mathbb{Z}, \\
6[\frac{r_0^5}{7776} + (\frac{r_1^4r_2}{7776} - \frac{3r_0r_1^2r_2^2}{7776} + \frac{r_0^2r_2^3}{7776} - \frac{2r_0r_1^3r_3}{7776} + \frac{6r_0^2r_1r_2r_3}{7776} - \frac{2r_0^3r_3^2}{7776} + \frac{3r_0^2r_1^2r_4}{7776} - \frac{4r_0^3r_2r_4}{7776} - \\
-\frac{4r_0^3r_1r_5}{7776})d + (\frac{r_2^3r_3^2}{7776} - \frac{2r_1r_2r_3^3}{7776} + \frac{r_0r_3^4}{7776} - \frac{r_2^4r_4}{7776} + \frac{3r_1^2r_3^2r_4}{7776} + \frac{3r_0r_2^2r_4^2}{7776} - \frac{6r_0r_1r_3r_4^2}{7776} + \\
+\frac{r_0^2r_4^3}{7776} + \frac{2r_1r_2^3r_5}{7776} - \frac{6r_0r_2^2r_3r_5}{7776} - \frac{2r_1^3r_4r_5}{7776} + \frac{6r_0^2r_3r_4r_5}{7776} + \frac{3r_0r_1^2r_5^2}{7776} + \frac{3r_0^2r_2r_5^2}{7776})d^2 + \\
+(\frac{r_3^2r_4^3}{7776} - \frac{r_2r_4^4}{7776} - \frac{2r_3^3r_4r_5}{7776} + \frac{2r_1r_4^3r_5}{7776} + \frac{3r_2r_3^2r_5^2}{7776} - \frac{3r_0r_4^2r_5^2}{7776} - \frac{2r_1r_2r_5^3}{7776} - \frac{2r_0r_3r_5^3}{7776})d^3 + \\
+(\frac{r_4r_5^4}{7776})d^4] \in \mathbb{Z} \text{ e} \\
\frac{r_0^6}{46656} + (-\frac{r_1^6}{46656} + \frac{6r_0r_1^4r_2}{46656} - \frac{9r_0^2r_1^2r_2^2}{46656} + \frac{2r_0^3r_2^3}{46656} - \frac{6r_0^2r_1^3r_3}{46656} + \frac{12r_0^3r_1r_2r_3}{46656} - \frac{3r_0^4r_3^2}{46656} + \\
+\frac{6r_0^3r_1^2r_4}{46656} - \frac{6r_0^4r_2r_4}{46656} - \frac{6r_0^4r_1r_5}{46656})d + (\frac{r_2^6}{46656} - \frac{6r_1r_2^4r_3}{46656} + \frac{9r_1^2r_2^2r_3^2}{46656} + \frac{6r_0r_2^3r_3^2}{46656} - \frac{2r_1^3r_3^3}{46656} - \\
-\frac{12r_0r_1r_2r_3^3}{46656} + \frac{3r_0^2r_3^4}{46656} + \frac{6r_1^2r_2^3r_4}{46656} - \frac{6r_0r_2^4r_4}{46656} - \frac{12r_1^3r_2r_3r_4}{46656} + \frac{18r_0r_1^2r_3^2r_4}{46656} + \frac{3r_1^4r_4^2}{46656} + \\
+\frac{9r_0^2r_2^2r_4^2}{46656} - \frac{18r_0^2r_1r_3r_4^2}{46656} + \frac{2r_0^3r_4^3}{46656} - \frac{6r_1^3r_2^2r_5}{46656} + \frac{12r_0r_1r_2^3r_5}{46656} + \frac{6r_1^4r_3r_5}{46656} - \frac{18r_0^2r_2^2r_3r_5}{46656} - \\
-\frac{12r_0r_1^3r_4r_5}{46656} + \frac{12r_0^3r_3r_4r_5}{46656} + \frac{9r_0^2r_1^2r_5^2}{46656} + \frac{6r_0^3r_2r_5^2}{46656})d^2 + (-\frac{r_3^6}{46656} + \frac{6r_2r_3^4r_4}{46656} - \frac{9r_2^2r_3^2r_4^2}{46656} - \\
-\frac{6r_1r_3^3r_4^2}{46656} + \frac{2r_2^3r_4^3}{46656} + \frac{12r_1r_2r_3r_4^3}{46656} + \frac{6r_0r_3^2r_4^3}{46656} - \frac{3r_1^2r_4^4}{46656} - \frac{6r_0r_2r_4^4}{46656} - \frac{6r_2^2r_3^3r_5}{46656} + \frac{6r_1r_4^4r_5}{46656} + \\
+\frac{12r_2^3r_3r_4r_5}{46656} - \frac{12r_0r_3^3r_4r_5}{46656} - \frac{18r_1r_2^2r_4^2r_5}{46656} + \frac{12r_0r_1r_4^3r_5}{46656} - \frac{3r_2^4r_5^2}{46656} - \frac{9r_1^2r_3^2r_5^2}{46656} + \frac{18r_0r_2r_3^2r_5^2}{46656} + \\
+\frac{18r_1^2r_2r_4r_5^2}{46656} - \frac{9r_0^2r_4^2r_5^2}{46656} - \frac{2r_1^3r_5^3}{46656} - \frac{12r_0r_1r_2r_5^3}{46656} - \frac{6r_0^2r_3r_5^3}{46656})d^3 + (\frac{r_4^6}{46656} - \frac{6r_3r_4^4r_5}{46656} + \\
+\frac{9r_3^2r_4^2r_5^2}{46656} + \frac{6r_2r_4^3r_5^2}{46656} - \frac{2r_3^3r_5^3}{46656} - \frac{12r_2r_3r_4r_5^3}{46656} - \frac{6r_1r_4^2r_5^3}{46656} + \frac{3r_2^2r_5^4}{46656} + \frac{6r_1r_3r_5^4}{46656} + \frac{6r_0r_4r_5^4}{46656})d^4 + \\
+(-\frac{r_5^6}{46656})d^5 \in \mathbb{Z}.
\end{cases}
\tag{7.4}
$$

Renomeando as expressões obtidas, segue

$$
\omega_1 = \frac{5r_0^2 - (r_3^2 + 2r_2r_4 + 2r_1r_5)d}{12}. \tag{7.5}
$$

$$
\begin{aligned}
\omega_2 = {} & \frac{10r_0^3 + (r_2^3 + 6r_1r_2r_3 - 6r_0r_3^2 + 3r_1^2r_4 - 12r_0r_2r_4 - 12r_0r_1r_5)d}{108} + \\
& + \frac{(r_4^3 + 6r_3r_4r_5 + 3r_2r_5^2)d^2}{108}.
\end{aligned} \tag{7.6}
$$

$$
\begin{aligned}
\omega_3 = {} & \frac{5r_0^4 + (-3r_1^2r_2^2 + 2r_0r_2^3 - 2r_1^3r_3 + 12r_0r_1r_2r_3 - 6r_0^2r_3^2 + 6r_0r_1^2r_4)d}{432} + \\
& + \frac{(-12r_0^2r_2r_4 - 12r_0^2r_1r_5)d + (r_3^4 + 3r_2^2r_4^2 - 6r_1r_3r_4^2 + 2r_0r_4^3 - 6r_2^2r_3r_5)d^2}{432} + \\
& + \frac{(12r_0r_3r_4r_5 + 3r_1^2r_5^2 + 6r_0r_2r_5^2)d^2 + (-3r_4^2r_5^2 - 2r_3r_5^3)d^3}{432}
\end{aligned} \tag{7.7}
$$

$$\begin{aligned}\omega_4 = &\frac{r_0^5 + (r_1^4 r_2 - 3r_0 r_1^2 r_2^2 + r_0^2 r_2^3 - 2r_0 r_1^3 r_3 + 6r_0^2 r_1 r_2 r_3 - 2r_0^3 r_3^2)d}{1296} + \\ &+ \frac{(3r_0^2 r_1^2 r_4 - 4r_0^3 r_2 r_4 - 4r_0^3 r_1 r_5)d + (r_2^3 r_3^2 - 2r_1 r_2 r_3^3 + r_0 r_3^4 - r_2^4 r_4)d^2}{1296} + \\ &+ \frac{(3r_1^2 r_3^2 r_4 + 3r_0 r_2^2 r_4^2 - 6r_0 r_1 r_3 r_4^2 + r_0^2 r_4^3 + 2r_1 r_2^3 r_5 - 6r_0 r_2^2 r_3 r_5)d^2}{1296} + \\ &+ \frac{(-2r_1^3 r_4 r_5 + 6r_0^2 r_3 r_4 r_5 + 3r_0 r_1^2 r_5^2 + 3r_0^2 r_2 r_5^2)d^2 + (r_3^2 r_4^3 - r_2 r_4^4 - 2r_3^3 r_4 r_5)d^3}{1296} + \\ &+ \frac{(2r_1 r_4^3 r_5 + 3r_2 r_3^2 r_5^2 - 3r_0 r_4^2 r_5^2 - 2r_1 r_2 r_5^3 - 2r_0 r_3 r_5^3)d^3 + (r_4 r_5^4)d^4}{1296}.\end{aligned} \tag{7.8}$$

$$\begin{aligned}\omega_5 = &\frac{r_0^6 + (-r_1^6 + 6r_0 r_1^4 r_2 - 9r_0^2 r_1^2 r_2^2 + 2r_0^3 r_2^3 - 6r_0^2 r_1^3 r_3 + 12r_0^3 r_1 r_2 r_3 - 3r_0^4 r_3^2)d}{46656} + \\ &+ \frac{(6r_0^3 r_1^2 r_4 - 6r_0^4 r_2 r_4 - 6r_0^4 r_1 r_5)d + (r_2^6 - 6r_1 r_2^4 r_3 + 9r_1^2 r_2^2 r_3^2 + 6r_0 r_2^3 r_3^2)d^2}{46656} + \\ &+ \frac{(-2r_1^3 r_3^3 - 12r_0 r_1 r_2 r_3^3 + 3r_0^2 r_3^4 + 6r_1^2 r_2^3 r_4 - 6r_0 r_2^4 r_4 - 12r_1^3 r_2 r_3 r_4)d^2}{46656} + \\ &+ \frac{(18r_0 r_1^2 r_3^2 r_4 + 3r_1^4 r_4^2 + 9r_0^2 r_2^2 r_4^2 - 18r_0^2 r_1 r_3 r_4^2 + 2r_0^3 r_4^3 - 6r_1^3 r_2^2 r_5)d^2}{46656} + \\ &+ \frac{(12r_0 r_1 r_2^3 r_5 + 6r_1^4 r_3 r_5 - 18r_0^2 r_2^2 r_3 r_5 - 12r_0 r_1^3 r_4 r_5 + 12r_0^3 r_3 r_4 r_5)d^2}{46656} + \\ &+ \frac{(9r_0^2 r_1^2 r_5^2 + 6r_0^3 r_2 r_5^2)d^2 + (-r_3^6 + 6r_2 r_3^4 r_4 - 9r_2^2 r_3^2 r_4^2 - 6r_1 r_3^3 r_4^2 + 2r_2^3 r_4^3)d^3}{46656} + \\ &+ \frac{(12r_1 r_2 r_3 r_4^3 + 6r_0 r_3^2 r_4^3 - 3r_1^2 r_4^4 - 6r_0 r_2 r_4^4 - 6r_2^2 r_3^3 r_5 + 6r_1 r_3^4 r_5)d^3}{46656} + \\ &+ \frac{(12r_2^3 r_3 r_4 r_5 - 12r_0 r_3^3 r_4 r_5 - 18r_1 r_2^2 r_4^2 r_5 + 12r_0 r_1 r_4^3 r_5 - 3r_2^4 r_5^2 - 9r_1^2 r_3^2 r_5^2)d^3}{46656} + \\ &+ \frac{(18r_0 r_2 r_3^2 r_5^2 + 18r_1^2 r_2 r_4 r_5^2 - 9r_0^2 r_4^2 r_5^2 - 2r_1^3 r_5^3 - 12r_0 r_1 r_2 r_5^3 - 6r_0^2 r_3 r_5^3)d^3}{46656} + \\ &+ \frac{(r_4^6 - 6r_3 r_4^4 r_5 + 9r_3^2 r_4^2 r_5^2 + 6r_2 r_4^3 r_5^2 - 2r_3^3 r_5^3 - 12r_2 r_3 r_4 r_5^3 - 6r_1 r_4^2 r_5^3)d^4}{46656} + \\ &+ \frac{(3r_2^2 r_5^4 + 6r_1 r_3 r_5^4 + 6r_0 r_4 r_5^4)d^4 + (-r_5^6)d^5}{46656}.\end{aligned} \tag{7.9}$$

Das implicações na Expressão (7.3) e na Expressão (7.4), segue que

$$\alpha \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \omega_1, \omega_2, \omega_3, \omega_4, \omega_5 \in \mathbb{Z}. \tag{7.10}$$

De acordo com os parâmetros $r_0, r_1, r_2, r_3, r_4, r_5 \in \{0, 1, 2, 3, 4, 5\}$, segue que este caso se trata da análise de 46656 possibilidades. Mas, por este resultado se tratar de uma equivalência biunívoca, vamos encontrar somente as possibilidades que são soluções da forma $s_j = (r_0, r_1, r_2, r_3, r_4, r_5)$, para algum j. Agora, vamos mostrar que a base integral é dada por

$$\left\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\right\},$$

$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right), \left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right)\right\},$$

$$\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1+2\theta^2+\theta^4}{3}\right), \left(\frac{\theta+2\theta^3+\theta^5}{3}\right)\right\},$$
$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right), \left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right)\right\},$$
$$\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1+\theta^2+\theta^4}{3}\right), \left(\frac{\theta+\theta^3+\theta^5}{3}\right)\right\} \text{ ou}$$
$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{\theta+\theta^4}{2}\right), \left(\frac{\theta^2+\theta^5}{2}\right)\right\},$$

e para quais valores de r_i's isso é verídico, com $i = 0, 1, 2, 3, 4, 5$.

1. Análise dos valores de r_i's para que a base integral seja $\{1, \theta, \theta^2, \theta^3, \theta^4\}$. Neste caso, consideramos α um elemento genérico que escolhemos inicialmente. Pela Equação (7.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 = \\ &= \left(q_0 + \frac{r_0}{6}\right) + \left(q_1 + \frac{r_1}{6}\right)\theta + \left(q_2 + \frac{r_2}{6}\right)\theta^2 + \left(q_3 + \frac{r_3}{6}\right)\theta^3 + \left(q_4 + \frac{r_4}{6}\right)\theta^4 + \\ &+ \left(q_5 + \frac{r_5}{6}\right)\theta^5.\end{aligned}$$

   com $q_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4, 5\}$ para $i = 0, 1, 2, 3, 4, 5$. Suponhamos que para $z_0, z_1, z_2, z_3, z_4, z_5$ quaisquer, α pode ser escrito como

$$\alpha = z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\theta^4 + z_5\theta^5.$$

   Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned}z_0 &= q_0 + \frac{r_0}{6} \ (1),\\ z_1 &= q_1 + \frac{r_1}{6} \ (2),\\ z_2 &= q_2 + \frac{r_2}{6} \ (3),\\ z_3 &= q_3 + \frac{r_3}{6} \ (4),\\ z_4 &= q_4 + \frac{r_4}{6} \ (5) \text{ e}\\ z_5 &= q_5 + \frac{r_5}{6} \ (6).\end{aligned}$$

   Logo, podemos visualizar que o conjunto $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ é um a base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4, z_5 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0, 1, 2, 3, 4, 5\}$, para $i = 0, 1, 2, 3, 4, 5$, segue que o conjunto citado é uma base integral, para os seguintes casos.

   (a) De (1), então $r_0 = 0$,

   (b) De (2), então $r_1 = 0$,

   (c) De (3), então $r_2 = 0$,

   (d) De (4), então $r_3 = 0$,

(e) De (5), então $r_4 = 0$ e

(f) De (6), então $r_5 = 0$.

Assim, a solução possível é $s_1 = (0, 0, 0, 0, 0, 0)$.

2. Análise dos valores de r_i's para que a base integral seja

$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right), \left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right)\right\}.$$

Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (7.2), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 =$$
$$= \left(q_0 + \frac{r_0}{6}\right) + \left(q_1 + \frac{r_1}{6}\right)\theta + \left(q_2 + \frac{r_2}{6}\right)\theta^2 + \left(q_3 + \frac{r_3}{6}\right)\theta^3 + \left(q_4 + \frac{r_4}{6}\right)\theta^4 + \left(q_5 + \frac{r_5}{6}\right)\theta^5.$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4, 5\}$ para $i = 0, 1, 2, 3, 4, 5$. Agora, suponhamos que para $z_0, z_1, z_2, z_3, z_4, z_5$ quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\left(\frac{1+\theta^3}{2}\right) + z_4\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right) + \\ &+ z_5\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right) \\ &= \left(z_0 + \frac{z_3}{2} + \frac{4z_4}{6} + \frac{3z_5}{6}\right) + \left(z_1 + \frac{3z_4}{6} + \frac{4z_5}{6}\right)\theta + \left(z_2 + \frac{4z_4}{6} + \frac{3z_5}{6}\right)\theta^2 + \\ &+ \left(\frac{z_3}{2} + \frac{z_5}{6}\right)\theta^3 + \left(\frac{z_4}{6}\right)\theta^4 + \left(\frac{z_5}{6}\right)\theta^5.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações.

$$\begin{aligned} z_0 + \frac{z_3}{2} + \frac{4z_4}{6} + \frac{3z_5}{6} &= q_0 + \frac{r_0}{6} \ (1), \\ z_1 + \frac{3z_4}{6} + \frac{4z_5}{6} &= q_1 + \frac{r_1}{6} \ (2), \\ z_2 + \frac{4z_4}{6} + \frac{3z_5}{6} &= q_2 + \frac{r_2}{6} \ (3), \\ \frac{z_3}{2} + \frac{z_5}{6} &= q_3 + \frac{r_3}{6} \ (4), \\ \frac{z_4}{6} &= q_4 + \frac{r_4}{6} \ (5) \text{ e} \\ \frac{z_5}{6} &= q_5 + \frac{r_5}{6} \ (6). \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right), \left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right)\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4, z_5 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0, 1, 2, 3, 4, 5\}$, para $i = 0, 1, 2, 3, 4, 5$, segue que o conjunto citado é uma base integral, para as seguintes condições.

(a) De (6), segue que $z_5 = 6q_5 + r_5$. Assim,

$$\boxed{r_5 = 0, 1, 2, 3, 4 \text{ ou } 5.}$$

(b) De (5), segue que $z_4 = 6q_4 + r_4$. Assim,

$$\boxed{r_4 = 0, 1, 2, 3, 4 \text{ ou } 5.}$$

(c) De (4) e (6), segue que $z_3 = 2q_3 - 2q_5 + \dfrac{r_3 - r_5}{3}$. Assim,

$$\boxed{r_3 \equiv r_5 (mod\ 3).}$$

(d) De (3), (5) e (6), segue que $z_2 = q_2 - 4q_4 - 3q_5 + \dfrac{r_2 - 4r_4 - 3r_5}{6}$. Assim,

$$\boxed{r_2 \equiv 4r_4 + 3r_5 (mod\ 6).}$$

(e) De (2), (5) e (6), segue que $z_1 = q_1 - 3q_4 - 4q_5 + \dfrac{r_1 - 3r_4 - 4r_5}{6}$. Assim,

$$\boxed{r_1 \equiv 3r_4 + 4r_5 (mod\ 6).}$$

(f) De (1), (4), (5) e (6), segue que $z_0 = q_0 - 2q_3 - 4q_4 - 2q_5 + \dfrac{r_0 - r_3 - 4r_4 - 2r_5}{6}$. Assim,

$$\boxed{r_0 \equiv r_3 + 4r_4 + 2r_5 (mod\ 6).}$$

Deste modo, as possíveis soluções são:

$s_1 = (0,0,0,0,0,0)$, $s_2 = (0,1,0,4,3,4)$, $s_3 = (0,1,3,4,3,1)$, $s_4 = (0,2,3,2,0,5)$,
$s_5 = (0,4,3,4,0,1)$, $s_6 = (0,5,0,2,3,2)$, $s_7 = (0,5,3,2,3,5)$, $s_8 = (1,0,1,3,4,3)$,
$s_9 = (1,0,4,3,4,0)$, $s_{10} = (1,1,1,1,1,1)$, $s_{11} = (1,1,4,1,1,4)$, $s_{12} = (1,2,1,5,4,5)$,
$s_{13} = (1,2,4,5,4,2)$, $s_{14} = (1,3,1,3,1,3)$, $s_{15} = (1,3,4,3,1,0)$, $s_{16} = (1,4,1,1,4,1)$,
$s_{17} = (1,4,4,1,4,4)$, $s_{18} = (1,5,1,5,1,5)$, $s_{19} = (1,5,4,5,1,2)$, $s_{20} = (2,0,5,0,2,3)$,
$s_{21} = (2,1,2,4,5,4)$, $s_{22} = (2,1,5,4,5,1)$, $s_{23} = (2,2,5,2,2,5)$, $s_{24} = (2,3,2,0,5,0)$,
$s_{25} = (2,3,5,0,5,3)$, $s_{26} = (2,4,5,4,2,1)$, $s_{27} = (2,5,2,2,5,2)$, $s_{28} = (2,5,5,2,5,5)$,
$s_{29} = (3,1,0,1,3,4)$, $s_{30} = (3,1,3,1,3,1)$, $s_{31} = (3,2,0,5,0,2)$, $s_{32} = (3,2,3,5,0,5)$,
$s_{33} = (3,4,0,1,0,4)$, $s_{34} = (3,4,3,1,0,1)$, $s_{35} = (3,5,0,5,3,2)$, $s_{36} = (3,5,3,5,3,5)$,
$s_{37} = (4,0,1,0,4,3)$, $s_{38} = (4,1,1,4,1,1)$, $s_{39} = (4,1,4,4,1,4)$, $s_{40} = (4,2,1,2,4,5)$,
$s_{41} = (4,3,1,0,1,3)$, $s_{42} = (4,3,4,0,1,0)$, $s_{43} = (4,4,1,4,4,1)$, $s_{44} = (4,5,1,2,1,5)$,
$s_{45} = (4,5,4,2,1,2)$, $s_{46} = (5,0,2,3,2,0)$, $s_{47} = (5,0,5,3,2,3)$, $s_{48} = (5,1,2,1,5,4)$,
$s_{49} = (5,1,5,1,5,1)$, $s_{50} = (5,2,2,5,2,2)$, $s_{51} = (5,2,5,5,2,5)$, $s_{52} = (5,3,2,3,5,0)$,
$s_{53} = (5,3,5,3,5,3)$, $s_{54} = (5,4,2,1,2,4)$, $s_{55} = (5,4,5,1,2,1)$, $s_{56} = (5,5,2,5,5,2)$,
$s_{57} = (5,5,5,5,5,5)$, $s_{58} = (0,2,0,2,0,2)$, $s_{59} = (0,4,0,4,0,4)$, $s_{60} = (2,0,2,0,2,0)$,
$s_{61} = (2,2,2,2,2,2)$, $s_{62} = (2,4,2,4,2,4)$, $s_{63} = (4,0,4,0,4,0)$, $s_{64} = (4,2,4,2,4,2)$,
$s_{65} = (4,4,4,4,4,4)$, $s_{66} = (0,0,3,0,0,3)$, $s_{67} = (0,3,0,0,3,0)$, $s_{68} = (0,3,3,0,3,3)$,
$s_{69} = (3,0,0,3,0,0)$, $s_{70} = (3,0,3,3,0,3)$, $s_{71} = (3,3,0,3,3,0)$ e $s_{72} = (3,3,3,3,3,3)$.

3. Análise dos valores de r_i's para que a base integral seja

$$\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1 + 2\theta^2 + \theta^4}{3}\right), \left(\frac{\theta + 2\theta^3 + \theta^5}{3}\right)\right\}.$$

Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (7.2), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 =$$
$$= \left(q_0 + \frac{r_0}{6}\right) + \left(q_1 + \frac{r_1}{6}\right)\theta + \left(q_2 + \frac{r_2}{6}\right)\theta^2 + \left(q_3 + \frac{r_3}{6}\right)\theta^3 + \left(q_4 + \frac{r_4}{6}\right)\theta^4 + \left(q_5 + \frac{r_5}{6}\right)\theta^5.$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3,4,5\}$, para $i = 0,1,2,3,4,5$. Agora, suponhamos que para $z_0, z_1, z_2, z_3, z_4, z_5$ quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1 + \theta + z_2\theta^2 + z_3\theta^3 + z_4\left(\frac{1+2\theta^2+\theta^4}{3}\right) + z_5\left(\frac{\theta+2\theta^3+\theta^5}{3}\right)\\ &= \left(z_0+\frac{z_4}{3}\right) + \left(z_1+\frac{z_5}{3}\right)\theta + \left(z_2+\frac{2z_4}{3}\right)\theta^2 + \left(z_3+\frac{2z_5}{3}\right)\theta^3 + \left(\frac{z_4}{3}\right)\theta^4 + \left(\frac{z_5}{3}\right)\theta^5.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_4}{3} &= q_0 + \frac{r_0}{6}\ (1),\\ z_1 + \frac{z_5}{3} &= q_1 + \frac{r_1}{6}\ (2),\\ z_2 + \frac{2z_4}{3} &= q_2 + \frac{r_2}{6}\ (3),\\ z_3 + \frac{2z_5}{3} &= q_3 + \frac{r_3}{6}\ (4),\\ \frac{z_4}{3} &= q_4 + \frac{r_4}{6}\ (5)\text{ e}\\ \frac{z_5}{3} &= q_5 + \frac{r_5}{6}\ (6).\end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1+2\theta^2+\theta^4}{3}\right), \left(\frac{\theta+2\theta^3+\theta^5}{3}\right)\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4, z_5 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3,4,5\}$, para $i = 0,1,2,3,4,5$, segue que o conjunto citado é uma base integral, nas seguintes condições.

(a) De (6), segue que $z_5 = 3q_5 + \frac{r_5}{2}$. Assim,

$$\boxed{r_5 = 0, 2 \text{ ou } 4.}$$

(b) De (5), segue que $z_4 = 3q_4 + \frac{r_4}{2}$. Assim,

$$\boxed{r_4 = 0, 2 \text{ ou } 4.}$$

(c) De (4) e (6), segue que $z_3 = q_3 - 2q_5 + \frac{r_3 - 2r_5}{3}$. Assim,

$$\boxed{r_3 \equiv 2r_5 (mod\ 6).}$$

(d) De (3) e (5), segue que $z_2 = q_2 - 2q_4 + \frac{r_2 - 2r_4}{6}$. Assim,

$$\boxed{r_2 \equiv 2r_4 (mod\ 6).}$$

(e) De (2) e (6), segue que $z_1 = q_1 - q_5 + \frac{r_1 - r_5}{6}$. Assim,

$$\boxed{r_1 = r_5.}$$

(f) De (1) e (5), segue que $z_0 = q_0 - q_4 + \frac{r_1 - r_4}{6}$. Assim,

$$\boxed{r_0 = r_4.}$$

Deste modo, as soluções possíveis são dadas por

$s_1 = (0,0,0,0,0,0)$, $s_{73} = (0,2,0,4,0,2)$, $s_{74} = (0,4,0,2,0,4)$, $s_{75} = (2,0,4,0,2,0)$, $s_{76} = (2,2,4,4,2,2)$, $s_{77} = (2,4,4,2,2,4)$, $s_{78} = (4,0,2,0,4,0)$, $s_{79} = (4,2,2,4,4,2)$ e $s_{80} = (4,4,2,2,4,4)$.

4. Análise dos valores de r_i's para que a base integral seja

$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right), \left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right)\right\}.$$

Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (7.2), segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 =$$
$$= \left(q_0 + \frac{r_0}{6}\right) + \left(q_1 + \frac{r_1}{6}\right)\theta + \left(q_2 + \frac{r_2}{6}\right)\theta^2 + \left(q_3 + \frac{r_3}{6}\right)\theta^3 + \left(q_4 + \frac{r_4}{6}\right)\theta^4 + \left(q_5 + \frac{r_5}{6}\right)\theta^5.$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3,4,5\}$, para $i = 0,1,2,3,4,5$. Agora, suponhamos que para $z_0, z_1, z_2, z_3, z_4, z_5$ quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\left(\frac{1+\theta^3}{2}\right) + z_4\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right) + \\ &+ z_5\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right) \\ &= \left(z_0 + \frac{z_3}{2} + \frac{4z_4}{6}\right) + \left(z_1 + \frac{3z_4}{6} + \frac{4z_5}{6}\right)\theta + \left(z_2 + \frac{2z_4}{6} + \frac{3z_5}{6}\right)\theta^2 + \\ &+ \left(\frac{z_3}{2} + \frac{2z_5}{6}\right)\theta^3 + \left(\frac{z_4}{6}\right)\theta^4 + \left(\frac{z_5}{6}\right)\theta^5.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_3}{2} + \frac{4z_4}{6} &= q_0 + \frac{r_0}{6} \ (1), \\ z_1 + \frac{3z_4}{6} + \frac{4z_5}{6} &= q_1 + \frac{r_1}{6} \ (2), \\ z_2 + \frac{2z_4}{6} + \frac{3z_5}{6} &= q_2 + \frac{r_2}{6} \ (3), \\ \frac{z_3}{2} + \frac{2z_5}{6} &= q_3 + \frac{r_3}{6} \ (4), \\ \frac{z_4}{6} &= q_4 + \frac{r_4}{6} \ (5) \text{ e} \\ \frac{z_5}{6} &= q_5 + \frac{r_5}{6} \ (6). \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right), \left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right)\right\}$ é um base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4, z_5 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3,4,5\}$, para $i = 0,1,2,3,4,5$, segue que o conjunto citado é uma base integral, nas seguintes condições.

(a) De (6), segue que $z_5 = 6q_5 + r_5$. Assim,

$$\boxed{r_5 = 0, 1, 2, 3, 4 \text{ ou } 5.}$$

(b) De (5), segue que $z_4 = 6q_4 + r_4$. Assim,

$$\boxed{r_4 = 0, 1, 2, 3, 4 \text{ ou } 5.}$$

(c) De (4) e (6), segue que $z_3 = 2q_3 - 4q_5 + \dfrac{r_3 - 2r_5}{3}$. Assim,

$$\boxed{r_3 \equiv 2r_5 (mod\ 3).}$$

(d) De (3), (5) e (6), segue que $z_2 = q_2 - 2q_4 - 3q_5 + \dfrac{r_2 - 2r_4 - 3r_5}{6}$. Assim,

$$\boxed{r_2 \equiv 2r_4 + 3r_5 (mod\ 6).}$$

(e) De (2), (5) e (6), segue que $z_1 = q_1 - 3q_4 - 4q_5 + \dfrac{r_1 - 3r_4 - 4r_5}{6}$. Assim,

$$\boxed{r_1 \equiv 3r_4 + 4r_5 (mod\ 6).}$$

(f) De (1), (4) e (5), segue que $z_0 = q_0 - q_3 - q_4 + \dfrac{r_0 - r_3 - 4r_4 + 2r_5}{6}$. Assim,

$$\boxed{r_0 \equiv r_3 + 4r_4 - 2r_5 (mod\ 6).}$$

Deste modo, as possíveis soluções são dadas por

$s_1 = (0,0,0,0,0,0)$, $s_{66} = (0,0,3,0,0,3)$, $s_{67} = (0,3,0,0,3,0)$, $s_{68} = (0,3,3,0,3,3)$, $s_{69} = (3,0,0,3,0,0)$, $s_{70} = (3,0,3,3,0,3)$, $s_{71} = (3,3,0,3,3,0)$, $s_{72} = (3,3,3,3,3,3)$, $s_{73} = (0,2,0,4,0,2)$, $s_{74} = (0,4,0,2,0,4)$, $s_{75} = (2,0,4,0,2,0)$, $s_{76} = (2,2,4,4,2,2)$, $s_{77} = (2,4,4,2,2,4)$, $s_{78} = (4,0,2,0,4,0)$, $s_{79} = (4,2,2,4,4,2)$, $s_{80} = (4,4,2,2,4,4)$, $s_{81} = (0,1,0,2,3,4)$, $s_{82} = (0,1,3,2,3,1)$, $s_{83} = (0,2,3,4,0,5)$, $s_{84} = (0,4,3,2,0,1)$, $s_{85} = (0,5,0,4,3,2)$, $s_{86} = (0,5,3,4,3,5)$, $s_{87} = (1,0,2,3,4,0)$, $s_{88} = (1,0,5,3,4,3)$, $s_{89} = (1,1,2,5,1,4)$, $s_{90} = (1,1,5,5,1,1)$, $s_{91} = (1,2,2,1,4,2)$, $s_{92} = (1,2,5,1,4,5)$, $s_{93} = (1,3,2,3,1,0)$, $s_{94} = (1,3,5,3,1,3)$, $s_{95} = (1,4,2,5,4,4)$, $s_{96} = (1,4,5,5,4,1)$, $s_{97} = (1,5,2,1,1,2)$, $s_{98} = (1,5,5,1,1,5)$, $s_{99} = (2,0,1,0,2,3)$, $s_{100} = (2,1,1,2,5,1)$, $s_{101} = (2,1,4,2,5,4)$, $s_{102} = (2,2,1,4,2,5)$, $s_{103} = (2,3,1,0,5,3)$, $s_{104} = (2,3,4,0,5,0)$, $s_{105} = (2,4,1,2,2,1)$, $s_{106} = (2,5,1,4,5,5)$, $s_{107} = (2,5,4,4,5,2)$, $s_{108} = (3,1,0,5,3,4)$, $s_{109} = (3,1,3,5,3,1)$, $s_{110} = (3,2,0,1,0,2)$, $s_{111} = (3,2,3,1,0,5)$, $s_{112} = (3,4,0,5,0,4)$, $s_{113} = (3,4,3,5,0,1)$, $s_{114} = (3,5,0,1,3,2)$, $s_{115} = (3,5,3,1,3,5)$, $s_{116} = (4,0,5,0,4,3)$, $s_{117} = (4,1,2,2,1,4)$, $s_{118} = (4,1,5,2,1,1)$, $s_{119} = (4,2,5,4,4,5)$, $s_{120} = (4,3,2,0,1,0)$, $s_{121} = (4,3,5,0,1,3)$, $s_{122} = (4,4,5,2,4,1)$, $s_{123} = (4,5,2,4,1,2)$, $s_{124} = (4,5,5,4,1,5)$, $s_{125} = (5,0,1,3,2,3)$, $s_{126} = (5,0,4,3,2,0)$, $s_{127} = (5,1,1,5,5,1)$, $s_{128} = (5,1,4,5,5,4)$, $s_{129} = (5,2,1,1,2,5)$, $s_{130} = (5,2,4,1,2,2)$, $s_{131} = (5,3,1,3,5,3)$, $s_{132} = (5,3,4,3,5,0)$, $s_{133} = (5,4,1,5,2,1)$, $s_{134} = (5,4,4,5,2,4)$, $s_{135} = (5,5,1,1,5,5)$ e $s_{136} = (5,5,4,1,5,2)$.

5. Valores de r_i's para que a base integral seja

$$\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1 + \theta^2 + \theta^4}{3}\right), \left(\frac{\theta + \theta^3 + \theta^5}{3}\right)\right\}.$$

Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (7.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 \\ &= \left(q_0 + \frac{r_0}{6}\right) + \left(q_1 + \frac{r_1}{6}\right)\theta + \left(q_2 + \frac{r_2}{6}\right)\theta^2 + \left(q_3 + \frac{r_3}{6}\right)\theta^3 + \left(q_4 + \frac{r_4}{6}\right)\theta^4 \\ &+ \left(q_5 + \frac{r_5}{6}\right)\theta^5.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2, 3, 4, 5\}$, para $i = 0, 1, 2, 3, 4, 5$. Agora, suponhamos que para $z_0, z_1, z_2, z_3, z_4, z_5$ quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3 + z_4\left(\frac{1+\theta^2+\theta^4}{3}\right) + z_5\left(\frac{\theta+\theta^3+\theta^5}{3}\right)\\ &= \left(z_0 + \frac{z_4}{3}\right) + \left(z_1 + \frac{z_5}{3}\right)\theta + \left(z_2 + \frac{z_4}{3}\right)\theta^2 + \left(z_3 + \frac{z_5}{3}\right)\theta^3 + \left(\frac{z_4}{3}\right)\theta^4 + \left(\frac{z_5}{3}\right)\theta^5.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_4}{3} &= q_0 + \frac{r_0}{6} \ (1),\\ z_1 + \frac{z_5}{3} &= q_1 + \frac{r_1}{6} \ (2),\\ z_2 + \frac{z_4}{3} &= q_2 + \frac{r_2}{6} \ (3),\\ z_3 + \frac{z_5}{3} &= q_3 + \frac{r_3}{6} \ (4),\\ \frac{z_4}{3} &= q_4 + \frac{r_4}{6} \ (5) \text{ e}\\ \frac{z_5}{3} &= q_5 + \frac{r_5}{6} \ (6).\end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1+\theta^2+\theta^4}{3}\right), \left(\frac{\theta+\theta^3+\theta^5}{3}\right)\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4, z_5 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0, 1, 2, 3, 4, 5\}$, para $i = 0, 1, 2, 3, 4, 5$, segue que o conjunto citado é uma base integral, nas seguintes condições.

(a) De (6), segue que $z_5 = 3q_5 + \frac{r_5}{2}$. Assim,

$$\boxed{r_5 = 0, 2 \text{ ou } 4.}$$

(b) De (5), segue que $z_4 = 3q_4 + \frac{r_4}{2}$. Assim,

$$\boxed{r_4 = 0, 2 \text{ ou } 4.}$$

(c) De (4) e (6), segue que $z_3 = q_3 - q_5 + \frac{r_3 - r_5}{6}$. Assim,

$$\boxed{r_3 = r_5.}$$

(d) De (3) e (5), segue que $z_2 = q_2 - q_4 + \frac{r_2 - r_4}{6}$. Assim,

$$\boxed{r_2 = r_4.}$$

(e) De (2) e (6), segue que $z_1 = q_1 - q_5 + \frac{r_1 - r_5}{6}$. Assim,

$$\boxed{r_1 = r_6.}$$

(f) De (1) e (5), segue que $z_0 = q_0 - q_4 + \frac{r_0 - r_4}{6}$. Assim,

$$\boxed{r_0 = r_4.}$$

Deste modo, as soluções possíveis são dadas por

$s_1 = (0, 0, 0, 0, 0, 0)$, $s_{58} = (0, 2, 0, 2, 0, 2)$, $s_{59} = (0, 4, 0, 4, 0, 4)$, $s_{60} = (2, 0, 2, 0, 2, 0)$, $s_{61} = (2, 2, 2, 2, 2, 2)$, $s_{62} = (2, 4, 2, 4, 2, 4)$, $s_{63} = (4, 0, 4, 0, 4, 0)$, $s_{64} = (4, 2, 4, 2, 4, 2)$ e $s_{65} = (4, 4, 4, 4, 4, 4)$.

6. Análise dos valores de r_i's para que a base integral seja

$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{\theta+\theta^4}{2}\right), \left(\frac{\theta^2+\theta^5}{2}\right)\right\}.$$

Neste caso, consideramos α o elemento genérico que escolhemos inicialmente. Pela Equação (7.2), segue que

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + q_3\theta^3 + q_4\theta^4 + q_5\theta^5 + \frac{r_0}{6} + \frac{r_1}{6}\theta + \frac{r_2}{6}\theta^2 + \frac{r_3}{6}\theta^3 + \frac{r_4}{6}\theta^4 + \frac{r_5}{6}\theta^5 = \\ &= \left(q_0 + \frac{r_0}{6}\right) + \left(q_1 + \frac{r_1}{6}\right)\theta + \left(q_2 + \frac{r_2}{6}\right)\theta^2 + \left(q_3 + \frac{r_3}{6}\right)\theta^3 + \left(q_4 + \frac{r_4}{6}\right)\theta^4 + \left(q_5 + \frac{r_5}{6}\right)\theta^5.\end{aligned}$$

com $q_i \in \mathbb{Z}$ e $r_i \in \{0,1,2,3,4,5\}$, para $i = 0,1,2,3,4,5$. Agora, suponhamos que para $z_0, z_1, z_2, z_3, z_4, z_5$ quaisquer, α pode ser escrito como

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\theta^2 + z_3\left(\frac{1+\theta^3}{2}\right) + z_4\left(\frac{\theta+\theta^4}{2}\right) + z_5\left(\frac{\theta+\theta^5}{2}\right) \\ &= \left(z_0 + \frac{z_3}{2}\right) + \left(z_1 + \frac{z_4}{2}\right)\theta + \left(z_2 + \frac{z_5}{2}\right)\theta^2 + \left(\frac{z_3}{2}\right)\theta^3 + \left(\frac{z_4}{2}\right)\theta^4 + \left(\frac{z_5}{2}\right)\theta^5.\end{aligned}$$

Comparando as maneiras de escrever α obtemos as seguintes relações

$$\begin{aligned} z_0 + \frac{z_3}{2} &= q_0 + \frac{r_0}{6} \ (1), \\ z_1 + \frac{z_4}{2} &= q_1 + \frac{r_1}{6} \ (2), \\ z_2 + \frac{z_5}{2} &= q_2 + \frac{r_2}{6} \ (3), \\ \frac{z_3}{2} &= q_3 + \frac{r_3}{6} \ (4), \\ \frac{z_4}{2} &= q_4 + \frac{r_4}{6} \ (5) \text{ e} \\ \frac{z_5}{2} &= q_5 + \frac{r_5}{6} \ (6). \end{aligned}$$

Logo, o conjunto $\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{\theta+\theta^4}{2}\right), \left(\frac{\theta^2+\theta^5}{2}\right)\right\}$ é uma base integral se, e somente se, $z_0, z_1, z_2, z_3, z_4, z_5 \in \mathbb{Z}$. Assim, respeitando a condição de $r_i \in \{0,1,2,3,4,5\}$, para $i = 0,1,2,3,4,5$, segue que o conjunto citado é uma base integral sob as seguintes condições.

(a) De (6), segue que $z_5 = 2q_5 + \frac{r_5}{3}$. Assim,

$$\boxed{r_5 = 0 \text{ ou } 3.}$$

(b) De (5), segue que $z_4 = 2q_4 + \frac{r_4}{3}$. Assim,

$$\boxed{r_4 = 0 \text{ ou } 3.}$$

(c) De (4), segue que $z_3 = 2q_3 + \frac{r_3}{3}$. Assim,

$$\boxed{r_3 = 0 \text{ ou } 3.}$$

(d) De (3) e (6), segue que $z_2 = q_2 - q_5 + \frac{r_2 - r_5}{6}$. Assim,

$$\boxed{r_2 = r_5.}$$

(e) De (2) e (5), segue que $z_1 = q_1 - q_4 + \dfrac{r_1 - r_4}{6}$. Assim,

$$\boxed{r_1 = r_4.}$$

(f) De (1) e (4), segue que $z_0 = q_0 - q_3 + \dfrac{r_0 - r_3}{6}$. Assim,

$$\boxed{r_0 = r_3.}$$

Deste modo, as possíveis soluções são dadas por

$s_1 = (0,0,0,0,0,0)$, $s_{66} = (0,0,3,0,0,3)$, $s_{67} = (0,3,0,0,3,0)$, $s_{68} = (0,3,3,0,3,3)$, $s_{69} = (3,0,0,3,0,0)$, $s_{70} = (3,0,3,3,0,3)$, $s_{71} = (3,3,0,3,3,0)$ e $s_{72} = (3,3,3,3,3,3)$.

Nos itens (1), (2), (3), (4), (5) e (6) encontramos 136 soluções que são da forma $s_j = (r_0, r_1, r_2, r_3, r_4, r_5)$, com $j = 1, 2, \ldots, 136$. Ao substituir essas soluções nas Equações (7.5), (7.6), (7.7), (7.8) e (7.9) encontramos as equivalências de d módulo 36 de modo que $\omega_1, \omega_2, \omega_3, \omega_4, \omega_5 \in \mathbb{Z}$. Essa análise será descrita na Tabela (7.1). Devido a quantidade de soluções encontradas, faremos uma tabela mais resumida com o auxílio do programa Wolfram Mathematica 11.3.

Tabela 7.1: $\mathbb{K} = \mathbb{Q}(\sqrt[6]{d})$, d livre de quadrados - casos para análise de $\mathcal{O}_{\mathbb{K}}$.

Soluções (s_j)	$d \equiv (?)(mod\ 36)$
s_1	$\forall d$
s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}, s_{19}, s_{20}, s_{21}, s_{22}, s_{23}, s_{24}, s_{25}, s_{26}, s_{27}, s_{28}, s_{29}, s_{30}, s_{31}, s_{32}, s_{33}, s_{34}, s_{35}, s_{36}, s_{37}, s_{38}, s_{39}, s_{40}, s_{41}, s_{42}, s_{43}, s_{44}, s_{45}, s_{46}, s_{47}, s_{48}, s_{49}, s_{50}, s_{51}, s_{52}, s_{53}, s_{54}, s_{55}, s_{56} e s_{57}.	$d \equiv 1$
s_{73}, s_{74}, s_{75}, s_{76}, s_{77}, s_{78}, s_{79} e s_{80}.	$d \equiv -10, -1, 17$
s_{81}, s_{82}, s_{83}, s_{84}, s_{85}, s_{86}, s_{87}, s_{88}, s_{89}, s_{90}, s_{91}, s_{92}, s_{93}, s_{94}, s_{95}, s_{96}, s_{97}, s_{98}, s_{99}, s_{100}, s_{101}, s_{102}, s_{103}, s_{104}, s_{105}, s_{106}, s_{107}, s_{108}, s_{109}, s_{110}, s_{111}, s_{112}, s_{113}, s_{114}, s_{115}, s_{116}, s_{117}, s_{118}, s_{119}, s_{120}, s_{121}, s_{122}, s_{123}, s_{124}, s_{125}, s_{126}, s_{127}, s_{128}, s_{129}, s_{130}, s_{131}, s_{132}, s_{133}, s_{134}, s_{135} e s_{136}.	$d \equiv 17$
s_{58}, s_{59}, s_{60}, s_{61}, s_{62}, s_{63}, s_{64} e s_{65}.	$d \equiv -17, 1, 10$
s_{66}, s_{67}, s_{68}, s_{69}, s_{70}, s_{71} e s_{72}.	$d \equiv -15, -11, -7, -3, 1, 5, 13, 17$

Fonte: Elaborada pela autora.

Na Tabela (7.1), a célula "$\forall d$" não inclui as equivalências não livre de quadrados, uma vez que d é livre de quadrados. Para estabelecer o anel dos inteiros algébricos, relacionamos as informações obtidas das possíveis bases integrais nos itens (1), (2), (3), (4), (5) e (6) com as informações da Tabela (7.1). Logo,

1. Para $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$ exclusivamente, a solução é s_1. Para esta solução uma base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\right\}.$$

2. Para $d \equiv 1 (mod\ 36)$ exclusivamente, as soluções são s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}, s_{19}, s_{20}, s_{21}, s_{22}, s_{23}, s_{24}, s_{25}, s_{26}, s_{27}, s_{28}, s_{29}, s_{30}, s_{31}, s_{32}, s_{33}, s_{34}, s_{35}, s_{36}, s_{37}, s_{38}, s_{39}, s_{40}, s_{41}, s_{42}, s_{43}, s_{44}, s_{45}, s_{46}, s_{47}, s_{48}, s_{49}, s_{50}, s_{51}, s_{52}, s_{53}, s_{54}, s_{55}, s_{56} e s_{57}. Para estas soluções uma base integral é dada por
$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right), \left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right)\right\}.$$

3. Para $d \equiv -10, -1 (mod\ 36)$ exclusivamente, as soluções são s_{73}, s_{74}, s_{75}, s_{76}, s_{77}, s_{78}, s_{79} e s_{80}. Para estas soluções uma base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1+2\theta^2+\theta^4}{3}\right), \left(\frac{\theta+2\theta^3+\theta^5}{3}\right)\right\}.$$

4. Para $d \equiv 17 (mod\ 36)$ exclusivamente, as soluções são s_{81}, s_{82}, s_{83}, s_{84}, s_{85}, s_{86}, s_{87}, s_{88}, s_{89}, s_{90}, s_{91},s_{92}, s_{93}, s_{94}, s_{95}, s_{96}, s_{97}, s_{98}, s_{99}, s_{100}, s_{101}, s_{102}, s_{103}, s_{104}, s_{105}, s_{106}, s_{107}, s_{108}, s_{109}, s_{110}, s_{111}, s_{112}, s_{113}, s_{114}, s_{115}, s_{116}, s_{117}, s_{118}, s_{119}, s_{120}, s_{121}, s_{122}, s_{123}, s_{124}, s_{125}, s_{126}, s_{127}, s_{128}, s_{129}, s_{130}, s_{131}, s_{132}, s_{133}, s_{134}, s_{135} e s_{136}. Para estas soluções uma base integral é dada por
$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right), \left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right)\right\}.$$

5. Para $d \equiv -17, 10 (mod\ 36)$ exclusivamente, as soluções são s_{58}, s_{59}, s_{60}, s_{61}, s_{62}, s_{63}, s_{64} e s_{65}. Para estas soluções uma base integral é dada por
$$\left\{1, \theta, \theta^2, \theta^3, \left(\frac{1+\theta^2+\theta^4}{3}\right), \left(\frac{\theta+\theta^3+\theta^5}{3}\right)\right\}.$$

6. Para $d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36)$ exclusivamente, as soluções são s_{66}, s_{67}, s_{68}, s_{69}, s_{70}, s_{71} e s_{72}. Para estas soluções uma base integral é dada por
$$\left\{1, \theta, \theta^2, \left(\frac{1+\theta^3}{2}\right), \left(\frac{\theta+\theta^4}{2}\right), \left(\frac{\theta^2+\theta^5}{2}\right)\right\}.$$

Portanto, o anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\begin{cases} \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\theta^4+\mathbb{Z}\theta^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 1 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+2\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+2\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -10, -1 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 17 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -17, 10 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{\theta+\theta^4}{2}\right)+\mathbb{Z}\left(\frac{\theta^2+\theta^5}{2}\right), \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36), \end{cases}$$

o que prova o teorema. □

Exemplo 7.3.2. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[6]{7}$. Como $d = 7$ e $7 \equiv 7 (mod\ 36)$, pelo Teorema 7.3.1, segue que o anel dos inteiros algébricos desse caso é dado por*
$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\theta^4+\mathbb{Z}\theta^5.$$

7.3.2 Norma, traço e discriminante em $\mathbb{Q}(\sqrt[6]{d})$

Nesta seção, apresentamos a norma, o traço e o discriminante em $\mathbb{K} = \mathbb{Q}(\sqrt[5]{d})$, com d um inteiro livre de quadrados.

Proposição 7.3.2. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}$. O traço de α é calculado por*

$$\mathcal{T}r(\alpha) = 6a_0.$$

Demonstração. Na Proposição 7.3.1, calculamos o polinômio característico de α, e assim, pela Observação 2.3.6, segue que

$$\mathcal{T}r(\alpha) = 6a_0,$$

o que prova a proposição. □

Proposição 7.3.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}$. A norma de α é calculada por*

$$\begin{aligned}\mathcal{N}(\alpha) = {} & a_0^6 + (-a_1^6 + 6a_0a_1^4a_2 - 9a_0^2a_1^2a_2^2 + 2a_0^3a_2^3 - 6a_0^2a_1^3a_3 + 12a_0^3a_1a_2a_3 - 3a_0^4a_3^2 + \\ & + 6a_0^3a_1^2a_4 - 6a_0^4a_2a_4 - 6a_0^4a_1a_5)d + (a_2^6 - 6a_1a_2^4a_3 + 9a_1^2a_2^2a_3^2 + 6a_0a_2^3a_3^2 - 2a_1^3a_3^3 - \\ & - 12a_0a_1a_2a_3^3 + 3a_0^2a_3^4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 - 12a_1^3a_2a_3a_4 + 18a_0a_1^2a_3^2a_4 + 3a_1^4a_4^2 + \\ & + 9a_0^2a_2^2a_4^2 - 18a_0^2a_1a_3a_4^2 + 2a_0^3a_4^3 - 6a_1^3a_2^2a_5 + 12a_0a_1a_2^3a_5 + 6a_1^4a_3a_5 - 18a_0^2a_2^2a_3a_5 - \\ & - 12a_0a_1^3a_4a_5 + 12a_0^3a_3a_4a_5 + 9a_0^2a_1^2a_5^2 + 6a_0^3a_2a_5^2)d^2 + (-a_3^6 + 6a_2a_3^4a_4 - 9a_2^2a_3^2a_4^2 - \\ & - 6a_1a_3^3a_4^2 + 2a_2^3a_4^3 + 12a_1a_2a_3a_4^3 + 6a_0a_3^2a_4^3 - 3a_1^2a_4^4 - 6a_0a_2a_4^4 - 6a_2^2a_3^3a_5 + 6a_1a_3^4a_5 + \\ & + 12a_2^3a_3a_4a_5 - 12a_0a_3^3a_4a_5 - 18a_1a_2^2a_4^2a_5 + 12a_0a_1a_4^3a_5 - 3a_2^4a_5^2 - 9a_1^2a_3^2a_5^2 + \\ & + 18a_0a_2a_3^2a_5^2 + 18a_1^2a_2a_4a_5^2 - 9a_0^2a_4^2a_5^2 - 2a_1^3a_5^3 - 12a_0a_1a_2a_5^3 - 6a_0^2a_3a_5^3)d^3 + \\ & + (a_4^6 - 6a_3a_4^4a_5 + 9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - 2a_3^3a_5^3 - 12a_2a_3a_4a_5^3 - 6a_1a_4^2a_5^3 + 3a_2^2a_5^4 + \\ & + 6a_1a_3a_5^4 + 6a_0a_4a_5^4)d^4 + (-a_5^6)d^5.\end{aligned}$$

Demonstração. Na Proposição 7.3.1, calculamos o polinômio característico de α, e assim, pela Observação 2.3.6, segue que

$$\begin{aligned}\mathcal{N}(\alpha) = {} & a_0^6 + (-a_1^6 + 6a_0a_1^4a_2 - 9a_0^2a_1^2a_2^2 + 2a_0^3a_2^3 - 6a_0^2a_1^3a_3 + 12a_0^3a_1a_2a_3 - 3a_0^4a_3^2 + \\ & + 6a_0^3a_1^2a_4 - 6a_0^4a_2a_4 - 6a_0^4a_1a_5)d + (a_2^6 - 6a_1a_2^4a_3 + 9a_1^2a_2^2a_3^2 + 6a_0a_2^3a_3^2 - 2a_1^3a_3^3 - \\ & - 12a_0a_1a_2a_3^3 + 3a_0^2a_3^4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 - 12a_1^3a_2a_3a_4 + 18a_0a_1^2a_3^2a_4 + 3a_1^4a_4^2 + \\ & + 9a_0^2a_2^2a_4^2 - 18a_0^2a_1a_3a_4^2 + 2a_0^3a_4^3 - 6a_1^3a_2^2a_5 + 12a_0a_1a_2^3a_5 + 6a_1^4a_3a_5 - 18a_0^2a_2^2a_3a_5 - \\ & - 12a_0a_1^3a_4a_5 + 12a_0^3a_3a_4a_5 + 9a_0^2a_1^2a_5^2 + 6a_0^3a_2a_5^2)d^2 + (-a_3^6 + 6a_2a_3^4a_4 - 9a_2^2a_3^2a_4^2 - \\ & - 6a_1a_3^3a_4^2 + 2a_2^3a_4^3 + 12a_1a_2a_3a_4^3 + 6a_0a_3^2a_4^3 - 3a_1^2a_4^4 - 6a_0a_2a_4^4 - 6a_2^2a_3^3a_5 + 6a_1a_3^4a_5 + \\ & + 12a_2^3a_3a_4a_5 - 12a_0a_3^3a_4a_5 - 18a_1a_2^2a_4^2a_5 + 12a_0a_1a_4^3a_5 - 3a_2^4a_5^2 - 9a_1^2a_3^2a_5^2 + \\ & + 18a_0a_2a_3^2a_5^2 + 18a_1^2a_2a_4a_5^2 - 9a_0^2a_4^2a_5^2 - 2a_1^3a_5^3 - 12a_0a_1a_2a_5^3 - 6a_0^2a_3a_5^3)d^3 + \\ & + (a_4^6 - 6a_3a_4^4a_5 + 9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - 2a_3^3a_5^3 - 12a_2a_3a_4a_5^3 - 6a_1a_4^2a_5^3 + 3a_2^2a_5^4 + \\ & + 6a_1a_3a_5^4 + 6a_0a_4a_5^4)d^4 + (-a_5^6)d^5,\end{aligned}$$

o que prova a proposição. □

Exemplo 7.3.3. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[6]{7}$ e $\alpha = 1 + 2(\sqrt[6]{7})^5 \in \mathbb{K}$.*

a) Pela Proposição 7.3.2, segue que o traço de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 2$, e $d = 7$ e substituição direta. Logo, $\mathcal{T}r(\alpha) = 6$.

b) Pela Proposição 7.3.3, segue que a norma de α é calculado através da identificação dos valores $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 2$, e $d = 7$ e substituição direta. Logo, $\mathcal{N}(\alpha) = -1075647$.

Proposição 7.3.4. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O discriminante do anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por*

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 46656d^5, \text{ se } d \not\equiv \pm1, \pm17, \pm10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ 9d^5, \text{ se } d \equiv 1, 17 (mod\ 36) \\ 576d^5, \text{ se } d \equiv -17, -10, -1, 10 (mod\ 36) \\ 729d^5, \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Demonstração. Pelo Teorema 7.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4 + \mathbb{Z}\theta^5, \text{ se } d \not\equiv \pm1, \pm17, \pm10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\left(\frac{1+\theta^3}{2}\right) + \mathbb{Z}\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right) + \mathbb{Z}\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 1 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+2\theta^2+\theta^4}{3}\right) + \mathbb{Z}\left(\frac{\theta+2\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -10, -1 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\left(\frac{1+\theta^3}{2}\right) + \mathbb{Z}\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right) + \mathbb{Z}\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 17 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta^2+\theta^4}{3}\right) + \mathbb{Z}\left(\frac{\theta+\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -17, 10 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\left(\frac{1+\theta^3}{2}\right) + \mathbb{Z}\left(\frac{\theta+\theta^4}{2}\right) + \mathbb{Z}\left(\frac{\theta^2+\theta^5}{2}\right), \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Assim, uma base integral (base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$) admite as possibilidades.

1. Se $d \not\equiv \pm1, \pm17, \pm10, -15, -11, -7, -3, 5, 13 (mod\ 36)$, a base integral é dada por $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$.
2. Se $d \equiv 1 (mod\ 36)$, a base integral é $\left\{1, \theta, \theta^2, \frac{1+\theta^3}{2}, \frac{4+3\theta+4\theta^2+\theta^4}{6}, \frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right\}$.
3. Se $d \equiv -10, -1 (mod\ 36)$, a base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+2\theta^2+\theta^4}{3}, \frac{\theta+2\theta^3+\theta^5}{3}\right\}$.
4. Se $d \equiv 17 (mod\ 36)$, a base integral é $\left\{1, \theta, \theta^2, \frac{1+\theta^3}{2}, \frac{4+3\theta+2\theta^2+\theta^4}{6}, \frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right\}$.
5. Se $d \equiv -17, 10 (mod\ 36)$, a base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+\theta^2+\theta^4}{3}, \frac{\theta++\theta^3+\theta^5}{3}\right\}$.
6. Se $d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36)$, a base integral é $\left\{1, \theta, \theta^2, \frac{1+\theta^3}{2}, \frac{\theta+\theta^4}{2}, \frac{\theta^2+\theta^5}{2}\right\}$.

Pela Proposição 2.6.8, segue que

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, 3, 4, 5 \\ 6d^s, \text{ se } k = 6s, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > 6 \text{ e } k \not\equiv 0 (mod\ 6) \end{cases} \tag{7.11}$$

Logo, $\mathcal{T}r(1) = 6$, $\mathcal{T}r(\theta) = 0$, $\mathcal{T}r(\theta^2) = 0$, $\mathcal{T}r(\theta^3) = 0$, $\mathcal{T}r(\theta^4) = 0$, $\mathcal{T}r(\theta^5) = 0$, $\mathcal{T}r(d) = 6d$, $\mathcal{T}r(\theta^7) = 0$, $\mathcal{T}r(\theta^8) = 0$, $\mathcal{T}r(\theta^9) = 0$ e $\mathcal{T}r(\theta^{10}) = 0$. Agora, analisamos o discriminante para cada possibilidade da base integral.

1. Se $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$, então a base integral é dada por $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (7.11), segue que

$$\mathcal{D}(1,\theta,\theta^2,\theta^3,\theta^4,\theta^5) = \det \begin{pmatrix} \mathcal{T}r(1) & \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta^5) \\ \mathcal{T}r(\theta) & \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta^5) & \mathcal{T}r(d) \\ \mathcal{T}r(\theta^2) & \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta^5) & \mathcal{T}r(d) & \mathcal{T}r(\theta^7) \\ \mathcal{T}r(\theta^3) & \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta^5) & \mathcal{T}r(d) & \mathcal{T}r(\theta^7) & \mathcal{T}r(\theta^8) \\ \mathcal{T}r(\theta^4) & \mathcal{T}r(\theta^5) & \mathcal{T}r(d) & \mathcal{T}r(\theta^7) & \mathcal{T}r(\theta^8) & \mathcal{T}r(\theta^9) \\ \mathcal{T}r(\theta^5) & \mathcal{T}r(d) & \mathcal{T}r(\theta^7) & \mathcal{T}r(\theta^8) & \mathcal{T}r(\theta^9) & \mathcal{T}r(\theta^{10}) \end{pmatrix}$$

$$= \det \begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6d \\ 0 & 0 & 0 & 0 & 6d & 0 \\ 0 & 0 & 0 & 6d & 0 & 0 \\ 0 & 0 & 6d & 0 & 0 & 0 \\ 0 & 6d & 0 & 0 & 0 & 0 \end{pmatrix} = (-1)^{1+1}.6.\det \begin{pmatrix} 0 & 0 & 0 & 0 & 6d \\ 0 & 0 & 0 & 6d & 0 \\ 0 & 0 & 6d & 0 & 0 \\ 0 & 6d & 0 & 0 & 0 \\ 6d & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= 6.(-1)^{1+5}.6d.\det \begin{pmatrix} 0 & 0 & 0 & 6d \\ 0 & 0 & 6d & 0 \\ 0 & 6d & 0 & 0 \\ 6d & 0 & 0 & 0 \end{pmatrix} = 36d.(-1)^{1+4}.6d.\det \begin{pmatrix} 0 & 0 & 6d \\ 0 & 6d & 0 \\ 6d & 0 & 0 \end{pmatrix}$$

$$= 46656d^5.$$

2. Se $d \equiv 1 (mod\ 36)$, então a base integral é $\left\{1, \theta, \theta^2, \frac{1+\theta^3}{2}, \frac{4+3\theta+4\theta^2+\theta^4}{6}, \frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (7.11), segue que

$$\mathcal{D}\left(1,\theta,\theta^2,\frac{1+\theta^3}{2},\frac{4+3\theta+4\theta^2+\theta^4}{6},\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right) = \det \begin{pmatrix} 6 & 0 & 0 & 3 & 4 & 3 \\ 0 & 0 & 0 & 0 & 0 & d \\ 0 & 0 & 0 & 0 & d & 0 \\ 3 & 0 & 0 & \frac{3+3d}{2} & 2 & \frac{3+d}{2} \\ 4 & 0 & d & 2 & \frac{8+4d}{3} & 2+d \\ 3 & d & 0 & \frac{3+d}{2} & 2+d & \frac{3+3d}{2} \end{pmatrix}$$

$$= (-1)^{2+6}.d.\det \begin{pmatrix} 6 & 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 0 & d \\ 3 & 0 & 0 & \frac{3+3d}{2} & 2 \\ 4 & 0 & d & 2 & \frac{8+4d}{3} \\ 3 & d & 0 & \frac{3+d}{2} & 2+d \end{pmatrix} = d.(-1)^{2+5}.d.\begin{pmatrix} 6 & 0 & 0 & 3 \\ 3 & 0 & 0 & \frac{3+3d}{2} \\ 4 & 0 & d & 2 \\ 3 & d & 0 & \frac{3+d}{2} \end{pmatrix}$$

$$= -d^2.(-1)^{4+2}.d.\det \begin{pmatrix} 6 & 0 & 3 \\ 3 & 0 & \frac{3+3d}{2} \\ 4 & d & 2 \end{pmatrix} = 9d^5.$$

3. Se $d \equiv -10, -1 (mod\ 36)$, então a base integral é $\left\{1, \theta, \theta^2, \theta^3, \frac{1+2\theta^2+\theta^4}{3}, \frac{\theta+2\theta^3+\theta^5}{3}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (7.11), segue que

$$\mathcal{D}\left(1,\theta,\theta^2,\theta^3,\tfrac{1+2\theta^2+\theta^4}{3},\tfrac{\theta+2\theta^3+\theta^5}{3}\right)=\det\begin{pmatrix}6&0&0&0&2&0\\0&0&0&0&0&2d\\0&0&0&0&2d&0\\0&0&0&6d&0&4d\\2&0&2d&0&\frac{2}{3}&\frac{4d}{3}\\0&2d&0&0&\frac{4d}{3}&4d\end{pmatrix}$$

$$=(-1)^{2+6}.2d.\det\begin{pmatrix}6&0&0&0&2\\0&0&0&0&2d\\0&0&0&6d&0\\2&0&2d&0&\frac{2}{3}\\0&2d&0&4d&\frac{4d}{3}\end{pmatrix}=2d.(-1)^{2+5}.2d.\det\begin{pmatrix}6&0&0&0\\0&0&0&6d\\2&0&2d&0\\0&2d&0&4d\end{pmatrix}$$

$$=-4d^2.(-1)^{4+2}.6.\det\begin{pmatrix}0&0&6d\\0&2d&0\\2d&0&4d\end{pmatrix}=576d^5.$$

4. Se $d\equiv 17(mod\ 36)$, então a base integral é $\left\{1,\theta,\theta^2,\frac{1+\theta^3}{2},\frac{4+3\theta+2\theta^2+\theta^4}{6},\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (7.11), segue que

$$\mathcal{D}\left(1,\theta,\theta^2,\tfrac{1+\theta^3}{2},\tfrac{4+3\theta+2\theta^2+\theta^4}{6},\tfrac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right)=\det\begin{pmatrix}6&0&0&3&4&0\\0&0&0&0&0&d\\0&0&0&0&d&0\\3&0&0&\frac{3+3d}{2}&2&d\\4&0&d&2&\frac{8+2d}{3}&d\\0&d&0&d&d&2d\end{pmatrix}$$

$$=(-1)^{2+6}.d.\det\begin{pmatrix}6&0&0&3&4\\0&0&0&0&d\\3&0&0&\frac{3+3d}{2}&2\\4&0&d&2&\frac{8+2d}{3}\\0&d&0&d&d\end{pmatrix}=d.(-1)^{2+5}.d.\det\begin{pmatrix}6&0&0&3\\3&0&0&\frac{3+3d}{2}\\4&0&d&2\\0&d&0&d\end{pmatrix}$$

$$=-d^2.(-1)^{4+2}.d.\det\begin{pmatrix}6&0&3\\3&0&\frac{3+3d}{2}\\4&d&2\end{pmatrix}=9d^5.$$

5. Se $d\equiv -17,10(mod\ 36)$, então a base integral é $\left\{1,\theta,\theta^2,\theta^3,\frac{1+\theta^2+\theta^4}{3},\frac{\theta++\theta^3+\theta^5}{3}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (7.11), segue que

$$\mathcal{D}\left(1,\theta,\theta^2,\theta^3,\tfrac{1+\theta^2+\theta^4}{3},\tfrac{\theta++\theta^3+\theta^5}{3}\right)=\det\begin{pmatrix}6&0&0&0&2&0\\0&0&0&0&0&2d\\0&0&0&0&2d&0\\0&0&0&6d&0&2d\\2&0&2d&0&\frac{2+4d}{3}&0\\0&2d&0&2d&0&2d\end{pmatrix}$$

$$=(-1)^{2+6}.2d.\det\begin{pmatrix}6&0&0&0&2\\0&0&0&0&2d\\0&0&0&6d&0\\2&0&2d&0&\frac{2+4d}{3}\\0&2d&0&2d&0\end{pmatrix}=2d.(-1)^{2+5}.2d.\det\begin{pmatrix}6&0&0&0\\0&0&0&6d\\2&0&2d&0\\0&2d&0&2d\end{pmatrix}$$

$$= -4d^2.(-1)^{1+1}.6.\det\begin{pmatrix} 0 & 0 & 6d \\ 0 & 2d & 0 \\ 2d & 0 & 2d \end{pmatrix} = 576d^5.$$

6. Se $d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36)$, então podemos concluir que a base integral é $\left\{1, \theta, \theta^2, \frac{1+\theta^3}{2}, \frac{\theta+\theta^4}{2}, \frac{\theta^2+\theta^5}{2}\right\}$. Assim, usando as propriedades de traço e as informações obtidas da Equação (7.11), segue que

$$\mathcal{D}\left(1, \theta, \theta^2, \tfrac{1+\theta^3}{2}, \tfrac{\theta+\theta^4}{2}, \tfrac{\theta^2+\theta^5}{2}\right) = \det\begin{pmatrix} 6 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3d \\ 0 & 0 & 0 & 0 & 3d & 0 \\ 3 & 0 & 0 & \frac{3+3d}{2} & 0 & 0 \\ 0 & 0 & 3d & 0 & 0 & 3d \\ 0 & 3d & 0 & 0 & 3d & 0 \end{pmatrix}$$

$$= (-1)^{2+6}.3d.\det\begin{pmatrix} 6 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3d \\ 3 & 0 & 0 & \frac{3+3d}{2} & 0 \\ 0 & 0 & 3d & 0 & 0 \\ 0 & 3d & 0 & 0 & 3d \end{pmatrix} = 3d.(-1)^{2+5}.3d.\det\begin{pmatrix} 6 & 0 & 0 & 3 \\ 3 & 0 & 0 & \frac{3+3d}{2} \\ 0 & 0 & 3d & 0 \\ 0 & 3d & 0 & 0 \end{pmatrix}$$

$$= -9d^2.(-1)^{4+2}.3d.\det\begin{pmatrix} 6 & 0 & 3 \\ 3 & 0 & \frac{3+3d}{2} \\ 0 & 3d & 0 \end{pmatrix} = 729d^5.$$

Logo, da análise dos itens (1), (2), (3), (4), (5) e (6), segue que

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 46656d^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ 9d^5, \text{ se } d \equiv 1, 17 (mod\ 36) \\ 576d^5, \text{ se } d \equiv -17, -10, -1, 10 (mod\ 36) \\ 729d^5, \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36), \end{cases}$$

o que prova a proposição. □

Exemplo 7.3.4. *Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[6]{7}$. Como $d = 7$ e $7 \equiv 7 (mod\ 36)$, pela Proposição 7.3.4, segue que o discriminante é dado por $\mathcal{D}(\mathbb{K}) = 784147392$.*

Observação 7.3.1. *Para $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$, com $d \in \mathbb{Z}$ livre de quadrados, podemos calcular o discriminante da base potente $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ através do polinômio minimal $p(x) = x^6 - d$, e assim, utilizando o Corolário 2.5.4, segue que*

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5) = (-1)^{\frac{6^2+6+2}{2}}[6^6 d^{6-1}] = 46656d^5.$$

8 Reticulados Algébricos

Os reticulados são subgrupos de pontos do $\mathbb{R}^n$ que aparecem em diversas aplicações com destaque na teoria de códigos corretores de erros na criptografia. O estudo dos reticulados está condicionado ao problema geométrico chamado empacotamento esférico que consiste em cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio que apenas se tangenciam. Durante o *Congresso Internacional de Matemática* em Paris no ano de 1900, David Hilbert citou a questão dos empacotamentos esféricos como sendo o 18° Problema de uma lista seleta de desafios que viriam ocupar destaque no desenvolvimento da ciência moderna. Atrelado diretamente aos capítulos anteriores, neste momento, o objetivo é apresentar a estrutura dos reticulados sobre o $\mathbb{R}^n$ e obtermos aplicações nas extensões via corpos de números através do homomorfismo de Minkowski (homomorfismo canônico). As referências utilizadas neste capítulo são [3] e [5].

8.1 Reticulados no $\mathbb{R}^n$

Nesta seção, apresentamos o conceito de reticulados no $\mathbb{R}^n$ e alguns de seus parâmetros como matriz de Gram, volume, raio de empacotamento e densidade de centro.

Definição 8.1.1. *Sejam $V \subseteq \mathbb{R}^n$ um espaço vetorial de dimensão finita n sobre o corpo $\mathbb{R}$ e $v_1, v_2, \ldots, v_m$ vetores de V linearmente independentes sobre $\mathbb{R}$, com $m \leq n$. O conjunto dos elementos de V da forma*

$$\Lambda_B = \left\{ x = \sum_{i=1}^{m} a_i v_i \mid a_i \in \mathbb{Z} \right\},$$

*é chamado de **reticulado** com base $B = \{v_1, v_2, \ldots, v_m\}$. Se $m = n$, o reticulado Λ_B é chamado um **reticulado completo**.*

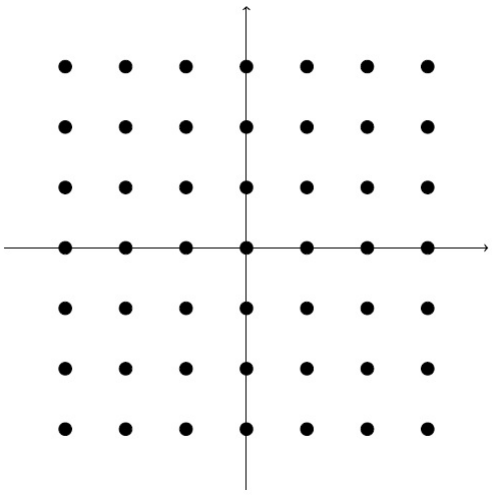
Observação 8.1.1. *Em outras palavras, um reticulado é um $\mathbb{Z}$-módulo livre de posto finito contido no $\mathbb{R}^n$, onde a base é linearmente independente sobre $\mathbb{R}$. Assim,*

$$\Lambda_B = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_m.$$

Observação 8.1.2. *Quando a base do reticulado estiver bem fixada, podemos simplesmente adotar a notação do reticulado como Λ. Em geral, trabalhamos com um reticulado completo, ou seja, quando $m = n$ e por convenção os reticulados completos serão chamados apenas de reticulados.*

Exemplo 8.1.1. *Sejam o espaço $\mathbb{R}^2$ e o reticulado $\Lambda = \{a(1,0) + b(0,1) | a, b \in \mathbb{Z}\}$, cuja base é a base canônica $\{(0,1),(1,0)\}$. Assim, $\Lambda = \mathbb{Z}^2$ e é ilustrado geometricamente na Figura (8.1).*

Figura 8.1: Ilustração do reticulado $\Lambda = \mathbb{Z}^2$.



Fonte: [3], p.182.

Um reticulado pode ter mais que uma base, e assim, a próxima proposição é uma condição necessária e suficiente para dizer se um conjunto de vetores linearmente independentes sobre $\mathbb{R}$ é uma base do reticulado em questão.

Proposição 8.1.1. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $B = \{v_1, v_2, \ldots, v_n\}$ uma base de Λ. O conjunto $C = \{w_1, w_2, \ldots, w_n\} \subseteq \Lambda$ de vetores linearmente independentes sobre $\mathbb{R}$ tal que*

$$w_i = \sum_{j=1}^{n} a_{ij} v_j, \ \textit{com } a_{ij} \in \mathbb{Z},$$

é uma base de Λ se, e somente se, $\det(a_{ij}) = \pm 1$.

Demonstração. Por hipótese os elementos de C podem ser escritos como combinação linear da base B, ou seja,

$$w_i = \sum_{j=1}^{n} a_{ij} v_j, \ \text{com } a_{ij} \in \mathbb{Z},$$

Na forma matricial, segue que

$$\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix},$$

e assim, $C = \{w_1, w_2, \ldots, w_n\}$ é uma base de Λ se, e somente se, $\det(a_{ij}) = \pm 1$, ou seja, a matriz mudança de base é inversível. □

Proposição 8.1.2. *O conjunto dos pontos de um reticulado $\Lambda \subseteq \mathbb{R}^n$ é discreto.*

Demonstração. Suponhamos $B = \{v_1, v_2, \ldots, v_n\}$ uma base para o reticulado Λ. Consideramos o sistema linear homogêneo com $n - 1$ equações e n incógnitas dado por $\langle x, v_2 \rangle, \langle x, v_3 \rangle, \ldots, \langle x, v_n \rangle$, com $x \neq 0$. Esse sistema deve possuir uma solução x não nula.

Se $\langle x, v_1\rangle = 0$, então o vetor x é ortogonal a todos os vetores de B, o que é impossível uma vez que $x \neq 0$. Portanto, $\langle x, v_1\rangle \neq 0$. Por outro lado, o vetor $s_1 = \dfrac{x}{\langle x, v_1\rangle}$ também é ortogonal a cada $v_2, v_3, \ldots, v_n$ e satisfaz $\langle s_1, v_1\rangle = 1$. Generalizando, para cada i=1,2,...,n, segue que existe um vetor s_i tal que $\langle s_i, v_i\rangle = 1$ e $\langle s_i, v_j\rangle = 0$ se $i \neq j$. Consideramos $z = \sum_{i=1}^{n} a_i v_i \in \Lambda$, com $a_i \in \mathbb{Z}$ tal que z pertence a uma bola de raio r. Logo, $a_i = \langle z, s_i\rangle$, e pela inequação de Cauchy-Schwartz, segue que $||a_i|| = ||\langle z, s_i\rangle|| \leq ||z||||s_i|| < r||s_i||$. Como $r||s_i||$ não depende de z, segue que existe um número finito de possibilidades para a_i. Portanto, o conjunto de todos os $z \in \Lambda$ tal que $||z|| < r$ é finito. Isso prova que a interseção de Λ com qualquer compacto de R^n é finito. Portanto, os pontos de Λ não são pontos de acumulação. □

Definição 8.1.2. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $B = \{v_1, v_2, \ldots, v_n\}$ uma base de Λ. O conjunto dado por*

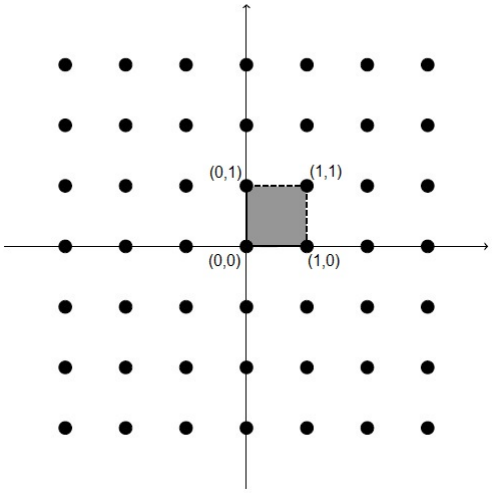
$$\mathcal{P}_B = \left\{ x = \sum_{i=1}^{n} \lambda_i v_i | 0 \leq \lambda_i < 1 \right\},$$

*é chamado de **região fundamental** do reticulado Λ.*

Observação 8.1.3. *Quando a base do reticulado estiver bem fixada, podemos simplesmente adotar a notação da região fundamental como $\mathcal{P}$.*

Exemplo 8.1.2. *A região fundamental do reticulado $\Lambda = \{a(1,0) + b(0,1) \mid a, b \in \mathbb{Z}\} = \mathbb{Z}^2$ (Exemplo 8.1.1) é o conjunto $\mathcal{P} = \{x = \lambda_1(1,0) + \lambda_2(0,1) | 0 \leq \lambda_1, \lambda_2 < 1\}$. Na Figura (8.2), a região fundamental é limitada pelos vértices do quadrado hachurado $\{(0,0), (0,1), (1,0), (1,1)\}$.*

Figura 8.2: Ilustração da região fundamental do reticulado $\Lambda = \mathbb{Z}^2$.



Fonte: Adaptado de [3], p.183.

Definição 8.1.3. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $B = \{v_1, v_2, \ldots, v_n\}$ uma base de Λ. Para $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, com $i = 1, 2, \ldots, n$ consideramos a matriz M dada por*

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

1. *A matriz M é chamada de **matriz geradora** do reticulado Λ.*
2. *O **volume do reticulado** Λ é definido por $\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\mathcal{P}) = |\det(M)|$.*
3. *A matriz $G = M^t M$ é chamada de **matriz de Gram** do reticulado Λ.*
4. *O **determinante do reticulado** Λ é definido como o determinante da matriz G, ou seja, $\det(\Lambda) = \det(G)$. O determinante do reticulado Λ também é o quadrado do volume da região fundamental de Λ, ou seja, $\det(\Lambda) = (\mathcal{V}ol(\mathcal{P}))^2$.*

As matrizes geradoras de um reticulado podem ser diferentes de acordo com a base escolhida. Assim como as matrizes de Gram, elas são simétricas, mas podem ser diferentes caso mude a base ou a matriz geradora de um mesmo reticulado. Por isso, as próximas proposições justificam as definições de volume e determinante do reticulado Λ, pois ambas independem da escolha das matrizes geradoras e matrizes de Gram.

Proposição 8.1.3. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Se M e M' são matrizes geradoras de Λ em relação as bases B e C, respectivamente, então $|\det(M)| = |\det(M')|$.*

Demonstração. Seja E a matriz mudança de base de B a C. Consideramos M e M' as matrizes geradoras de Λ em relação as bases B e C, respectivamente. Logo, $M' = EM$ e como $|\det(E)| = 1$, pelas propriedades de determinante, segue que

$$|\det(M')| = |\det(EM)| = |\det(E)\det(M)| = |\det(E)||\det(M)| = |\det(M)|.$$

Portanto, $|\det(M)| = |\det(M')|$. □

Proposição 8.1.4. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. Se G e G' são as matrizes de Gram de Λ em relação as bases B e C, respectivamente, então $\det(G) = \det(G')$.*

Demonstração. Seja E a matriz mudança de base de B a C. Consideramos M e M' as matrizes geradoras de Λ em relação as bases B e C, respectivamente. Logo, $M' = EM$ e como $|\det(E)| = 1$, pelas propriedades de determinante, segue que

$$\begin{aligned} \det(G') = \det((M')^t M') = \det(M^t E^t E M) = \det(M^t)\det(E^t)\det(E)\det(M) = \\ = \det(M^t)|\det(E)|\det(M) = \det(M^t)\det(M) = \det(M^t M) = \det(G). \end{aligned}$$

Portanto, $\det(G) = \det(G')$. □

Um empacotamento esférico é a disposição de esferas de mesmo raio no espaço euclidiano n-dimensional de tal modo que a interseção de duas delas tenha no máximo um ponto (as esferas são tangentes). Um problema associado ao empacotamento esférico é o de dispor essas esferas no espaço, de modo que elas ocupem a maior fração desse espaço, ou seja, que esta distribuição tenha alta densidade.

Em um empacotamento associado a um reticulado Λ as esferas são centradas nos pontos de Λ e necessitam terem raio máximo. Para a determinação deste raio, fixamos um número real $k > 0$ e o conjunto $\{x \in \mathbb{R}^n : ||x|| \leq k\} \cap \Lambda$. Como o conjunto $\{x \in \mathbb{R}^n : ||x|| \leq k\}$ é compacto (fechado e limitado em $\mathbb{R}^n$) e Λ é um discreto, a intersecção desses conjuntos admite ponto de mínimo. Então podemos definir o número $\Lambda_{\min} = \min\{||\lambda|| : \lambda \in \Lambda \text{ e } \lambda \neq 0\}$.

Definição 8.1.4. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $\Lambda_{\min} = \min\{||\lambda|| : \lambda \in \Lambda \text{ e } \lambda \neq 0\}$.*

1. *O número $(\Lambda_{\min})^2$ é chamado de **norma mínima** de Λ.*
2. *O maior raio para o qual é possível distribuir as esferas centradas nos pontos de Λ e obter um empacotamento é $\rho = \dfrac{\Lambda_{\min}}{2}$, e assim, ρ é chamado de **raio de empacotamento** de Λ.*

Definição 8.1.5. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e ρ o raio de empacotamento Λ. Consideramos $\mathcal{B}(0, \rho)$ a esfera de centro na origem e raio ρ. A **densidade de empacotamento** associada a Λ é definida por*

$$\Delta(\Lambda) = \frac{\textit{Volume da esfera}}{\textit{Volume da região fundamental}} = \frac{\mathcal{V}ol(\mathcal{B}(0, \rho))}{\mathcal{V}ol(\Lambda)}.$$

Observação 8.1.4. *Pelas considerações feitas na Definição 8.1.5, observamos que é possível mostrar que $\mathcal{V}ol(\mathcal{B}(0, \rho)) = \mathcal{V}ol(\mathcal{B}(0, 1))\rho^n$ utilizando recursos de integração em $\mathbb{R}^n$, ou seja,*

$$\Delta(\Lambda) = \frac{\mathcal{V}ol(\mathcal{B}(0, 1))\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Como $\mathcal{V}ol(\mathcal{B}(0, 1))$ é um valor fixo em cada dimensão n, segue que o problema do empacotamento associado a Λ se reduz ao estudo de maximizar o parâmetro

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Definição 8.1.6. *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e ρ o raio de empacotamento Λ. O parâmetro*

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)},$$

*é chamado de **densidade de centro** de Λ.*

Observação 8.1.5. *A densidade de empacotamento de Λ é igual ao produto entre o volume da esfera com centro na origem e raio 1 e a densidade de centro $\delta(\Lambda)$, ou seja, $\Delta(\Lambda) = \mathcal{V}ol(\mathcal{B}(0, 1))\delta(\Lambda)$.*

Através dos estudos sobre os reticulados, foram encontrados a densidade de centro considerada "alta" para cada dimensão, chamada de **densidade de centro ótima**. Os reticulados de densidade de centro ótima de empacotamento conhecidos são apenas nas dimensões 1 a 8 e 24. No nosso universo, trabalhamos com reticulados comparando as densidades de centro ótimas nas dimensões 2, 3, 4, 5 e 6 expressas na Tabela (8.1) obtidas pelas literaturas existentes.

Tabela 8.1: Densidade de centro ótima de dimensão menor ou igual a 6.

Dimensão	Densidade de centro ótima	Valor aproximado
2	$\frac{1}{2\sqrt{3}}$	$0,28868$
3	$\frac{1}{4\sqrt{2}}$	$0,17678$
4	$\frac{1}{8}$	$0,12500$
5	$\frac{1}{8\sqrt{2}}$	$0,08839$
6	$\frac{1}{8\sqrt{3}}$	$0,07217$

Fonte: Adaptado de [17].

8.2 Reticulados algébricos

Os reticulados algébricos são estruturas identificadas no $\mathbb{R}^n$ via um $\mathbb{Z}$-módulo livre de posto finito contido em um corpo de números $\mathbb{K}$. Nesta seção, apresentamos uma maneira de obter reticulados através da Teoria Algébrica dos Números na imersão de um corpo de números $\mathbb{K}$ no $\mathbb{R}^n$ de modo que a imagem de ideais ($\mathbb{Z}$-módulos livres) no anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$, corresponda a reticulados neste espaço.

Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n, θ o elemento primitivo de $\mathbb{K}$ e $p(x)$ o polinômio minimal de θ, onde $\partial(p) = n$. Pelo Teorema 2.3.2, segue que existem exatamente n $\mathbb{Q}$-monomorfismos distintos $\sigma_k : \mathbb{K} \to \mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e que $\sigma_k(\theta) = \theta_k$, onde θ_k são as raízes de $p(x)$, para $k = 1, 2, \ldots, n$ e por convenção consideramos $\theta_1 = \theta$.

Definição 8.2.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Os $\mathbb{Q}$-monomorfismos σ_k, para $k = 1, 2, \ldots, n$, recebem as seguintes nomenclaturas:*

1. *Se $\sigma_k(\mathbb{K}) \subset \mathbb{R}$, o monomorfismo σ_k é chamado **real**.*

2. *Se $\sigma_k(\mathbb{K}) \not\subset \mathbb{R}$, o monomorfismo σ_k é chamado **imaginário**.*

Definição 8.2.2. *Seja $\mathbb{K}$ um corpo de números de grau n. O corpo $\mathbb{K}$ recebe as seguintes nomenclaturas de acordo com os $\mathbb{Q}$-monomorfismos:*

1. *Se todos os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ são reais, o corpo $\mathbb{K}$ é chamado de **corpo totalmente real**.*

2. *Se todos os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ são imaginários, o corpo $\mathbb{K}$ é chamado de **corpo totalmente imaginário**.*

3. *Caso contrário, se $\mathbb{K}$ possui $\mathbb{Q}$-monomorfismos reais e imaginários, o corpo $\mathbb{K}$ é chamado de **corpo misto**.*

Consideramos r_1 o número que representa a quantidade de índices k tal que $\sigma_k(\mathbb{K}) \subset \mathbb{K}$, ou seja, são reais. Sendo assim, $n - r_1$ é um número par. Portanto, existe um número natural r_2 tal que $r_1 + 2r_2 = n$. Logo, vamos reordenar os $\mathbb{Q}$-monomorfismos σ_k.

- Se $\sigma_k(\mathbb{K}) \subset \mathbb{R}$, então $1 \leq k \leq r_1$.
- Se $\sigma_k(\mathbb{K}) \not\subset \mathbb{R}$, então $\sigma_{k+r_2}(\mathbb{K}) = \overline{\sigma_k(\mathbb{K})}$, para $r_1 + 1 \leq k \leq r_1 + r_2$.

Pela construção, os primeiros $r_1 + r_2$ monomorfismos determinam os últimos r_2. Logo, para cada $x \in \mathbb{K}$ podemos definir

$$\begin{aligned} \sigma_{\mathbb{K}} : \mathbb{K} &\to \mathbb{R}^n \\ x &\mapsto \sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}. \end{aligned} \tag{8.1}$$

Definição 8.2.3. *A aplicação $\sigma_{\mathbb{K}}$ definida na Equação (8.1) é um homomorfismo injetor de anéis, chamado* ***homomorfismo de Minkowski*** *ou* ***homomorfismo canônico*** *de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ como $\mathbb{R}^n$, e este homomorfismo pode ser visto como*

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

onde $\Re(x)$ representa a parte real de x e $\Im(x)$ representa a parte imaginária de x.

Observação 8.2.1. *Pela teoria de Números Complexos, a seguinte relação é válida para $x \in \mathbb{C}$,*

$$(\Re(x))^2 + (\Im(x))^2 = x\overline{x},$$

onde $\overline{x}$ é o conjugado de x.

Exemplo 8.2.1. *Seja $\mathbb{K} = \mathbb{Q}(i)$ o corpo gaussiano, onde i é a unidade imaginária. Para $\alpha = a + bi \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, segue que os monomorfismos $\sigma_1(\alpha) = a + bi = id(\alpha)$ e $\sigma_2(\alpha) = a - bi = \overline{(\sigma_1(\alpha))}$. Logo, para este caso, $r_1 = 0$ e $r_2 = 1$. Portanto, para qualquer α, o homomorfismo de Minkowski associado a $\mathbb{K}$ é dado por $\sigma_{\mathbb{K}}(\alpha) = (\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha))) = (a, b)$.*

Teorema 8.2.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{M} \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, então $\sigma_{\mathbb{K}}(\mathcal{M}) \subset \mathbb{R}^n$ é um reticulado.*

Demonstração. Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(\alpha_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$(\sigma_1(\alpha_j), \cdots, \sigma_{r_1}(\alpha_j), \Re(\sigma_{r_1+1}(\alpha_j)), \Im(\sigma_{r_1+1}(\alpha_j)), \ldots, \Re(\sigma_{r_1+r_2}(\alpha_j)), \Im(\sigma_{r_1+r_2}(\alpha_j))). \tag{8.2}$$

Agora, calculamos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (8.2), fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z + \bar{z})$, $\Im(z) = \frac{1}{2i}(z - \bar{z})$ para $z \in \mathbb{C}$ e das transformações elementares no determinante, a saber, pela adição da $(r_1 + 2l)$-ésima linha a sua anterior e em seguida pela subtração da $(r_1 + 2l - 1)$-ésima coluna da sua posterior, para $l = 1, 2, \cdots, r_2$. A matriz geradora G do reticulado é dada por

$$D = \det \begin{bmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_j) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \ldots & \sigma_2(\alpha_j) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \ldots & \sigma_{r_1}(\alpha_j) & \ldots & \sigma_{r_1}(\alpha_n) \\ \Re(\sigma_{r_1+1}(\alpha_1)) & \ldots & \Re(\sigma_{r_1+1}(\alpha_j)) & \ldots & \Re(\sigma_{r_1+1}(\alpha_n)) \\ \Im(\sigma_{r_1+1}(\alpha_1)) & \ldots & \Im(\sigma_{r_1+1}(\alpha_j)) & \ldots & \Im(\sigma_{r_1+1}(\alpha_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sigma_{r_1+r_2}(\alpha_1)) & \ldots & \Re(\sigma_{r_1+r_2}(\alpha_j)) & \ldots & \Re(\sigma_{r_1+r_2}(\alpha_n)) \\ \Im(\sigma_{r_1+r_2}(\alpha_1)) & \ldots & \Im(\sigma_{r_1+r_2}(\alpha_j)) & \ldots & \Im(\sigma_{r_1+r_2}(\alpha_n)) \end{bmatrix}.$$

Assim,

$$D = \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2} \det(D_1),$$

onde D_1 é a seguinte matriz

$$\begin{bmatrix}
\sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\
\sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\
\sigma_{r_1+1}(\alpha_1) + \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) + \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) + \overline{\sigma_{r_1+1}(\alpha_n)} \\
\sigma_{r_1+1}(\alpha_1) - \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) - \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) - \overline{\sigma_{r_1+1}(\alpha_n)} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1+r_2}(\alpha_1) + \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) + \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) + \overline{\sigma_{r_1+r_2}(\alpha_n)} \\
\sigma_{r_1+r_2}(\alpha_1) - \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) - \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) - \overline{\sigma_{r_1+r_2}(\alpha_n)}
\end{bmatrix},$$

e desse modo,

$$D = \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2} 2^{r_2} \det(D_2),$$

onde D_2 é a seguinte matriz

$$\begin{bmatrix}
\sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\
\sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\
\sigma_{r_1+1}(\alpha_1) + \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) + \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) + \overline{\sigma_{r_1+1}(\alpha_n)} \\
\sigma_{r_1+1}(\alpha_1) - \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) - \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) - \overline{\sigma_{r_1+1}(\alpha_n)} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1+r_2}(\alpha_1) + \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) + \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) + \overline{\sigma_{r_1+r_2}(\alpha_n)} \\
\sigma_{r_1+r_2}(\alpha_1) - \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) - \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) - \overline{\sigma_{r_1+r_2}(\alpha_n)}
\end{bmatrix}.$$

Logo,

$$D = (-1)^{r_2} \left(\frac{1}{2}\right)^{\frac{r_2}{2}} \left(\frac{1}{2i}\right)^{r_2} 2^{r_2} \det \begin{bmatrix}
\sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\
\sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\
\sigma_{r_1+1}(\alpha_1) & \dots & \sigma_{r_1+1}(\alpha_j) & \dots & \sigma_{r_1+1}(\alpha_n) \\
\overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \overline{\sigma_{r_1+1}(\alpha_n)} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1+r_2}(\alpha_1) & \dots & \sigma_{r_1+r_2}(\alpha_j) & \dots & \sigma_{r_1+r_2}(\alpha_n) \\
\overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \overline{\sigma_{r_1+r_2}(\alpha_n)}
\end{bmatrix},$$

ou seja,

$$D = \left(\frac{1}{2i}\right)^{r_2} \det \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \dots & \sigma_{r_1+1}(\alpha_j) & \dots & \sigma_{r_1+1}(\alpha_n) \\ \sigma_{r_1+2}(\alpha_1) & \dots & \sigma_{r_1+2}(\alpha_j) & \dots & \sigma_{r_1+2}(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(\alpha_1) & \dots & \sigma_{r_1+2r_2}(\alpha_j) & \dots & \sigma_{r_1+2r_2}(\alpha_n) \end{bmatrix} = (2i)^{-r_2} \det(\sigma_j(\alpha_k)).$$

Portanto, $D = (2i)^{-r_2} \det(\sigma_j(\alpha_i))$, onde $j, i = 1, \dots, n$. Como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, pelo Corolário 2.5.3, segue que $\det(\sigma_j(\alpha_i)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(\alpha_j)$ do $\mathbb{R}^n$ são linearmente independente e geram $\sigma_{\mathbb{K}}(\mathcal{M})$, ou seja, $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado do $\mathbb{R}^n$. □

Corolário 8.2.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{M} \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com base $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$, então o volume do reticulado $\sigma_{\mathbb{K}}(\mathcal{M})$ é dado por*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{M})) = \frac{|\det(\sigma_i(\alpha_j))|}{2^{r_2}}. \tag{8.3}$$

Demonstração. Considerando as informações obtidas no Teorema 8.2.1, como $\{\alpha_1, \cdots, \alpha_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$, segue que $m = \sum_{j=1}^{n} a_j \alpha_j$, com $a_j \in \mathbb{Z}$, e portanto, $m \in \mathcal{M}$. Assim, $\sigma_{\mathbb{K}}(m) = \sum_{j=1}^{n} a_j \sigma(\alpha_j)$, com $a_j \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{K}}(\mathcal{M}) = \left\{ \sum_{j=1}^{n} a_j \sigma(\alpha_j); a_j \in \mathbb{Z} \right\}$. Logo,

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{M})) = |D| = \frac{|\det(\sigma_i(\alpha_j))|}{2^{r_2}},$$

o que prova o corolário. □

Definição 8.2.4. *Seja $\mathbb{K}$ um corpo de números de grau n e $\mathcal{M} \subset \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n. O reticulado $\sigma_{\mathbb{K}}(\mathcal{M}) \subset \mathbb{R}^n$ (Teorema 8.2.1) é chamado de* ***reticulado algébrico****.*

Observação 8.2.2. *Se não houver dúvidas que $\mathbb{K}$ é um corpo de números, então podemos simplesmente dizer que $\sigma_K(\mathcal{M})$ é um reticulado.*

Proposição 8.2.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n, então*

1. *$\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado algébrico.*
2. *O volume do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é dado por*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{M})) = \frac{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}{2^{r_2}}. \tag{8.4}$$

3. *A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathcal{M})))^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}. \tag{8.5}$$

Demonstração. Vamos provar os itens da proposição.

1. Por hipótese, como $\mathcal{M}$ é um $\mathbb{Z}$-módulo livre de posto n, pelo Teorema 8.2.1, segue que $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado algébrico.

2. Pelo Teorema 2.1.3, segue que existe uma base integral $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de $\mathbb{K}$ e inteiros não nulos $a_1, a_2, \ldots, a_n$ tal que $\{a_1\alpha_1, a_2\alpha_2, \ldots, a_n\alpha_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$. Logo, pelo Corolário 8.2.1, segue que

$$\mathcal{V}ol(\sigma(\mathcal{M})) = \frac{|\det(\sigma_i(\alpha_j))|}{2^{r_2}} = \frac{|\det(\sigma_i(\alpha_j))||a_1a_2\cdots a_n|}{2^{r_2}}.$$

   Como $|\det(\sigma_i(\alpha_j))| = \sqrt{|\mathcal{D}(\mathbb{K})|}$ (pela Proposição 2.5.3 e por $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ ser uma base integral) e $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}] = |a_1a_2\cdots a_n|$, segue que

$$\mathcal{V}ol(\sigma(\mathcal{M})) = \frac{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}{2^{r_2}}.$$

3. Pela definição de densidade de centro de um reticulado e pelo item (2) desta proposição, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M})) = \frac{\rho(\sigma_{\mathbb{K}}(\mathcal{M})))^n}{\mathcal{V}ol(\sigma(\mathcal{M}))} = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathcal{M})))^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}.$$

Portanto, segue o resultado. □

Corolário 8.2.2. *Seja $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$, então*

1. *$\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é um reticulado algébrico.*

2. *O volume do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dado por*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{\sqrt{|\mathcal{D}(\mathbb{K})|}}{2^{r_2}}. \tag{8.6}$$

3. *A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})))^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}}. \tag{8.7}$$

Demonstração. Pelo Corolário 2.4.3, segue que $\mathcal{O}_{\mathbb{K}}$ é um Z-módulo livre de posto n e de imediato $[\mathcal{O}_{\mathbb{K}} : \mathcal{O}_{\mathbb{K}}] = 1$. Portanto, pela Proposição 8.2.1, segue que os itens deste corolário são satisfeitos. □

Observação 8.2.3. *Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal, então $\mathcal{I}$ é um $\mathbb{Z}$-módulo livre de posto n (Corolário 2.4.4) e pela Proposição 8.2.1, segue que $\sigma_{\mathbb{K}}(\mathcal{I})$ é um reticulado algébrico. O volume e a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{I})$ são dados pela Proposição 8.2.1 com uma pequena sutiliza ao definir a norma de um ideal como $\mathcal{N}(\mathcal{I}) = [\mathcal{O}_{\mathbb{K}} : \mathcal{I}]$.*

Pela Teoria Algébrica dos Números é possível construir reticulados em uma dimensão n utilizando $\mathbb{K}$ um corpo de números de grau n a partir de $\mathcal{O}_\mathbb{K}$ o anel dos inteiros algébricos de $\mathbb{K}$ (também é possível construir reticulados a partir dos ideias de $\mathcal{O}_\mathbb{K}$). Para construir $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ um reticulado algébrico e obter sua densidade de centro é preciso os seguintes passos.

1. Conhecer a estrutura de $\mathcal{O}_\mathbb{K}$ (anel dos inteiros algébricos de $\mathbb{K}$);
2. Conhecer a estrutura de $\mathcal{D}(\mathbb{K})$ (discriminante da base integral);
3. Calcular $||\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})||^2$ (norma mínima dos elementos de $\mathcal{O}_\mathbb{K}$);
4. Obter $\rho = \dfrac{||\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})||}{2}$ (raio de empacotamento do reticulado);
5. Calcular $\delta(\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})) = \dfrac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}}$ (densidade de centro do reticulado).

8.3 Aplicações nas extensões quadráticas

Nesta seção, as referências citadas farão menção ao Capítulo 3 de Extensões Quadráticas. O objetivo é encontrar $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ reticulados algébricos via $\mathbb{K} = \mathbb{Q}(\theta)$ corpo de números de grau 2, onde o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ é $p(x) = x^2 + ax + b$, com a e b não nulos, ou $p(x) = x^2 - d$, com d livre de quadrados. Para obter a norma mínima do reticulado algébrico $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ utilizamos o programa Wolfram Mathematica 11.3, assim como também o exploramos para obter exemplos.

8.3.1 Reticulados na quádrica $p(x) = x^2 + ax + b$

Consideramos $p(x) = x^2 + ax + b$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta_k$, e θ_k é uma raiz de $p(x)$, para $k = 1, 2$. Por convenção, seja $\theta_1 = \theta$.

Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta | a_0, a_1 \in \mathbb{Z}\}.$$

Pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta) = a^2 - 4b.$$

Pela Tabela (8.1), segue que a densidade de centro ótima para a dimensão 2 é

$$\delta = \frac{1}{2\sqrt{3}} \approx 0,28868.$$

Teorema 8.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números e $p(x) = x^2 + ax + b$ o polinômio minimal de θ, com a e b não nulos. Se $\mathcal{D}(\mathbb{K})$ é livre de quadrados, então densidade de centro do reticulado algébrico $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é dada por*

$$\delta(\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})) = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

Demonstração. Por hipótese, como $\mathcal{D}(\mathbb{K})$ é livre de quadrados, pela Proposição 2.5.5, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha = a_0 + a_1\theta, \quad \text{com} \quad a_0, a_1 \in \mathbb{Z}.$$

Para este caso os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_1(\theta) = \theta_1$ e $\sigma_2(\theta) = \theta_2$. Dividimos a demonstração em casos de acordo com o corpo $\mathbb{K}$:

1. Se $\mathbb{K}$ é totalmente real de grau $n = 2$, então $r_1 = 2$ e $r_2 = 0$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_2(\alpha))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 = \\ &= (a_0 + a_1\theta_1)^2 + (a_0 - a_1\theta_2)^2 = \\ &= 2a_0^2 + 2a_0a_1(\theta_1 + \theta_2) + a_1^2(\theta_1^2 + \theta_2^2). \end{aligned}$$

   Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

   Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\left(\frac{\sqrt{2}}{2}\right)^2}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

2. Se $\mathbb{K}$ é totalmente imaginário de grau $n = 2$, então $r_1 = 0$ e $r_2 = 1$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)))||^2 = \\ &= \Re^2(\sigma_1(\alpha)) + \Im^2(\sigma_1(\alpha)) = \\ &= \sigma_1(\alpha)\overline{\sigma_1(\alpha)} = \\ &= \sigma_1(\alpha)\sigma_2(\alpha) = \\ &= (a_0 + a_1\theta_1)(a_0 + a_1\theta_2) = \\ &= a_0^2 + a_0a_1(\theta_1 + \theta_2) + a_1^2(\theta_1\theta_2). \end{aligned}$$

   Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Assim,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 1 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 1 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{1}{2}.$$

   Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{1}{2}\right)^2}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

Portanto, dos itens (1) e (2), segue o resultado. □

Exemplo 8.3.1. *Seja $\mathbb{K}$ um corpo de números de grau 2. Sob as condições do Teorema 8.3.1, obtemos densidade de centro ótima do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^2 - 5x + 7$ é o minimal de θ. Neste caso, $\mathbb{K}$ é totalmente imaginário, pois $\theta_1 = \dfrac{5 + i\sqrt{3}}{2}$ e $\theta_2 = \dfrac{5 - i\sqrt{3}}{2}$. Como $\mathcal{D}(\mathbb{K}) = -3$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{2\sqrt{3}} \approx 0,28868.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^2 + x + 1$ é o minimal de θ. Neste caso, $\mathbb{K}$ é totalmente imaginário, pois $\theta_1 = \dfrac{-1 + i\sqrt{3}}{2}$ e $\theta_2 = \dfrac{-1 - i\sqrt{3}}{2}$. Como $\mathcal{D}(\mathbb{K}) = -3$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{2\sqrt{3}} \approx 0,28868.$$

8.3.2 Reticulados na quádrica $p(x) = x^2 - d$

Consideramos $p(x) = x^2 - d$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ e os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são σ_1 e σ_2 que fixam os elementos de $\mathbb{Q}$ e $\sigma_1(\theta) = \theta$ e $\sigma_2(\theta) = -\theta$.

Pelo Teorema 3.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta, \text{ se } d \not\equiv 1 (mod\ 4) \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\theta}{2}\right), \text{ se } d \equiv 1 (mod\ 4). \end{cases}$$

Pela Proposição 3.3.4, segue que o discriminante do anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 4d, \text{ se } d \not\equiv 1 (mod\ 4) \\ d, \text{ se } d \equiv 1 (mod\ 4). \end{cases}$$

Pela Tabela (8.1), segue a densidade de centro ótima para a dimensão 2 é

$$\delta = \frac{1}{2\sqrt{3}} \approx 0,28868.$$

Teorema 8.3.2. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt{d}$ com $d \in \mathbb{Z}_+^*$ livre de quadrados. A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de $\mathbb{K}$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{1}{4\sqrt{d}}, \text{ se } d \not\equiv 1 (mod\ 4) \\ \dfrac{1}{2\sqrt{d}}, \text{ se } d \equiv 1 (mod\ 4). \end{cases}$$

Demonstração. Suponhamos que d é um inteiro positivo e livre de quadrados. Dessa forma, $\theta = \sqrt{d} \in \mathbb{K}$. Para este caso, os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_1(\theta) = \theta$ e $\sigma_2(\theta) = -\theta$, e assim, $\mathbb{K}$ é um corpo totalmente real de grau $n = 2$, onde $r_1 = 2$ e $r_2 = 0$. Vamos dividir esta demonstração em casos de acordo com a base integral obtida no Teorema 3.3.1:

1. Seja $d \not\equiv 1(mod\ 4)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 3.3.1, segue que

$$\alpha = a_0 + a_1\theta, \text{com } a_0, a_1 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_2(\alpha))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 = \\ &= (a_0 + a_1\theta)^2 + (a_0 - a_1\theta)^2 = \\ &= 2(a_0^2 + a_1^2 d). \end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Como $d \not\equiv 1(mod\ 4)$, pela Proposição 3.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 4d$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\left(\frac{\sqrt{2}}{2}\right)^2}{\sqrt{4d}} = \frac{1}{4\sqrt{d}}.$$

2. Seja $d \equiv 1(mod\ 4)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 3.3.1, segue que

$$\alpha = a_0 + a_1\left(\frac{1+\theta}{2}\right), \text{com } a_0, a_1 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_2(\alpha))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 = \\ &= \left(a_0 + a_1\left(\frac{1+\theta}{2}\right)\right)^2 + \left(a_0 + a_1\left(\frac{1-\theta}{2}\right)\right)^2 = \\ &= \frac{4a_0^2 + 4a_0a_1 + a_1^2 + a_1^2 d}{2}. \end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Como $d \equiv 1(mod\ 4)$, pela Proposição 3.3.4, segue que $|\mathcal{D}(\mathbb{K})| = d$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\left(\frac{\sqrt{2}}{2}\right)^2}{\sqrt{d}} = \frac{1}{2\sqrt{d}}.$$

Portanto, dos itens (1) e (2), segue o resultado. □

Exemplo 8.3.2. *Seja $\mathbb{K}$ um corpo de números de grau 2. Sob as condições do Teorema 8.3.2, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Como $d = 2$ e $2 \not\equiv 1(mod\ 4)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{4\sqrt{2}} \approx 0,17677.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Como $d = 5$ e $5 \equiv 1(mod\ 4)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2\sqrt{2}} \approx 0,22360.$$

Teorema 8.3.3. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = d$ com $\sqrt{d} \in \mathbb{Z}^*_-$ livre de quadrados. A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de $\mathbb{K}$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{1}{4\sqrt{|d|}}, \text{ se } d \not\equiv 1(mod\ 4) \\ \dfrac{1}{2\sqrt{|d|}}, \text{ se } d \equiv 1(mod\ 4). \end{cases}$$

Demonstração. Suponhamos que d é um inteiro negativo e livre de quadrados. Dessa forma, $\theta = \sqrt{d} \in \mathbb{C}$. Para este caso, os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_1(\theta) = \theta$ e $\sigma_2(\theta) = -\theta$, e assim, $\mathbb{K}$ é um corpo totalmente imaginário de grau $n = 2$, onde $r_1 = 0$ e $r_2 = 1$. Vamos dividir esta demonstração em casos de acordo com a base integral obtida no Teorema 3.3.1:

1. Seja $d \not\equiv 1(mod\ 4)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 3.3.1, segue que

$$\alpha = a_0 + a_1\theta, \text{com } a_0, a_1 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)))||^2 = \\ &= \Re^2(\sigma_1(\alpha)) + \Im^2(\sigma_1(\alpha)) = \\ &= \sigma_1(\alpha)\overline{\sigma_1(\alpha)} = \\ &= \sigma_1(\alpha)\sigma_2(\alpha) = \\ &= (a_0 + a_1\theta)(a_0 - a_1\theta) = \\ &= (a_0^2 - a_1^2 d). \end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 1 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 1 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{1}{2}.$$

Como $d \not\equiv 1(mod\ 4)$, pela Proposição 3.3.4, segue que $|\mathcal{D}(\mathbb{K})| = |4d| = 4|d|$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{1}{2}\right)^2}{\sqrt{4|d|}} = \frac{1}{4\sqrt{|d|}}.$$

2. Seja $d \equiv 1(mod\ 4)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 3.3.1, segue que

$$\alpha = a_0 + a_1\left(\frac{1+\theta}{2}\right), \text{com } a_0, a_1 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)))||^2 = \\
&= \Re^2(\sigma_1(\alpha)) + \Im^2(\sigma_1(\alpha)) = \\
&= \sigma_1(\alpha)\overline{\sigma_1(\alpha)} = \\
&= \sigma_1(\alpha)\sigma_2(\alpha) = \\
&= \left(a_0 + a_1\left(\frac{1+\theta}{2}\right)\right)\left(a_0 + a_1\left(\frac{1-\theta}{2}\right)\right) \\
&= \frac{4a_0^2 + 4a_0a_1 + a_1^2 - a_1^2 d}{4}.
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 1 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 1 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{1}{2}.$$

Como $d \equiv 1(mod\ 4)$, pela Proposição 3.3.4, segue que $|\mathcal{D}(\mathbb{K})| = |d|$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{1}{2}\right)^2}{\sqrt{|d|}} = \frac{1}{2\sqrt{|d|}}.$$

Portanto, dos itens (1) e (2), segue o resultado. □

Exemplo 8.3.3. *Seja $\mathbb{K}$ um corpo de números de grau 2. Sob as condições do Teorema 8.3.3, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$. Como $d = -2$ e $-2 \not\equiv 1(mod\ 4)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{4\sqrt{|-2|}} = \frac{1}{4\sqrt{2}} = \approx 0,17677.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Como $d = -3$ e $-3 \equiv 1(mod\ 4)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2\sqrt{|-3|}} = \frac{1}{2\sqrt{3}} \approx 0,28868.$$

8.4 Aplicações nas extensões cúbicas

Nesta seção, as referências citadas farão menção ao Capítulo 4 de Extensões Cúbicas. O objetivo é encontrar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ reticulados algébricos via $\mathbb{K} = \mathbb{Q}(\theta)$ corpo de números de grau 3, onde o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ é $p(x) = x^3 + ax + b$, com a e b não nulos, ou $p(x) = x^3 - d$, com d livre de quadrados.

8.4.1 Reticulados na cúbica $p(x) = x^3 + ax + b$

Consideramos $p(x) = x^3 + ax + b$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$, e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta_k$, e θ_k é uma raiz de $p(x)$, para $k = 1, 2, 3$. Por convenção, seja $\theta_1 = \theta$.

Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 | a_0, a_1, a_2 \in \mathbb{Z}\}.$$

Pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2) = -(4a^3 + 27b^2).$$

Pela Tabela (8.1), segue que a densidade de centro ótima para a dimensão 3 é dada por

$$\delta = \frac{1}{4\sqrt{2}} \approx 0,17678.$$

Teorema 8.4.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números e $p(x) = x^3 + ax + b$ o polinômio minimal de θ, com a e b não nulos. Se $\mathcal{D}(\mathbb{K})$ é livre de quadrados, então a densidade de centro do reticulado algébrico $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é dada por*

$$\delta(\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})) = \begin{cases} \dfrac{9}{8\sqrt{3|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem 3 raízes reais,} \\ \dfrac{1}{\sqrt{2|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem somente 1 raiz real.} \end{cases}$$

Demonstração. Por hipótese, como $\mathcal{D}(\mathbb{K})$ é livre de quadrados, pela Proposição 2.5.5, segue que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$. Seja $\alpha \in \mathcal{O}_\mathbb{K}$, então

$$\alpha = a_0 + a_1\theta + a_2\theta^2, \text{com } a_0, a_1, a_2 \in \mathbb{Z}.$$

Para este caso os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta_k$, para $k = 1, 2, 3$. Dividimos esta demonstração em casos de acordo com o corpo $\mathbb{K}$.

1. Se $\mathbb{K}$ é totalmente real de grau $n = 3$, ou seja, θ_1, θ_2 e θ_3 são reais, então $r_1 = 3$ e $r_2 = 0$. Ao calcular a norma mínima de $\sigma_\mathbb{K}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_\mathbb{K}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_2(\alpha)), \sigma_3(\alpha))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 = \\ &= (a_0 + a_1\theta_1 + a_2\theta_1^2)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2)^2 + (a_0 + a_1\theta_3 + a_2\theta_3^2)^2 = \\ &= 3a_0^2 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3^2) + 2a_1a_2(\theta_1^3 + \theta_2^3 + \theta_3^3) + a_2^2(\theta_1^4 + \theta_2^4 + \theta_3^4) + \\ &+ 2a_0(a_1(\theta_1 + \theta_2 + \theta_3) + a_2(\theta_1^2 + \theta_2^2 + \theta_3^2)). \end{aligned}$$

   Assim, $||\sigma_\mathbb{K}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = 0$. Desse modo,

$$||\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})||^2 = 3 \Leftrightarrow ||\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})||}{2} = \frac{\sqrt{3}}{2}.$$

   Portanto, a densidade de centro de $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é dada por

$$\delta(\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\left(\frac{\sqrt{3}}{2}\right)^3}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{9}{8\sqrt{3|\mathcal{D}(\mathbb{K})|}}.$$

2. Se $\mathbb{K}$ é misto de grau $n = 3$, ou seja, θ_1 é real e θ_2 e θ_3 são imaginárias, então $r_1 = 2$ e $r_2 = 1$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_3(\alpha) = \\
&= (a_0 + a_1\theta_1 + a_2\theta_1^2)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2)(a_0 + a_1\theta_3 + a_2\theta_3^2) = \\
&= 2a_0^2 + 2a_1a_2\theta_1^3 + a_1a_2\theta_2\theta_3(\theta_2 + \theta_3) + a_0a_1(2\theta_1 + \theta_2 + \theta_3) + \\
&+ a_1^2(\theta_1^2 + \theta_2\theta_3) + a_0a_2(2\theta_1^2 + \theta_2^2 + \theta_3^2) + a_2^2(\theta_1^4 + \theta_2^2\theta_3^2).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{2}}{2}\right)^3}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{\sqrt{2|\mathcal{D}(\mathbb{K})|}}.$$

Portanto, dos itens (1) e (2), segue o resultado. □

Exemplo 8.4.1. *Seja $\mathbb{K}$ um corpo de números de grau 3. Sob as condições do Teorema 8.4.1, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^3 - x - 1$ é o minimal de θ. Neste caso, $p(x)$ tem somente 1 raiz real. Como $\mathcal{D}(\mathbb{K}) = -23$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{2\sqrt{23}} \approx 0,10425.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^3 + x + 1$ é o minimal de θ. Neste caso, $p(x)$ tem somente 1 raiz real. Como $\mathcal{D}(\mathbb{K}) = -31$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{2\sqrt{31}} \approx 0,08980.$$

8.4.2 Reticulados na cúbica $p(x) = x^3 - d$

Consideramos $p(x) = x^3 - d$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta\xi_3^{k-1}$, onde $k = 1, 2, 3$.

Pelo Teorema 4.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-2\theta+\theta^2}{3}\right), \text{ se } d \equiv 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-\theta+\theta^2}{3}\right), \text{ se } d \equiv -1 (mod\ 9). \end{cases}$$

Pela Proposição 4.3.4, segue que o discriminante do anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\begin{cases} -27d^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ -3d^2, \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

Pela Tabela (8.1), segue a densidade de centro ótima para a dimensão 3 é

$$\delta = \frac{1}{4\sqrt{2}} \approx 0,17678.$$

Teorema 8.4.2. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[3]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de $\mathbb{K}$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{1}{\sqrt{54d^2}}, \text{ se } d \not\equiv \pm 1 (mod\ 9), \\ \dfrac{1}{\sqrt{6d^2}}, \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

Demonstração. Suponhamos que d é um inteiro positivo e livre de quadrados. Dessa forma, $\theta = \sqrt[3]{d} \in \mathbb{K}$. Para este caso, os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta\xi_3^{k-1}$, com $1 \leq k \leq 3$ e assim, $\mathbb{K}$ é um corpo misto de grau $n = 3$, onde $r_1 = 1$ e $r_2 = 1$. Vamos dividir esta demonstração em casos de acordo com a base integral obtida no Teorema 4.3.1:

1. Seja $d \not\equiv \pm 1 (mod\ 9)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 4.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2, \text{com } a_0, a_1, a_2 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\ &= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\ &= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\ &= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_3(\alpha) = \\ &= (a_0 + a_1\theta + a_2\theta^2)^2 + (a_0 + a_1\theta\xi_3 + a_2\theta^2\xi_3^2)(a_0 + a_1\theta\xi_3^2 + a_2\theta^2\xi_3) = \\ &= 2a_0^2 + a_0a_1\theta + 2a_1^2\theta^2 + a_0a_1\theta^2 + a_1a_2d + 2a_2d\theta. \end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Como $d \not\equiv \pm 1 (mod\ 9)$, pela Proposição 4.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 27d^2$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\dfrac{\sqrt{2}}{2}\right)^3}{\sqrt{27d^2}} = \frac{1}{\sqrt{54d^2}}.$$

2. Seja $d \equiv 1(mod\ 9)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 4.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\left(\frac{-2-2\theta+\theta^2}{3}\right), \text{com } a_0, a_1, a_2 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
&||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_3(\alpha) = \\
&= \left(a_0 + a_1\theta + a_2\left(\frac{-2-2\theta+\theta^2}{3}\right)\right)^2 + \left(a_0 + a_1\theta\xi_3 + a_2\left(\frac{-2-2\theta\xi_3+\theta^2\xi_3^2}{3}\right)\right) \times \\
&\times \left(a_0 + a_1\theta\xi_3^2 + a_2\left(\frac{-2-2\theta\xi_3^2+\theta^2\xi_3}{3}\right)\right) \\
&= \frac{1}{9}(18a_0^2 - 24a_0a_2 + 8a_2^2 + 9a_0a_1\theta - 6a_0a_2\theta - 6a_1a_2\theta + 4a_2\theta + 18a_1^2\theta^2 + 3a_0a_2\theta^2 - \\
&- 24a_1a_2\theta^2 + 6a_2^2\theta^2 + 3a_1a_2d - 2a_2^2d + 2a_2^2d\theta).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Como $d \equiv 1(mod\ 9)$, pela Proposição 4.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 3d^2$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{2}}{2}\right)^3}{\sqrt{3d^2}} = \frac{1}{\sqrt{6d^2}}.$$

3. Seja $d \equiv -1(mod\ 9)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 4.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\left(\frac{-2-\theta+\theta^2}{3}\right), \text{com } a_0, a_1, a_2 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
&||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_3(\alpha) = \\
&= \left(a_0 + a_1\theta + a_2\left(\frac{-2-\theta+\theta^2}{3}\right)\right)^2 + \left(a_0 + a_1\theta\xi_3 + a_2\left(\frac{-2-\theta\xi_3+\theta^2\xi_3^2}{3}\right)\right) \times \\
&\times \left(a_0 + a_1\theta\xi_3^2 + a_2\left(\frac{-2-\theta\xi_3^2+\theta^2\xi_3}{3}\right)\right) \\
&= \frac{1}{9}(18a_0^2 - 24a_0a_2 + 8a_2^2 + 9a_0a_1\theta - 6a_1a_2\theta + 2a_2^2\theta + 18a_1^2\theta^2 + 3a_0a_2\theta^2 - \\
&- 12a_1a_2\theta^2 + 3a_1a_2d - a_2^2d + 2a_2^2d\theta).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Como $d \equiv -1(mod\ 9)$, pela Proposição 4.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 3d^2$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{2}}{2}\right)^3}{\sqrt{3d^2}} = \frac{1}{\sqrt{6d^2}}.$$

Portanto, dos itens (1), (2) e (3), segue o resultado. □

Exemplo 8.4.2. *Seja $\mathbb{K}$ um corpo de números de grau 3. Sob as condições do Teorema 8.4.2, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[3]{6})$. Como $d = 6$ e $6 \not\equiv 1(mod\ 9)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{\sqrt{54 \times 6^2}} = \frac{1}{\sqrt{2}} \approx 0,02268.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[3]{17})$. Como $d = 17$ e $17 \equiv -1(mod\ 9)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{\sqrt{6 \times 17^2}} \approx 0,02401.$$

8.5 Aplicações nas extensões quárticas

Nesta seção, as referências citadas farão menção ao Capítulo 5 de Extensões Quárticas. O objetivo é encontrar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ reticulados algébricos via $\mathbb{K} = \mathbb{Q}(\theta)$ corpo de números de grau 4, onde o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ é $p(x) = x^4 + ax + b$, com a e b não nulos, ou $p(x) = x^4 - d$, com $d \in \mathbb{Z}_+$ livre de quadrados.

8.5.1 Reticulados na quártica $p(x) = x^4 + ax + b$

Consideramos $p(x) = x^4 + ax + b$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$, e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta_k$, e θ_k é uma raiz de $p(x)$, para $k = 1, 2, 3, 4$. Por convenção, seja $\theta_1 = \theta$.

Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2, \theta^3)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 | a_0, a_1, a_2, a_3 \in \mathbb{Z}\}.$$

Pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3) = -27a^4 + 256b^3.$$

Pela Tabela (8.1), segue que a densidade de centro ótima para a dimensão 4 é dada por

$$\delta = \frac{1}{8} \approx 0,12500.$$

Teorema 8.5.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números e $p(x) = x^4 + ax + b$ o polinômio minimal de θ, com a e b não nulos. Se $\mathcal{D}(\mathbb{K})$ é livre de quadrados, então a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{1}{\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem 4 raízes reais,} \\ \dfrac{9}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem somente 2 raízes reais,} \\ \dfrac{1}{\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ não tem raiz real.} \end{cases}$$

Demonstração. Por hipótese, como $\mathcal{D}(\mathbb{K})$ é livre de quadrados, pela Proposição 2.5.5, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3, \text{com } a_0, a_1, a_2, a_3 \in \mathbb{Z}.$$

Para este caso os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta_k$, para $k = 1, 2, 3, 4$. Dividimos esta demonstração em casos de acordo com o corpo $\mathbb{K}$.

1. Se $\mathbb{K}$ é totalmente real de grau $n = 4$, ou seja, θ_1, θ_2, θ_3 e θ_4 são reais, então $r_1 = 4$ e $r_2 = 0$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_2(\alpha)), \sigma_3(\alpha), \sigma_4(\alpha))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + (\sigma_4(\alpha))^2 = \\ &= (a_0 + a_1\theta_1 + a_2\theta_1^2 + a_3\theta_1^3)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2 + a_3\theta_2^3)^2 + \\ &+ (a_0 + a_1\theta_3 + a_2\theta_3^2 + a_3\theta_3^3)^2 + (a_0 + a_1\theta_4 + a_2\theta_4^2 + a_3\theta_4^3)^2 = \\ &= 4a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + a_2^2\theta_2^4 + 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + a_2^2\theta_3^4 + 2a_2a_3\theta_3^5 + \\ &+ a_3^2\theta_3^6 + a_2^2\theta_4^4 + 2a_2a_3\theta_4^5 + a_3^2\theta_4^6 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2) + \\ &+ 2a_0(a_1(\theta_1 + \theta_2 + \theta_3 + \theta_4) + a_2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2) + a_3(\theta_1^3 + \theta_2^3 + \theta_3^3 + \theta_4^3)) + \\ &+ 2a_1(a_2(\theta_1^3 + \theta_2^3 + \theta_3^3 + \theta_4^3) + a_3(\theta_1^4 + \theta_2^4 + \theta_3^4 + \theta_4^4)). \end{aligned}$$

   Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

   Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\,(1)^4}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

2. Se $\mathbb{K}$ é misto de grau $n = 4$, ou seja, θ_1, θ_2 são reais θ_3 e θ_4 são imaginárias (conjugadas respectivamente), então $r_1 = 2$ e $r_2 = 1$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em

$\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_2(\alpha), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + \sigma_3(\alpha)\sigma_4(\alpha) = \\
&= (a_0 + a_1\theta_1 + a_2\theta_1^2 + a_3\theta_1^3)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2 + a_3\theta_2^3)^2 + \\
&+ (a_0 + a_1\theta_3 + a_2\theta_3^2 + a_3\theta_3^3)^2 \times (a_0 + a_1\theta_4 + a_2\theta_4^2 + a_3\theta_4^3)^2 = \\
&= 3a_0^2 + a2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + a_2^2\theta_2^4 + 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + a_2^2\theta_3^2\theta_4^2 + \\
&+ a_2a_3\theta_3^3\theta_4^2 + a_2a_3\theta_3^2\theta_4^3 + a_3^2\theta_3^3\theta_4^3 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3\theta_4) + \\
&+ a_1a_2(2\theta_1^3 + 2\theta_2^3 + \theta_3\theta_4(\theta_3 + \theta_4)) + a_1a_3(2\theta_1^4 + 2\theta_2^4 + \theta_3\theta_4(\theta_3^2 + \theta_4^2)) + \\
&+ a_0(a_1(2\theta_1 + 2\theta_2 + \theta_3 + \theta_4) + a_2(2\theta_1^2 + 2\theta_2^2 + \theta_3^2 + \theta_4^2) + \\
&+ a_3(2\theta_1^3 + 2\theta_2^3 + \theta_3^3 + \theta_4^3)).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{3}}{2}\right)^4}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{9}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

3. Se $\mathbb{K}$ é totalmente imaginário de grau $n = 4$, ou seja, θ_1, θ_2, θ_3 e θ_4 são imaginárias (conjugadas respectivamente), então $r_1 = 0$ e $r_2 = 2$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= \Re^2(\sigma_1(\alpha)) + \Im^2(\sigma_1(\alpha)) + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= \sigma_1(\alpha)\overline{\sigma_1(\alpha)} + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= \sigma_1(\alpha)\sigma_3(\alpha) + \sigma_2(\alpha)\sigma_4(\alpha) = \\
&= (a_0 + a_1\theta_1 + a_2\theta_1^2 + a_3\theta_1^3) \times (a_0 + a_1\theta_3 + a_2\theta_3^2 + a_3\theta_3^3) + \\
&+ (a_0 + a_1\theta_2 + a_2\theta_2^2 + a_3\theta_2^3)^2 \times (a_0 + a_1\theta_4 + a_2\theta_4^2 + a_3\theta_4^3)^2 = \\
&= 2a_0^2 + a_2^2\theta_1^2\theta_3^2 + a_2a_3\theta_1^3\theta_3^2 + a_2a_3\theta_1^2\theta_3^3 + a_3^2\theta_1^3\theta_3^3 + a_2^2\theta_2^2\theta_4^2 + a_2a_3\theta_2^3\theta_4^2 + \\
&+ a_2a_3\theta_2^2\theta_4^3 + a_3^2\theta_2^3\theta_4^3 + a_1^2(\theta_1\theta_3 + \theta_2\theta_4) + a_1a_2(\theta_1^2\theta_3 + \theta_1\theta_3^2 + \theta_2\theta_4(\theta_2 + \theta_4)) + \\
&+ a_1a_3(\theta_1^3\theta_3 + \theta_1\theta_3^3 + \theta_2\theta_4(\theta_2^2 + \theta_4^2)) + a_0(a_1(\theta_1 + \theta_2 + \theta_3 + \theta_4) + \\
&+ a_2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2) + a_3(\theta_1^3 + \theta_2^3 + \theta_3^3 + \theta_4^3)).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 2 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{2} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{2}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{2}}{2}\right)^4}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

Portanto, dos itens (1), (2) e (3), segue o resultado. □

Exemplo 8.5.1. *Seja $\mathbb{K}$ um corpo de números de grau 4. Sob as condições do Teorema 8.5.1, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^4 - x - 1$ é o minimal de θ. Neste caso, $p(x)$ tem somente 2 raízes reais. Como $\mathcal{D}(\mathbb{K}) = -283$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9}{8\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{9}{8\sqrt{283}} \approx 0,00687.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^4 + x + 1$ é o minimal de θ. Neste caso, $p(x)$ não tem raiz real. Como $\mathcal{D}(\mathbb{K}) = 229$ é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{1}{\sqrt{229}} \approx 0,06608.$$

8.5.2 Reticulados na quártica $p(x) = x^4 - d$

Consideramos $p(x) = x^4 - d$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$, com $d \in \mathbb{Z}_+$ livre de quadrados e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta\xi_4^{k-1}$, onde $k = 1, 2, 3, 4$.

Pelo Teorema 5.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3, \text{ se } d \not\equiv 1, 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right), \text{ se } d \equiv 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Pela Proposição 5.3.4, segue que o discriminante do anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -256d^3, \text{ se } d \not\equiv 1, 5 (mod\ 8) \\ -16d^3, \text{ se } d \equiv 5 (mod\ 8) \\ -4d^3, \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Pela Tabela (8.1), segue a densidade de centro ótima para a dimensão 4 é

$$\delta = \frac{1}{8} \approx 0,12500.$$

Teorema 8.5.2. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[4]{d}$ com $d \in \mathbb{Z}_+$ livre de quadrados. A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de $\mathbb{K}$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \frac{9}{128\sqrt{d^3}}, \text{ se } d \not\equiv 1, 5 (mod\ 8), \\ \frac{9}{32\sqrt{d^3}}, \text{ se } d \equiv 5 (mod\ 8), \\ \frac{9}{16\sqrt{d^3}}, \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Demonstração. Suponhamos que d é um inteiro positivo e livre de quadrados. Dessa forma, $\theta = \sqrt[4]{d} \in \mathbb{K}$. Para este caso, os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta\xi_4^{k-1}$, com $1 \leq k \leq 4$ e assim, $\mathbb{K}$ é um corpo misto de grau $n = 4$, onde $r_1 = 2$ e $r_2 = 1$. Vamos dividir esta demonstração em casos de acordo com a base integral obtida no Teorema 5.3.1:

1. Seja $d \not\equiv 1, 5(mod\ 8)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 5.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3, \text{com } a_0, a_1, a_2, a_3 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_3(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_2(\alpha)\sigma_4(\alpha) = \\
&= (a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3)^2 + (a_0 + a_1\theta\xi_4^2 + a_2\theta^2 + a_3\theta^3\xi_4^2)^2 + \\
&+ (a_0 + a_1\theta\xi_4 + a_2\theta^2\xi_4^2 + a_3\theta^3\xi_4^3) \times (a_0 + a_1\theta\xi_4^3 + a_2\theta^2\xi_4^2 + a_3\theta^3\xi_4) = \\
&= 3a_0^2 + 3a_1^2\theta^2 + 2a_0a_2\theta^2 + 3a_2d + 2a_1a_3d + 3a_3^2d\theta^2.
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \not\equiv 1, 5(mod\ 8)$, pela Proposição 5.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 256d^3$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{3}}{2}\right)^4}{\sqrt{256d^3}} = \frac{9}{128\sqrt{d^3}}.$$

2. Seja $d \equiv 5(mod\ 8)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 4.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\left(\frac{\theta^2 - 1}{2}\right) + a_3\left(\frac{1 + \theta + \theta^2 + \theta^3}{2}\right), \text{com } a_0, a_1, a_2, a_3 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski

(usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_3(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_2(\alpha)\sigma_4(\alpha) = \\
&= \left(a_0 + a_1\theta + a_2\left(\frac{\theta^2-1}{2}\right) + a_3\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right)\right)^2 + \\
&+ \left(a_0 + a_1\theta\xi_4^2 + a_2\left(\frac{\theta^2-1}{2}\right) + a_3\left(\frac{1+\theta\xi_4^2+\theta^2+\theta^3\xi_4^2}{2}\right)\right)^2 + \\
&+ \left(a_0 + a_1\theta\xi_4 + a_2\left(\frac{\theta^2\xi_4^2-1}{2}\right) + a_3\left(\frac{1+\theta\xi_4+\theta^2\xi_4^2+\theta^3\xi_4^3}{2}\right)\right) \times \\
&\times \left(a_0 + a_1\theta\xi_4^3 + a_2\left(\frac{\theta^2\xi_4^2-1}{2}\right) + a_3\left(\frac{1+\theta\xi_4^3+\theta^2\xi_4^2+\theta^3\xi_4}{2}\right)\right) \\
&= \frac{1}{4}(12a_0^2 - 12a_0a_2 + 3a_2^2 + 12a_0a_3 - 6a_2a_3 + 3a_3^2 + 12a_1^2\theta^2 + 4a_0a_2\theta^2 - \\
&- 2a_2\theta^2 + 4a_0a_3\theta^2 + 12a_1a_3\theta^2 + 5a_3^2\theta^2 + 3a_2\theta^2 d + 4a_1a_3d + 6a_2a_3d + \\
&+ 5a_3^2d + 3a_3^2d\theta^2).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \equiv 5(mod\ 8)$, pela Proposição 5.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 16d^3$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{3}}{2}\right)^4}{\sqrt{16d^3}} = \frac{9}{32\sqrt{d^3}}.$$

3. Seja $d \equiv 1(mod\ 8)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 4.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\left(\frac{\theta^2-1}{2}\right) + a_3\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{com } a_0, a_1, a_2, a_3 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski

(usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_3(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_2(\alpha)\sigma_4(\alpha) = \\
&= \left(a_0 + a_1\theta + a_2\left(\frac{\theta^2-1}{2}\right) + a_3\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right)\right)^2 + \\
&+ \left(a_0 + a_1\theta\xi_4^2 + a_2\left(\frac{\theta^2-1}{2}\right) + a_3\left(\frac{1+\theta\xi_4^2+\theta^2+\theta^3\xi_4^2}{4}\right)\right)^2 + \\
&+ \left(a_0 + a_1\theta\xi_4 + a_2\left(\frac{\theta^2\xi_4^2-1}{2}\right) + a_3\left(\frac{1+\theta\xi_4+\theta^2\xi_4^2+\theta^3\xi_4^3}{4}\right)\right) \times \\
&\times \left(a_0 + a_1\theta\xi_4^3 + a_2\left(\frac{\theta^2\xi_4^2-1}{2}\right) + a_3\left(\frac{1+\theta\xi_4^3+\theta^2\xi_4^2+\theta^3\xi_4}{4}\right)\right) \\
&= \frac{1}{16}(48a_0^2 - 48a_0a_2 + 12a_2^2 + 24a_0a_3 - 12a_2a_3 + 3a_3^2 + 48a_1^2\theta^2 + \\
&+ 16a_0a_2\theta^2 - 8a_2^2\theta^2 + 8a_0a_3\theta^2 + 24a_1a_3\theta^2 + 5a_3^2\theta^2 + 12a_2^2d + 8a_1a_3d + \\
&+ 12a_2a_3d + 5a_3^2d + 3a_3^2d\theta^2).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \equiv 1(mod\ 8)$, pela Proposição 5.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 4d^3$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{3}}{2}\right)^4}{\sqrt{4d^3}} = \frac{9}{16\sqrt{d^3}}.$$

Portanto, dos itens (1) e (2), segue o resultado. □

Exemplo 8.5.2. *Seja $\mathbb{K}$ um corpo de números de grau 4. Sob as condições do Teorema 8.5.2, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2})$. Como $d = 2$ e $2 \not\equiv 1, 5(mod\ 8)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9}{128\sqrt{2^3}} \approx 0,02485.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[4]{5})$. Como $d = 5$ e $5 \equiv 5(mod\ 8)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9}{32\sqrt{5^3}} \approx 0,02515.$$

8.6 Aplicações nas extensões quínticas

Nesta seção, as referências citadas farão menção ao Capítulo 6 de Extensões Quínticas. O objetivo é encontrar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ reticulados algébricos via $\mathbb{K} = \mathbb{Q}(\theta)$ corpo de números de grau 5, onde o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ é $p(x) = x^5 + ax + b$, com a e b não nulos, ou $p(x) = x^5 - d$, com d livre de quadrados.

8.6.1 Reticulados na quinta $p(x) = x^5 + ax + b$

Consideramos $p(x) = x^5 + ax + b$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$, e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta_k$, e θ_k é uma raiz de $p(x)$, para $k = 1, 2, 3, 4, 5$. Por convenção, seja $\theta_1 = \theta$.

Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 | a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}\}.$$

Pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4) = 256a^5 + 3125b^4.$$

Pela Tabela (8.1), segue que a densidade de centro ótima para a dimensão 5 é dada por

$$\delta = \frac{1}{8\sqrt{2}} \approx 0,08839.$$

Teorema 8.6.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números e $p(x) = x^5 + ax + b$ o polinômio minimal de θ, com a e b não nulos. Se $\mathcal{D}(\mathbb{K})$ é livre de quadrados, então a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{25\sqrt{5}}{32\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem 5 raízes reais,} \\ \dfrac{2}{\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem somente 3 raízes reais,} \\ \dfrac{9\sqrt{3}}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem somente 1 raiz real.} \end{cases}$$

Demonstração. Por hipótese, como $\mathcal{D}(\mathbb{K})$ é livre de quadrados, pela Proposição 2.5.5, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4, \text{com } a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}.$$

Para este caso os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta_k$, para $k = 1, 2, 3, 4, 5$. Dividimos esta demonstração em dois casos de acordo com o corpo $\mathbb{K}$.

1. Se $\mathbb{K}$ é totalmente real de grau $n = 5$, ou seja, θ_1, θ_2, θ_3, θ_4 e θ_5 são reais, então $r_1 = 5$ e $r_2 = 0$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha), \sigma_4(\alpha), \sigma_5(\alpha))||^2 =$$
$$= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + (\sigma_4(\alpha))^2 + (\sigma_5(\alpha))^2 =$$

$= (a_0 + a_1\theta_1 + a_2\theta_1^2 + a_3\theta_1^3 + a_4\theta_1^4)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2 + a_3\theta_2^3 + a_4\theta_2^4)^2 +$
$+ (a_0 + a_1\theta_3 + a_2\theta_3^2 + a_3\theta_3^3 + a_4\theta_3^4)^2 + (a_0 + a_1\theta_4 + a_2\theta_4^2 + a_3\theta_4^3 + a_4\theta_4^4)^2 +$
$+ (a_0 + a_1\theta_5 + a_2\theta_5^2 + a_3\theta_5^3 + a_4\theta_5^4)^2 =$
$= 5a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + 2a_2a_4\theta_1^6 + 2a_3a_4\theta_1^7 + a_4^2\theta_1^8 + a_2^2\theta_2^4 +$
$+ 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + 2a_2a_4\theta_2^6 + 2a_3a_4\theta_2^7 + a_4^2\theta_2^8 + a_2^2\theta_3^4 + 2a_2a_3\theta_3^5 + a_3^2\theta_3^6 +$
$+ 2a_2a_4\theta_3^6 + 2a_3a_4\theta_3^7 + a_4^2\theta_3^8 + a_2^2\theta_4^4 + 2a_2a_3\theta_4^5 + a_3^2\theta_4^6 + 2a_2a_4\theta_4^6 + 2a_3a_4\theta_4^7 +$
$+ a_4^2\theta_4^8 + a_2^2\theta_5^4 + 2a_2a_3\theta_5^5 + a_3^2\theta_5^6 + 2a_2a_4\theta_5^6 + 2a_3a_4\theta_5^7 + a_4^2\theta_5^8 + a_1^2(\theta_1^2 + \theta_2^2 +$
$+ \theta_3^2 + \theta_4^2 + \theta_5^2) + 2a_0(a_3\theta_1^3 + a_4\theta_1^4 + a_3\theta_2^3 + a_4\theta_2^4 + a_3\theta_3^3 + a_4\theta_3^4 + a_3\theta_4^3 +$
$+ a_4\theta_4^4 + a_3\theta_5^3 + a_4\theta_5^4 + a_1(\theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5) + a_2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 +$
$+ \theta_5^2)) + 2a_1(a_2(\theta_1^3 + \theta_2^3 + \theta_3^3 + \theta_4^3 + \theta_5^3) + a_3(\theta_1^4 + \theta_2^4 + \theta_3^4 + \theta_4^4 + \theta_5^4) +$
$+ a_4(\theta_1^5 + \theta_2^5 + \theta_3^5 + \theta_4^5 + \theta_5^5)).$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 5 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{5} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{5}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\left(\frac{\sqrt{5}}{2}\right)^5}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{25\sqrt{5}}{32\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

2. Se $\mathbb{K}$ é misto de grau $n = 5$, de modo que θ_1, θ_2, θ_3 são reais e θ_4 e θ_5 são imaginárias (conjugadas respectivamente), então $r_1 = 2$ e $r_2 = 1$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha), \Re(\sigma_4(\alpha)), \Im(\sigma_4(\alpha)))||^2 =$
$= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + \Re^2(\sigma_4(\alpha)) + \Im^2(\sigma_4(\alpha)) =$
$= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_4(\alpha)\overline{\sigma_4(\alpha)} =$
$= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + \sigma_4(\alpha)\sigma_5(\alpha) =$
$= (a_0 + a_1\theta_1 + a_2\theta_1^2 + a_3\theta_1^3 + a_4\theta_1^4)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2 + a_3\theta_2^3 + a_4\theta_2^4)^2 +$
$+ (a_0 + a_1\theta_3 + a_2\theta_3^2 + a_3\theta_3^3 + a_4\theta_3^4)^2 + (a_0 + a_1\theta_4 + a_2\theta_4^2 + a_3\theta_4^3 + a_4\theta_4^4) \times$
$\times (a_0 + a_1\theta_5 + a_2\theta_5^2 + a_3\theta_5^3 + a_4\theta_5^4) =$
$= 4a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + 2a_2a_4\theta_1^6 + 2a_3a_4\theta_1^7 + a_4^2\theta_1^8 + a_2^2\theta_2^4 +$
$+ 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + 2a_2a_4\theta_2^6 + 2a_3a_4\theta_2^7 + a_4^2\theta_2^8 + a_2^2\theta_3^4 + 2a_2a_3\theta_3^5 + a_3^2\theta_3^6 +$
$+ 2a_2a_4\theta_3^6 + 2a_3a_4\theta_3^7 + a_4^2\theta_3^8 + a_2^2\theta_4^2\theta_5^2 + a_2a_3\theta_4^3\theta_5^2 + a_2a_4\theta_4^4\theta_5^2 + a_2a_3\theta_4^2\theta_5^3 +$
$+ a_3^2\theta_4^3\theta_5^3 + a_3a_4\theta_4^4\theta_5^3 + a_2a_4\theta_4^2\theta_5^4 + a_3a_4\theta_4^3\theta_5^4 + a_4^2\theta_4^4\theta_5^4 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3^2 +$
$+ \theta_4\theta_5) + a_0(2a_3\theta_1^3 + 2a_4\theta_1^4 + 2a_3\theta_2^3 + 2a_4\theta_2^4 + 2a_3\theta_3^3 + 2a_4\theta_3^4 + a_3\theta_4^3 +$
$+ a_4\theta_4^4 + a_3\theta_5^3 + a_4\theta_5^4 + a_1(2\theta_1 + 2\theta_2 + 2\theta_3 + \theta_4 + \theta_5) + a_2(2\theta_1^2 + 2\theta_2^2 +$
$+ 2\theta_3^2 + \theta_4^2 + \theta_5^2)) + a_1(a_2(2\theta_1^3 + 2\theta_2^3 + 2\theta_3^3 + \theta_4^2\theta_5 + \theta_4\theta_5^2) + a_3(2\theta_1^4 + 2\theta_2^4 +$
$+ 2\theta_3^4 + \theta_4^3\theta_5 + \theta_4\theta_5^3) + a_4(2\theta_1^5 + 2\theta_2^5 + 2\theta_3^5 + \theta_4^4\theta_5 + \theta_4\theta_5^4)).$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\,(1)^5}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2}{\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

3. Se $\mathbb{K}$ é misto de grau $n = 5$, de modo que θ_1 é real e θ_2, θ_3, θ_4 e θ_5 são imaginárias (conjugadas respectivamente), então $r_1 = 1$ e $r_2 = 2$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
&||\sigma_{\mathbb{K}}(\alpha)||^2 = ||((\sigma_1(\alpha)), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_4(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\
&= (a_0 + a_1\theta_1 + a_2\theta_1^2 + a_3\theta_1^3 + a_4\theta_1^4)^2 + (a_0 + a_1\theta_2 + a_2\theta_2^2 + a_3\theta_2^3 + a_4\theta_2^4) \times \\
&\times (a_0 + a_1\theta_4 + a_2\theta_4^2 + a_3\theta_4^3 + a_4\theta_4^4) + (a_0 + a_1\theta_3 + a_2\theta_3^2 + a_3\theta_3^3 + a_4\theta_3^4) \times \\
&\times (a_0 + a_1\theta_5 + a_2\theta_5^2 + a_3\theta_5^3 + a_4\theta_5^4) = \\
&= 3a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + 2a_2a_4\theta_1^6 + 2a_3a_4\theta_1^7 + a_4^2\theta_1^8 + a_2^2\theta_2^2\theta_4^2 + \\
&+ a_2a_3\theta_2^3\theta_4^2 + a_2a_4\theta_2^4\theta_4^2 + a_2a_3\theta_2^2\theta_4^3 + a_3^2\theta_2^3\theta_4^3 + a_3a_4\theta_2^4\theta_4^3 + a_2a_4\theta_2^2\theta_4^4 + \\
&+ a_3a_4\theta_2^3\theta_4^4 + a_4^2\theta_2^4\theta_4^4 + a_2^2\theta_3^2\theta_5^2 + a_2a_3\theta_3^3\theta_5^2 + a_2a_4\theta_3^4\theta_5^2 + a_2a_3\theta_3^2\theta_5^3 + a_3^2\theta_3^3\theta_5^3 + \\
&+ a_3a_4\theta_3^4\theta_5^3 + a_2a_4\theta_3^2\theta_5^4 + a_3a_4\theta_3^3\theta_5^4 + a_4^2\theta_3^4\theta_5^4 + a_1^2(\theta_1^2 + \theta_2\theta_4 + \theta_3\theta_5) + \\
&+ a_0(2a_3\theta_1^3 + 2a_4\theta_1^4 + a_3\theta_2^3 + a_4\theta_2^4 + a_3\theta_3^3 + a_4\theta_3^4 + a_3\theta_4^3 + a_4\theta_4^4 + a_3\theta_5^3 + \\
&+ a_4\theta_5^4 + a_1(2\theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5) + a_2(2\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 + \theta_5^2)) + \\
&+ a_1(a_2(2\theta_1^3 + \theta_2^2\theta_4 + \theta_2\theta_4^2 + \theta_3\theta_5(\theta_3 + \theta_5)) + a_3(2\theta_1^4 + \theta_2^3\theta_4 + \theta_2\theta_4^3 + \\
&+ \theta_3\theta_5(\theta_3^2 + \theta_5^2)) + a_4(2\theta_1^5 + \theta_2^4\theta_4 + \theta_2\theta_4^4 + \theta_3\theta_5(\theta_3^3 + \theta_5^3))).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{3}}{2}\right)^5}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{9\sqrt{3}}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

Portanto, dos itens (1), (2) e (3), segue o resultado. □

Exemplo 8.6.1. *Seja $\mathbb{K}$ um corpo de números de grau 5. Sob as condições do Teorema 8.6.1, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^5 - x - 1$ é o minimal de θ. Neste caso, $p(x)$ tem somente 1 raiz real. Como $\mathcal{D}(\mathbb{K}) = 2869 = 19 \times 151$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9\sqrt{3}}{8\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{9\sqrt{3}}{8\sqrt{2869}} \approx 0,03637.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\theta)$*, cujo o polinômio* $p(x) = x^5 + 2x + 1$ *é o minimal de* θ*. Neste caso,* $p(x)$ *tem somente* 1 *raiz real. Como* $\mathcal{D}(\mathbb{K}) = 11317 = 83 \times 137$ *e é livre de quadrados, segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9\sqrt{3}}{8\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{9\sqrt{3}}{8\sqrt{11317}} \approx 0,01831.$$

8.6.2 Reticulados na quinta $p(x) = x^5 - d$

Consideramos $p(x) = x^5 - d$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta\xi_5^{k-1}$, onde $k = 1, 2, 3, 4, 5$.

Pelo Teorema 6.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+4\theta+\theta^2+4\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -1 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+3\theta+4\theta^2+2\theta^3+\theta^4}{5}\right), \text{ se } d \equiv 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+2\theta+4\theta^2+3\theta^3+\theta^4}{5}\right), \text{ se } d \equiv -7 (mod\ 25). \end{cases}$$

Pela Proposição 6.3.4, segue que o discriminante do anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 3125d^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ 125d^4, \text{ se } d \equiv \pm 1, \pm 7 (mod\ 25). \end{cases}$$

Pela Tabela (8.1), segue a densidade de centro ótima para a dimensão 5 é

$$\delta = \frac{1}{8\sqrt{2}} \approx 0,08839.$$

Teorema 8.6.2. *Seja* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números, onde* $\theta = \sqrt[5]{d}$ *com* $d \in \mathbb{Z}$ *livre de quadrados. A densidade de centro do reticulado algébrico* $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ *de* $\mathbb{K}$ *é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{9\sqrt{3}}{200d^2\sqrt{5}}, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25), \\ \dfrac{9\sqrt{3}}{40d^2\sqrt{5}}, \text{ se } d \equiv \pm 1, \pm 7 (mod\ 25). \end{cases}$$

Demonstração. Suponhamos que d é um inteiro positivo e livre de quadrados. Dessa forma, $\theta = \sqrt[5]{d} \in \mathbb{K}$. Para este caso, os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta\xi_5^{k-1}$, com $1 \leq k \leq 5$ e assim, $\mathbb{K}$ é um corpo misto de grau $n = 5$, onde $r_1 = 1$ e $r_2 = 2$. Vamos dividir esta demonstração em casos de acordo com a base integral obtida no Teorema 6.3.1:

1. Seja $d \not\equiv \pm 1, \pm 7 (mod\ 25)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 6.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4, \text{com } a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\ &= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\ &= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\ &= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_5(\alpha) + \sigma_3(\alpha)\sigma_4(\alpha) = \\ &= 3a_0^2 + a_0a_1\theta + 3a_1^2\theta^2 + a_0a_2\theta^2 + a_1a_2\theta^3 + a_0a_3\theta^3 + 3a_2^2\theta^4 + a_1a_3\theta^4 + \\ &+ a_0a_4\theta^4 + a_2a_3d + a_1a_4d + 3a_3^2d\theta + a_2a_4d\theta + a_3a_4d\theta^2 + 3a_4^2d\theta^3.\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \not\equiv \pm 1, \pm 7 (mod\ 25)$, pela Proposição 6.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 3125d^4$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{3}}{2}\right)^5}{\sqrt{3125d^4}} = \frac{9\sqrt{3}}{200d^2\sqrt{5}}.$$

2. Seja $d \equiv 1 (mod\ 25)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 6.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\left(\frac{1 + \theta + \theta^2 + \theta^3 + \theta^4}{5}\right), \text{com } a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\ &= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\ &= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\ &= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_5(\alpha) + \sigma_3(\alpha)\sigma_4(\alpha) = \\ &= \frac{1}{25}(75a_0^2 + 30a_0a_4 + 3a_4^2 + 25a_0a_1\theta + 5a_0a_4\theta + 5a_1a_4\theta + a_4^2\theta + 75a_1^2\theta^2 + \\ &+ 25a_0a_2\theta^2 + 5a_0a_4\theta^2 + 30a_1a_4\theta^2 + 5a_2a_4\theta^2 + 4a_4^2\theta^2 + 25a_1a_2\theta^3 + 25a_0a_3\theta^3 + \\ &+ 5a_0a_4\theta^3 + 5a_1a_4\theta^3 + 5a_2a_4\theta^3 + 5a_3a_4\theta^3 + 2a_4^2\theta^3 + 75a_2^2\theta^4 + 25a_1a_3\theta^4 + \\ &+ 5a_0a_4\theta^4 + 5a_1a_4\theta^4 + 30a_2a_4\theta^4 + 5a_3a_4\theta^4 + 5a_4^2\theta^4 + 25a_2a_3d + 5a_1a_4d + \\ &+ 5a_2a_4d + 5a_3a_4d + 2a_4^2d + 75a_3^2d\theta + 5a_2a_4d\theta + 30a_3a_4d\theta + 4a_4^2d\theta + \\ &+ 5a_3a_4d\theta^2 + a_4^2d\theta^2 + 3a_4^2d\theta^3).\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \equiv 1(mod\ 25)$, pela Proposição 6.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 125d^4$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{3}}{2}\right)^5}{\sqrt{125d^4}} = \frac{9\sqrt{3}}{40d^2\sqrt{5}}.$$

3. Seja $d \equiv -1(mod\ 25)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 6.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\left(\frac{1 + 4\theta + \theta^2 + 4\theta^3 + \theta^4}{5}\right), \text{com } a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_5(\alpha) + \sigma_3(\alpha)\sigma_4(\alpha) = \\
&= \frac{1}{25}(75a_0^2 + 30a_0a_4 + 3a_4^2 + 25a_0a_1\theta + 20a_0a_4\theta + 5a_1a_4\theta + 4a_4^2\theta + 75a_1^2\theta^2 + \\
&+ 25a_0a_2\theta^2 + 5a_0a_4\theta^2 + 120a_1a_4\theta^2 + 5a_2a_4\theta^2 + 49a_4^2\theta^2 + 25a_1a_2\theta^3 + 25a_0a_3\theta^3 + \\
&+ 20a_0a_4\theta^3 + 5a_1a_4\theta^3 + 20a_2a_4\theta^3 + 5a_3a_4\theta^3 + 8a_4^2\theta^3 + 75a_2^2\theta^4 + 25a_1a_3\theta^4 + \\
&+ 5a_0a_4\theta^4 + 20a_1a_4\theta^4 + 30a_2a_4\theta^4 + 20a_3a_4\theta^4 + 20a_4^2\theta^4 + 25a_2a_3d + 5a_1a_4d + \\
&+ 20a_2a_4d + 5a_3a_4d + 8a_4^2d + 75a_3^2d\theta + 5a_2a_4d\theta + 120a_3a_4d\theta + 49a_4^2d\theta + \\
&+ 5a_3a_4d\theta^2 + 4a_4^2d\theta^2 + 3a_4^2d\theta^3).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \equiv -1(mod\ 25)$, pela Proposição 6.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 125d^4$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{3}}{2}\right)^5}{\sqrt{125d^4}} = \frac{9\sqrt{3}}{40d^2\sqrt{5}}.$$

4. Seja $d \equiv 7(mod\ 25)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 6.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\left(\frac{1 + 3\theta + 4\theta^2 + 2\theta^3 + \theta^4}{5}\right), \text{com } a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski

(usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_5(\alpha) + \sigma_3(\alpha)\sigma_4(\alpha) = \\
&= \frac{1}{25}(75a_0^2 + 30a_0a_4 + 3a_4^2 + 25a_0a_1\theta + 15a_0a_4\theta + 5a_1a_4\theta + 3a_4^2\theta + 75a_1^2\theta^2 + \\
&+ 25a_0a_2\theta^2 + 20a_0a_4\theta^2 + 90a_1a_4\theta^2 + 5a_2a_4\theta^2 + 31a_4^2\theta^2 + 25a_1a_2\theta^3 + 25a_0a_3\theta^3 + \\
&+ 10a_0a_4\theta^3 + 20a_1a_4\theta^3 + 15a_2a_4\theta^3 + 5a_3a_4\theta^3 + 14a_4^2\theta^3 + 75a_2^2\theta^4 + 25a_1a_3\theta^4 + \\
&+ 5a_0a_4\theta^4 + 10a_1a_4\theta^4 + 120a_2a_4\theta^4 + 15a_3a_4\theta^4 + 55a_4^2\theta^4 + 25a_2a_3d + 5a_1a_4d + \\
&+ 10a_2a_4d + 20a_3a_4d + 11a_4^2d + 75a_3^2\theta^6 + 5a_2a_4d\theta + 60a_3a_4d\theta + 16a_4^2d\theta + \\
&+ 5a_3a_4d\theta^2 + 2a_4^2d\theta^2 + 3a_4^2d\theta^3).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \equiv 7(mod\ 25)$, pela Proposição 6.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 125d^4$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{3}}{2}\right)^5}{\sqrt{125d^4}} = \frac{9\sqrt{3}}{40d^2\sqrt{5}}.$$

5. Seja $d \equiv -7(mod\ 25)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 6.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\left(\frac{1 + 2\theta + 4\theta^2 + 3\theta^3 + \theta^4}{5}\right), \text{com } a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}.$$

Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + \sigma_2(\alpha)\sigma_5(\alpha) + \sigma_3(\alpha)\sigma_4(\alpha) = \\
&= \frac{1}{25}(75a_0^2 + 30a_0a_4 + 3a_4^2 + 25a_0a_1\theta + 10a_0a_4\theta + 5a_1a_4\theta + 2a_4^2\theta + 75a_1^2\theta^2 + \\
&+ 25a_0a_2\theta^2 + 20a_0a_4\theta^2 + 60a_1a_4\theta^2 + 5a_2a_4\theta^2 + 16a_4^2\theta^2 + 25a_1a_2\theta^3 + 25a_0a_3\theta^3 + \\
&+ 15a_0a_4\theta^3 + 20a_1a_4\theta^3 + 10a_2a_4\theta^3 + 5a_3a_4\theta^3 + 11a_4^2\theta^3 + 75a_2^2\theta^4 + 25a_1a_3\theta^4 + \\
&+ 5a_0a_4\theta^4 + 15a_1a_4\theta^4 + 120a_2a_4\theta^4 + 10a_3a_4\theta^4 + 55a_4^2\theta^4 + 25a_2a_3d + 5a_1a_4d + \\
&+ 15a_2a_4d + 20a_3a_4d + 14a_4^2d + 75a_3^2d\theta + 5a_2a_4d\theta + 90a_3a_4d\theta + 31a_4^2d\theta + \\
&+ 5a_3a_4d\theta^2 + 3a_4^2d\theta^2 + 3a_4^2d\theta^3).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Como $d \equiv -7(mod\ 25)$, pela Proposição 6.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 125d^4$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\left(\frac{\sqrt{3}}{2}\right)^5}{\sqrt{125d^4}} = \frac{9\sqrt{3}}{40d^2\sqrt{5}}.$$

Portanto, dos itens (1), (2), (3), (4) e (5), segue o resultado. □

Exemplo 8.6.2. *Seja $\mathbb{K}$ um corpo de números de grau 5. Sob as condições do Teorema 8.6.2, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[5]{-2})$. Como $d = -2$ e $-2 \not\equiv \pm 1, \pm 7(mod\ 25)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9\sqrt{3}}{200d^2\sqrt{5}} = \frac{9\sqrt{3}}{200(-2)^2\sqrt{5}} \approx 0,00871.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[5]{7})$. Como $d = 7$ e $7 \equiv 7(mod\ 25)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9\sqrt{3}}{40d^2\sqrt{5}} = \frac{9\sqrt{3}}{40(7)^2\sqrt{5}} \approx 0,00355.$$

8.7 Aplicações nas extensões sextas

Nesta seção, as referências citadas farão menção ao Capítulo 7 de Extensões Sêxticas. O objetivo é encontrar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ reticulados algébricos via $\mathbb{K} = \mathbb{Q}(\theta)$ corpo de números de grau 6, onde o polinômio minimal do elemento primitivo θ de $\mathbb{K}$ é $p(x) = x^6 + ax + b$, com a e b não nulos, ou $p(x) = x^6 - d$, com $d \in \mathbb{Z}_+$ livre de quadrados.

8.7.1 Reticulados na sexta $p(x) = x^6 + ax + b$

Consideramos $p(x) = x^6 + ax + b$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$, e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta_k$, e θ_k é uma raiz de $p(x)$, para $k = 1, 2, 3, 4, 5, 6$. Por convenção, seja $\theta_1 = \theta$.

Pela Proposição 2.5.5, se o discriminante $\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5)$ é livre de quadrados, então o anel dos inteiros algébricos é dado por

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5 | a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}\}.$$

Pela Proposição 2.5.6, segue que

$$\mathcal{D}(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5) = 3125a^6 - 46656b^5.$$

Pela Tabela (8.1), segue que a densidade de centro ótima para a dimensão 6 é dada por

$$\delta = \frac{1}{8\sqrt{3}} \approx 0,07217.$$

Teorema 8.7.1. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números e $p(x) = x^6 + ax + b$ o polinômio minimal de θ, com a e b não nulos. Se $\mathcal{D}(\mathbb{K})$ é livre de quadrados, então a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{27}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem 6 raízes reais,} \\ \dfrac{125}{32\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem somente 4 raízes reais,} \\ \dfrac{4}{\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ tem somente 2 raízes reais,} \\ \dfrac{27}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}, & \text{se } p(x) \text{ não tem raiz real.} \end{cases}$$

Demonstração. Por hipótese, como $\mathcal{D}(\mathbb{K})$ é livre de quadrados, pela Proposição 2.5.5, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5, \text{com } a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}.$$

Para este caso os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta_k$, para $k = 1, 2, 3, 4, 5, 6$. Dividimos esta demonstração em dois casos de acordo com o corpo $\mathbb{K}$.

1. Se $\mathbb{K}$ é totalmente real de grau $n = 6$, ou seja, θ_1, θ_2, θ_3, θ_4, θ_5 e θ_6 são reais, então $r_1 = 6$ e $r_2 = 0$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} &||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha), \sigma_4(\alpha), \sigma_5(\alpha), \sigma_6(\alpha))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + (\sigma_4(\alpha))^2 + (\sigma_5(\alpha))^2 + (\sigma_6(\alpha))^2 = \\ &= 6a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + 2a_2a_4\theta_1^6 + 2a_3a_4\theta_1^7 + 2a_2a_5\theta_1^7 + a_4^2\theta_1^8 + \\ &+ 2a_3a_5\theta_1^8 + 2a_4a_5\theta_1^9 + a_5^2\theta_1^10 + a_2^2\theta_2^4 + 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + 2a_2a_4\theta_2^6 + 2a_3a_4\theta_2^7 + \\ &+ 2a_2a_5\theta_2^7 + a_4^2\theta_2^8 + 2a_3a_5\theta_2^8 + 2a_4a_5\theta_2^9 + a_5^2\theta_2^10 + a_2^2\theta_3^4 + 2a_2a_3\theta_3^5 + a_3^2\theta_3^6 + \\ &+ 2a_2a_4\theta_3^6 + 2a_3a_4\theta_3^7 + 2a_2a_5\theta_3^7 + a_4^2\theta_3^8 + 2a_3a_5\theta_3^8 + 2a_4a_5\theta_3^9 + a_5^2\theta_3^10 + a_2^2\theta_4^4 + \\ &+ 2a_2a_3\theta_4^5 + a_3^2\theta_4^6 + 2a_2a_4\theta_4^6 + 2a_3a_4\theta_4^7 + 2a_2a_5\theta_4^7 + a_4^2\theta_4^8 + 2a_3a_5\theta_4^8 + 2a_4a_5\theta_4^9 + \\ &+ a_5^2\theta_4^10 + a_2^2\theta_5^4 + 2a_2a_3\theta_5^5 + a_3^2\theta_5^6 + 2a_2a_4\theta_5^6 + 2a_3a_4\theta_5^7 + 2a_2a_5\theta_5^7 + a_4^2\theta_5^8 + \\ &+ 2a_3a_5\theta_5^8 + 2a_4a_5\theta_5^9 + a_5^2\theta_5^10 + a_2^2\theta_6^4 + 2a_2a_3\theta_6^5 + a_3^2\theta_6^6 + 2a_2a_4\theta_6^6 + 2a_3a_4\theta_6^7 + \\ &+ 2a_2a_5\theta_6^7 + a_4^2\theta_6^8 + 2a_3a_5\theta_6^8 + 2a_4a_5\theta_6^9 + a_5^2\theta_6^10 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 + \theta_5^2 + \theta_6^2) + \\ &+ 2a_0(a_3\theta_1^3 + a_4\theta_1^4 + a_5\theta_1^5 + a_3\theta_2^3 + a_4\theta_2^4 + a_5\theta_2^5 + a_3\theta_3^3 + a_4\theta_3^4 + a_5\theta_3^5 + a_3\theta_4^3 + \\ &+ a_4\theta_4^4 + a_5\theta_4^5 + a_3\theta_5^3 + a_4\theta_5^4 + a_5\theta_5^5 + a_3\theta_6^3 + a_4\theta_6^4 + a_5\theta_6^5 + a_1(\theta_1 + \theta_2 + \theta_3 + \\ &+ \theta_4 + \theta_5 + \theta_6) + a_2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 + \theta_5^2 + \theta_6^2)) + 2a_1(a_4\theta_1^5 + a_5\theta_1^6 + a_4\theta_2^5 + \\ &+ a_5\theta_2^6 + a_4\theta_3^5 + a_5\theta_3^6 + a_4\theta_4^5 + a_5\theta_4^6 + a_4\theta_5^5 + a_5\theta_5^6 + a_4\theta_6^5 + a_5\theta_6^6 + a_2(\theta_1^3 + \theta_2^3 + \\ &+ \theta_3^3 + \theta_4^3 + \theta_5^3 + \theta_6^3) + a_3(\theta_1^4 + \theta_2^4 + \theta_3^4 + \theta_4^4 + \theta_5^4 + \theta_6^4)). \end{aligned}$$

   Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 6 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{6} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{6}}{2}.$$

   Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^0\left(\frac{\sqrt{6}}{2}\right)^6}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{27}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

2. Se $\mathbb{K}$ é misto de grau $n = 6$, de modo que θ_1, θ_2, θ_3, θ_4 são reais e θ_5 e θ_6 são imaginárias (conjugadas respectivamente), então $r_1 = 4$ e $r_2 = 1$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$
\begin{aligned}
&||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha), \sigma_4(\alpha), \Re(\sigma_5(\alpha)), \Im(\sigma_5(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_5(\alpha)) + \Im^2(\sigma_5(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_5(\alpha)\overline{\sigma_5(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + (\sigma_3(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_5(\alpha)\sigma_6(\alpha) = \\
&= 5a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + 2a_2a_4\theta_1^6 + 2a_3a_4\theta_1^7 + 2a_2a_5\theta_1^7 + a_4^2\theta_1^8 + \\
&+ 2a_3a_5\theta_1^8 + 2a_4a_5\theta_1^9 + a_5^2\theta_1^10 + a_2^2\theta_2^4 + 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + 2a_2a_4\theta_2^6 + 2a_3a_4\theta_2^7 + \\
&+ 2a_2a_5\theta_2^7 + a_4^2\theta_2^8 + 2a_3a_5\theta_2^8 + 2a_4a_5\theta_2^9 + a_5^2\theta_2^10 + a_2^2\theta_3^4 + 2a_2a_3\theta_3^5 + a_3^2\theta_3^6 + \\
&+ 2a_2a_4\theta_3^6 + 2a_3a_4\theta_3^7 + 2a_2a_5\theta_3^7 + a_4^2\theta_3^8 + 2a_3a_5\theta_3^8 + 2a_4a_5\theta_3^9 + a_5^2\theta_3^10 + a_2^2\theta_4^4 + \\
&+ 2a_2a_3\theta_4^5 + a_3^2\theta_4^6 + 2a_2a_4\theta_4^6 + 2a_3a_4\theta_4^7 + 2a_2a_5\theta_4^7 + a_4^2\theta_4^8 + 2a_3a_5\theta_4^8 + 2a_4a_5\theta_4^9 + \\
&+ a_5^2\theta_4^10 + a_2^2\theta_5^2\theta_6^2 + a_2a_3\theta_5^3\theta_6^2 + a_2a_4\theta_5^4\theta_6^2 + a_2a_5\theta_5^5\theta_6^2 + a_2a_3\theta_5^2\theta_6^3 + a_3^2\theta_5^3\theta_6^3 + \\
&+ a_3a_4\theta_5^4\theta_6^3 + a_3a_5\theta_5^5\theta_6^3 + a_2a_4\theta_5^2\theta_6^4 + a_3a_4\theta_5^3\theta_6^4 + a_4^2\theta_5^4\theta_6^4 + a_4a_5\theta_5^5\theta_6^4 + a_2a_5\theta_5^2\theta_6^5 + \\
&+ a_3a_5\theta_5^3\theta_6^5 + a_4a_5\theta_5^4\theta_6^5 + a_5^2\theta_5^5\theta_6^5 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 + \theta_5\theta_6) + a_0(2a_3\theta_1^3 + \\
&+ 2a_4\theta_1^4 + 2a_5\theta_1^5 + 2a_3\theta_2^3 + 2a_4\theta_2^4 + 2a_5\theta_2^5 + 2a_3\theta_3^3 + 2a_4\theta_3^4 + 2a_5\theta_3^5 + 2a_3\theta_4^3 + \\
&+ 2a_4\theta_4^4 + 2a_5\theta_4^5 + a_3\theta_5^3 + a_4\theta_5^4 + a_5\theta_5^5 + a_3\theta_6^3 + a_4\theta_6^4 + a_5\theta_6^5 + a_1(2\theta_1 + 2\theta_2 + \\
&+ 2\theta_3 + 2\theta_4 + \theta_5 + \theta_6) + a_2(2\theta_1^2 + 2\theta_2^2 + 2\theta_3^2 + 2\theta_4^2 + \theta_5^2 + \theta_6^2)) + a_1(2a_4\theta_1^5 + \\
&+ 2a_5\theta_1^6 + 2a_4\theta_2^5 + 2a_5\theta_2^6 + 2a_4\theta_3^5 + 2a_5\theta_3^6 + 2a_4\theta_4^5 + 2a_5\theta_4^6 + a_4\theta_5^4\theta_6 + a_5\theta_5^5\theta_6 + \\
&+ a_4\theta_5\theta_6^4 + a_5\theta_5\theta_6^5 + a_2(2\theta_1^3 + 2\theta_2^3 + 2\theta_3^3 + 2\theta_4^3 + \theta_5^2\theta_6 + \theta_5\theta_6^2) + a_3(2\theta_1^4 + 2\theta_2^4 + \\
&+ 2\theta_3^4 + 2\theta_4^4 + \theta_5^3\theta_6 + \theta_5\theta_6^3)).
\end{aligned}
$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 5 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{5} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{5}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^1\left(\frac{\sqrt{5}}{2}\right)^6}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{125}{32\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

3. Se $\mathbb{K}$ é misto de grau $n = 6$, de modo que θ_1 e θ_2 são reais e θ_3, θ_4, θ_5 e θ_6 são imaginárias (conjugadas respectivamente), então $r_1 = 2$ e $r_2 = 2$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$
\begin{aligned}
&||\sigma_{\mathbb{K}}(\alpha)||^2 = ||((\sigma_1(\alpha)), (\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)), \Re(\sigma_4(\alpha)), \Im(\sigma_4(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) + \Re^2(\sigma_4(\alpha)) + \Im^2(\sigma_4(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} + \sigma_4(\alpha)\overline{\sigma_4(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_2(\alpha))^2 + \sigma_3(\alpha)\sigma_5(\alpha) + \sigma_4(\alpha)\sigma_6(\alpha) = \\
&= 4a_0^2 + a_2^2\theta_1^4 + 2a_2a_3\theta_1^5 + a_3^2\theta_1^6 + 2a_2a_4\theta_1^6 + 2a_3a_4\theta_1^7 + 2a_2a_5\theta_1^7 + a_4^2\theta_1^8 + \\
&+ 2a_3a_5\theta_1^8 + 2a_4a_5\theta_1^9 + a_5^2\theta_1^10 + a_2^2\theta_2^4 + 2a_2a_3\theta_2^5 + a_3^2\theta_2^6 + 2a_2a_4\theta_2^6 + 2a_3a_4\theta_2^7 + \\
&+ 2a_2a_5\theta_2^7 + a_4^2\theta_2^8 + 2a_3a_5\theta_2^8 + 2a_4a_5\theta_2^9 + a_5^2\theta_2^10 + a_2^2\theta_3^2\theta_5^2 + a_2a_3\theta_3^3\theta_5^2 + a_2a_4\theta_3^4\theta_5^2 +
\end{aligned}
$$

$$+ a_2a_5\theta_3^5\theta_5^2 + a_2a_3\theta_3^2\theta_5^3 + a_3^2\theta_3^3\theta_5^3 + a_3a_4\theta_3^4\theta_5^3 + a_3a_5\theta_3^5\theta_5^3 + a_2a_4\theta_3^2\theta_5^4 + a_3a_4\theta_3^3\theta_5^4 +$$
$$+ a_4^2\theta_3^4\theta_5^4 + a_4a_5\theta_3^5\theta_5^4 + a_2a_5\theta_3^2\theta_5^5 + a_3a_5\theta_3^3\theta_5^5 + a_4a_5\theta_3^4\theta_5^5 + a_5^2\theta_3^5\theta_5^5 + a_2^2\theta_4^2\theta_6^2 +$$
$$+ a_2a_3\theta_4^3\theta_6^2 + a_2a_4\theta_4^4\theta_6^2 + a_2a_5\theta_4^5\theta_6^2 + a_2a_3\theta_4^2\theta_6^3 + a_3^2\theta_4^3\theta_6^3 + a_3a_4\theta_4^4\theta_6^3 + a_3a_5\theta_4^5\theta_6^3 +$$
$$+ a_2a_4\theta_4^2\theta_6^4 + a_3a_4\theta_4^3\theta_6^4 + a_4^2\theta_4^4\theta_6^4 + a_4a_5\theta_4^5\theta_6^4 + a_2a_5\theta_4^2\theta_6^5 + a_3a_5\theta_4^3\theta_6^5 + a_4a_5\theta_4^4\theta_6^5 +$$
$$+ a_5^2\theta_4^5\theta_6^5 + a_1^2(\theta_1^2 + \theta_2^2 + \theta_3\theta_5 + \theta_4\theta_6) + a_0(2a_3\theta_1^3 + 2a_4\theta_1^4 + 2a_5\theta_1^5 + 2a_3\theta_2^3 +$$
$$+ 2a_4\theta_2^4 + 2a_5\theta_2^5 + a_3\theta_3^3 + a_4\theta_3^4 + a_5\theta_3^5 + a_3\theta_4^3 + a_4\theta_4^4 + a_5\theta_4^5 + a_3\theta_5^3 + a_4\theta_5^4 +$$
$$+ a_5\theta_5^5 + a_3\theta_6^3 + a_4\theta_6^4 + a_5\theta_6^5 + a_1(2\theta_1 + 2\theta_2 + \theta_3 + \theta_4 + \theta_5 + \theta_6) + a_2(2\theta_1^2 +$$
$$+ 2\theta_2^2 + \theta_3^2 + \theta_4^2 + \theta_5^2 + \theta_6^2)) + a_1(2a_4\theta_1^5 + 2a_5\theta_1^6 + 2a_4\theta_2^5 + 2a_5\theta_2^6 + a_4\theta_3^4\theta_5 +$$
$$+ a_5\theta_3^5\theta_5 + a_4\theta_3\theta_4^4 + a_5\theta_3\theta_5^5 + a_4\theta_4^4\theta_6 + a_5\theta_4^5\theta_6 + a_4\theta_4\theta_6^4 + a_5\theta_4\theta_6^5 + a_2(2\theta_1^3 +$$
$$+ 2\theta_2^3 + \theta_3^2\theta_5 + \theta_3\theta_5^2 + \theta_4^2\theta_6 + \theta_4\theta_6^2) + a_3(2\theta_1^4 + 2\theta_2^4 + \theta_3^3\theta_5 + \theta_3\theta_5^3 + \theta_4^3\theta_6 + \theta_4\theta_6^3)).$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{4}{\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

4. Se $\mathbb{K}$ é totalmente imaginário de grau $n = 6$, de modo que θ_1, θ_2, θ_3, θ_4, θ_5 e θ_6 são imaginárias (conjugadas respectivamente), então $r_1 = 0$ e $r_2 = 3$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$||\sigma_{\mathbb{K}}(\alpha)||^2 = ||(\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 =$$
$$= \Re^2(\sigma_1(\alpha)) + \Im^2(\sigma_1(\alpha)) + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) =$$
$$= \sigma_1(\alpha)\overline{\sigma_1(\alpha)} + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} =$$
$$= \sigma_1(\alpha)\sigma_4(\alpha) + \sigma_2(\alpha)\sigma_5(\alpha) + \sigma_3(\alpha)\sigma_6(\alpha) =$$
$$= 3a_0^2 + a_2^2\theta_1^2\theta_4^2 + a_2a_3\theta_1^3\theta_4^2 + a_2a_4\theta_1^4\theta_4^2 + a_2a_5\theta_1^5\theta_4^2 + a_2a_3\theta_1^2\theta_4^3 + a_3^2\theta_1^3\theta_4^3 + a_3a_4\theta_1^4\theta_4^3 +$$
$$+ a_3a_5\theta_1^5\theta_4^3 + a_2a_4\theta_1^2\theta_4^4 + a_3a_4\theta_1^3\theta_4^4 + a_4^2\theta_1^4\theta_4^4 + a_4a_5\theta_1^5\theta_4^4 + a_2a_5\theta_1^2\theta_4^5 + a_3a_5\theta_1^3\theta_4^5 +$$
$$+ a_4a_5\theta_1^4\theta_4^5 + a_5^2\theta_1^5\theta_4^5 + a_2^2\theta_2^2\theta_5^2 + a_2a_3\theta_2^3\theta_5^2 + a_2a_4\theta_2^4\theta_5^2 + a_2a_5\theta_2^5\theta_5^2 + a_2a_3\theta_2^2\theta_5^3 +$$
$$+ a_3^2\theta_2^3\theta_5^3 + a_3a_4\theta_2^4\theta_5^3 + a_3a_5\theta_2^5\theta_5^3 + a_2a_4\theta_2^2\theta_5^4 + a_3a_4\theta_2^3\theta_5^4 + a_4^2\theta_2^4\theta_5^4 + a_4a_5\theta_2^5\theta_5^4 +$$
$$+ a_2a_5\theta_2^2\theta_5^5 + a_3a_5\theta_2^3\theta_5^5 + a_4a_5\theta_2^4\theta_5^5 + a_5^2\theta_2^5\theta_5^5 + a_2^2\theta_3^2\theta_6^2 + a_2a_3\theta_3^3\theta_6^2 + a_2a_4\theta_3^4\theta_6^2 +$$
$$+ a_2a_5\theta_3^5\theta_6^2 + a_2a_3\theta_3^2\theta_6^3 + a_3^2\theta_3^3\theta_6^3 + a_3a_4\theta_3^4\theta_6^3 + a_3a_5\theta_3^5\theta_6^3 + a_2a_4\theta_3^2\theta_6^4 + a_3a_4\theta_3^3\theta_6^4 +$$
$$+ a_4^2\theta_3^4\theta_6^4 + a_4a_5\theta_3^5\theta_6^4 + a_2a_5\theta_3^2\theta_6^5 + a_3a_5\theta_3^3\theta_6^5 + a_4a_5\theta_3^4\theta_6^5 + a_5^2\theta_3^5\theta_6^5 + a_1^2(\theta_1\theta_4 +$$
$$+ \theta_2\theta_5 + \theta_3\theta_6) + a_0(a_3\theta_1^3 + a_4\theta_1^4 + a_5\theta_1^5 + a_3\theta_2^3 + a_4\theta_2^4 + a_5\theta_2^5 + a_3\theta_3^3 + a_4\theta_3^4 +$$
$$+ a_5\theta_3^5 + a_3\theta_4^3 + a_4\theta_4^4 + a_5\theta_4^5 + a_3\theta_5^3 + a_4\theta_5^4 + a_5\theta_5^5 + a_3\theta_6^3 + a_4\theta_6^4 + a_5\theta_6^5 +$$
$$+ a_1(\theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5 + \theta_6) + a_2(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 + \theta_5^2 + \theta_6^2)) +$$
$$+ a_1(a_3\theta_1^3\theta_4 + a_4\theta_1^4\theta_4 + a_5\theta_1^5\theta_4 + a_3\theta_1\theta_4^3 + a_4\theta_1\theta_4^4 + a_5\theta_1\theta_4^5 + a_3\theta_2^3\theta_5 + a_4\theta_2^4\theta_5 +$$
$$+ a_5\theta_2^5\theta_5 + a_3\theta_2\theta_5^3 + a_4\theta_2\theta_5^4 + a_5\theta_2\theta_5^5 + a_3\theta_3^3\theta_6 + a_4\theta_3^4\theta_6 + a_5\theta_3^5\theta_6 + a_3\theta_3\theta_6^3 +$$
$$+ a_4\theta_3\theta_6^4 + a_5\theta_3\theta_6^5 + a_2(\theta_1^2\theta_4 + \theta_1\theta_4^2 + \theta_2^2\theta_5 + \theta_2\theta_5^2 + \theta_3\theta_6(\theta_3 + \theta_6))).$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 3 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = \sqrt{3} \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = \frac{\sqrt{3}}{2}.$$

Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^3\left(\frac{\sqrt{3}}{2}\right)^6}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{27}{8\sqrt{|\mathcal{D}(\mathbb{K})|}}.$$

Portanto, dos itens (1), (2), (3) e (4), segue o resultado. □

Exemplo 8.7.1. *Seja $\mathbb{K}$ um corpo de números de grau 6. Sob as condições do Teorema 8.7.1, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^6 - x - 1$ é o minimal de θ. Neste caso, $p(x)$ tem somente 2 raízes reais. Como $\mathcal{D}(\mathbb{K}) = 49781 = 67 \times 743$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{4}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{4}{\sqrt{49781}} \approx 0,01792.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\theta)$, cujo o polinômio $p(x) = x^6 + x + 1$ é o minimal de θ. Neste caso, $p(x)$ não tem raiz real. Como $\mathcal{D}(\mathbb{K}) = 43531 = 101 \times 431$ e é livre de quadrados, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{27}{8\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{27}{8\sqrt{43531}} \approx 0,01617.$$

8.7.2 Reticulados na sexta $p(x) = x^6 - d$

Consideramos $p(x) = x^6 - d$ o polinômio minimal do elemento primitivo θ de $\mathbb{K}$, com $d \in \mathbb{Z}_+$ livre de quadrados e σ_k's os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tais que $\sigma_k(\theta) = \theta\xi_6^{k-1}$, onde $k = 1, 2, 3, 4, 5, 6$.

Pelo Teorema 7.3.1, segue que o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4 + \mathbb{Z}\theta^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\left(\frac{1+\theta^3}{2}\right) + \mathbb{Z}\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right) + \mathbb{Z}\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 1 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+2\theta^2+\theta^4}{3}\right) + \mathbb{Z}\left(\frac{\theta+2\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -10, -1 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\left(\frac{1+\theta^3}{2}\right) + \mathbb{Z}\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right) + \mathbb{Z}\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 17 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta^2+\theta^4}{3}\right) + \mathbb{Z}\left(\frac{\theta+\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -17, 10 (mod\ 36) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\left(\frac{1+\theta^3}{2}\right) + \mathbb{Z}\left(\frac{\theta+\theta^4}{2}\right) + \mathbb{Z}\left(\frac{\theta^2+\theta^5}{2}\right), \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Pela Proposição 7.3.4, segue que o discriminante do anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 46656d^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ 9d^5, \text{ se } d \equiv 1, 17 (mod\ 36) \\ 576d^5, \text{ se } d \equiv -17, -10, -1, 10 (mod\ 36) \\ 729d^5, \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Pela Tabela (8.1), segue a densidade de centro ótima para a dimensão 6 é

$$\delta = \frac{1}{8\sqrt{3}} \approx 0,07217.$$

Teorema 8.7.2. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}_+$ livre de quadrados. A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de $\mathbb{K}$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{1}{54\sqrt{d^5}}, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \dfrac{4}{3\sqrt{d^5}}, \text{ se } d \equiv 1, 17 (mod\ 36), \\ \dfrac{1}{6\sqrt{d^5}}, \text{ se } d \equiv -17, -10, -1, 10 (mod\ 36), \\ \dfrac{4}{27\sqrt{d^5}}, \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Demonstração. Suponhamos que d é um inteiro positivo e livre de quadrados. Dessa forma, $\theta = \sqrt[6]{d} \in \mathbb{K}$. Para este caso, os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta\xi_6^{k-1}$, com $1 \leq k \leq 6$ e assim, $\mathbb{K}$ é um corpo misto de grau $n = 6$, onde $r_1 = 2$ e $r_2 = 2$. Vamos dividir esta demonstração em casos de acordo com a base integral obtida no Teorema 7.3.1:

1. Seja $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 7.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5,$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_4(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\ &= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\ &= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\ &= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\sigma_6(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\ &= 2(2a_0^2 + 2a_1^2\theta^2 + a_0a_2\theta^2 + 2a_2^2\theta^4 + a_1a_3\theta^4 + a_0a_4\theta^4 + 2a_3^2\theta^6 + a_2a_4d + \\ &+ a_1a_5d + 2a_4^2d\theta^2 + a_3a_5d\theta^2 + 2a_5^2d\theta^4). \end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Como $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$, pela Proposição 7.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 46656d^5$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{46656d^5}} = \frac{1}{54\sqrt{d^5}}.$$

2. Seja $d \equiv 1 (mod\ 36)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 7.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\left(\frac{1+\theta^3}{2}\right) + a_4\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right) + a_5\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right),$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_4(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\sigma_6(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\
&= \frac{1}{8}(72a_0^2 + 72a_0a_3 + 18a_3^2 + 96a_0a_4 + 48a_3a_4 + 32a_4^2 + 72a_0a_5 + 36a_3a_5 + \\
&+ 48a_4a_5 + 18a_5^2 + 72a_1^2\theta^2 + 36a_0a_2\theta^2 + 18a_2a_3\theta^2 + 24a_0a_4\theta^2 + 72a_1a_4\theta^2 + \\
&+ 24a_2a_4\theta^2 + 12a_3a_4\theta^2 + 34a_4^2\theta^2 + 18a_0a_5\theta^2 + 96a_1a_5\theta^2 + 18a_2a_5\theta^2 + \\
&+ 9a_3a_5\theta^2 + 72a_4a_5\theta^2 + 41a_5^2\theta^2 + 72a_2^2\theta^4 + 18a_1a_3\theta^4 + 6a_0a_4\theta^4 + 96a_2a_4\theta^4 + \\
&+ 12a_3a_4\theta^4 + 36a_4^2\theta^4 + 6a_1a_5\theta^4 + 72a_2a_5\theta^4 + 12a_3a_5\theta^4 + 54a_4a_5\theta^4 + 22a_5^2\theta^4 + \\
&+ 18a_3^2d + 6a_2a_4d + 4a_4^2d + 6a_1a_5d + 12a_3a_5d + 6a_4a_5d + 6a_5^2d + 2a_4^2d\theta^2 + \\
&+ 3a_3a_5d\theta^2 + a_5^2d\theta^2 + 2a_5^2d\theta^4).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Como $d \equiv 1 (mod\ 36)$, pela Proposição 7.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 9d^5$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{9d^5}} = \frac{4}{3\sqrt{d^5}}.$$

3. Seja $d \equiv -10, -1 (mod\ 36)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 7.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\left(\frac{1 + 2\theta^2 + \theta^4}{3}\right) + a_5\left(\frac{\theta + 2\theta^3 + \theta^5}{3}\right),$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_4(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\sigma_6(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\
&= \frac{2}{9}(18a_0^2 + 12a_0a_4 + 2a_4^2 + 18a_1^2\theta^2 + 9a_0a_2\theta^2 + 6a_0a_4\theta^2 + 3a_2a_4\theta^2 + 2a_4^2\theta^2 + \\
&+ 12a_1a_5\theta^2 + 2a_5^2\theta^2 + 18a_2^2\theta^4 + 9a_1a_3\theta^4 + 3a_0a_4\theta^4 + 24a_2a_4\theta^4 + 9a_4^2\theta^4 + \\
&+ 6a_1a_5\theta^4 + 3a_3a_5\theta^4 + 2a_5^2\theta^4 + 18a_3^2d + 3a_2a_4d + 2a_4^2d + 3a_1a_5d + 24a_3a_5d + \\
&+ 9a_5^2d + 2a_4^2d\theta^2 + 3a_3a_5d\theta^2 + 2a_5^2d\theta^2 + 2a_5^2d\theta^4).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Como $d \equiv -10, -1 (mod\ 36)$, pela Proposição 7.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 576d^5$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{576d^5}} = \frac{1}{6\sqrt{d^5}}.$$

4. Seja $d \equiv 17 (mod\ 36)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 7.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\left(\frac{1+\theta^3}{2}\right) + a_4\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right) + a_5\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right),$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_4(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\sigma_6(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\
&= \frac{1}{8}(72a_0^2 + 72a_0a_3 + 18a_3^2 + 96a_0a_4 + 48a_3a_4 + 32a_4^2 + 72a_1^2\theta^2 + 36a_0a_2\theta^2 + \\
&+ 18a_2a_3\theta^2 + 12a_0a_4\theta^2 + 72a_1a_4\theta^2 + 24a_2a_4\theta^2 + 6a_3a_4\theta^2 + 26a_4^2\theta^2 + 18a_0a_5\theta^2 + \\
&+ 96a_1a_5\theta^2 + 9a_3a_5\theta^2 + 60a_4a_5\theta^2 + 32a_5^2\theta^2 + 72a_2^2\theta^4 + 18a_1a_3\theta^4 + 6a_0a_4\theta^4 + \\
&+ 48a_2a_4\theta^4 + 12a_3a_4\theta^4 + 12a_4^2\theta^4 + 12a_1a_5\theta^4 + 72a_2a_5\theta^4 + 12a_3a_5\theta^4 + 30a_4a_5\theta^4 + \\
&+ 26a_5^2\theta^4 + 18a_3^2d + 6a_2a_4d + 2a_4^2d + 6a_1a_5d + 24a_3a_5d + 6a_4a_5d + 12a_5^2d + \\
&+ 2a_4^2d\theta^2 + 3a_3a_5d\theta^2 + 2a_5^2d\theta^2 + 2a_5^2d\theta^4).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Como $d \equiv 17 (mod\ 36)$, pela Proposição 7.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 9d^5$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{9d^5}} = \frac{4}{3\sqrt{d^5}}.$$

5. Seja $d \equiv -17, 10 (mod\ 36)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 7.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\left(\frac{1+\theta^2+\theta^4}{3}\right) + a_5\left(\frac{\theta+\theta^3+\theta^5}{3}\right),$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_4(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\sigma_6(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\
&= \frac{2}{9}(18a_0^2 + 12a_0a_4 + 2a_4^2 + 18a_1^2\theta^2 + 9a_0a_2\theta^2 + 3a_0a_4\theta^2 + 3a_2a_4\theta^2 + a_4^2\theta^2 + \\
&+ 12a_1a_5\theta^2 + 2a_5^2\theta^2 + 18a_2^2\theta^4 + 9a_1a_3\theta^4 + 3a_0a_4\theta^4 + 12a_2a_4\theta^4 + 3a_4^2\theta^4 + \\
&+ 3a_1a_5\theta^4 + 3a_3a_5\theta^4 + a_5^2\theta^4 + 18a_3^2d + 3a_2a_4d + a_4^2d + 3a_1a_5d + 12a_3a_5d + \\
&+ 3a_5^2d + 2a_4^2d\theta^2 + 3a_3a_5d\theta^2 + a_5^2d\theta^2 + 2a_5^2d\theta^4).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Como $d \equiv -17, 10 (mod\ 36)$, pela Proposição 7.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 576d^5$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{576d^5}} = \frac{1}{6\sqrt{d^5}}.$$

6. Seja $d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36)$. Para $\alpha \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 7.3.1, segue que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\left(\frac{1+\theta^3}{2}\right) + a_4\left(\frac{\theta+\theta^4}{2}\right) + a_5\left(\frac{\theta^2+\theta^5}{2}\right),$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. Ao calcular a norma mínima de $\sigma_{\mathbb{K}}(\alpha)$ através do homomorfismo de Minkowski (usando a norma euclidiana em $\mathbb{R}^2$), obtemos

$$\begin{aligned}
||\sigma_{\mathbb{K}}(\alpha)||^2 &= ||(\sigma_1(\alpha), \sigma_4(\alpha), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha)), \Re(\sigma_3(\alpha)), \Im(\sigma_3(\alpha)))||^2 = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \Re^2(\sigma_2(\alpha)) + \Im^2(\sigma_2(\alpha)) + \Re^2(\sigma_3(\alpha)) + \Im^2(\sigma_3(\alpha)) = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = \\
&= (\sigma_1(\alpha))^2 + (\sigma_4(\alpha))^2 + \sigma_2(\alpha)\sigma_6(\alpha) + \sigma_3(\alpha)\sigma_5(\alpha) = \\
&= \frac{1}{2}(8a_0^2 + 8a_0a_3 + 2a_3^2 + 8a_1^2\theta^2 + 4a_0a_2\theta^2 + 2a_2a_3\theta^2 + 8a_1a_4\theta^2 + 2a_4^2\theta^2 + \\
&+ 2a_0a_5\theta^2 + a_3a_5\theta^2 + 8a_2^2\theta^4 + 2a_1a_3\theta^4 + 2a_0a_4\theta^4 + 2a_3a_4\theta^4 + 8a_2a_5\theta^4 + \\
&+ 2a_5^2\theta^4 + 2a_3^2d + 2a_2a_4d + 2a_1a_5d + 2a_4a_5d + 2a_4^2d\theta^2 + a_3a_5d\theta^2 + 2a_5^2d\theta^4).
\end{aligned}$$

Assim, $||\sigma_{\mathbb{K}}(\alpha)||^2$ assume mínimo quando $a_0 = \pm 1$ e $a_1 = a_2 = a_3 = a_4 = a_5 = 0$. Desse modo,

$$||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2 = 4 \Leftrightarrow ||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|| = 2 \Leftrightarrow \rho = \frac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2} = 1.$$

Como $d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36)$, pela Proposição 7.3.4, segue que $|\mathcal{D}(\mathbb{K})| = 729d^5$. Portanto, a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}} = \frac{2^2\,(1)^6}{\sqrt{729d^5}} = \frac{4}{27\sqrt{d^5}}.$$

Portanto, dos itens (1), (2), (3), (4), (5) e (6), segue o resultado. □

Exemplo 8.7.2. *Seja $\mathbb{K}$ um corpo de números de grau 6. Sob as condições do Teorema 8.7.2, obtemos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

(a) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[6]{2})$. Como $d = 2$ e $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{54\sqrt{d^5}} = \frac{1}{54\sqrt{2^5}} \approx 0,00327.$$

(b) Seja $\mathbb{K} = \mathbb{Q}(\sqrt[6]{3})$. Como $d = 3$ e $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$, segue que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{54\sqrt{d^5}} = \frac{1}{54\sqrt{3^5}} \approx 0,00118.$$

9 Conclusão

O segundo capítulo possibilitou a familiaridade com a área Teoria Algébrica dos Números e disponibilizou as ferramentas necessárias para consolidar este trabalho. Para a última seção deste capítulo, generalizamos as propriedades dos corpos de números $\mathbb{Q}(\sqrt[n]{d})$, com d livre de quadrados que forneceu aos demais capítulos as condições necessárias para a construção dos anéis de inteiros.

A busca pelos anéis de inteiros depende da estrutura do corpo e do seu elemento primitivo causando a complexidade de alguns casos e exigindo o auxílio computacional. Neste trabalho foi explorado uma maneira de encontrá-los de acordo com as características do polinômio minimal consequentemente usando os $\mathbb{Q}$-monomorfismos.

Nos capítulos de extensão de corpos de grau $2, 3, 4, 5, 6$ ficou registrado a procura dos anéis de inteiros com a obtenção das bases integrais e o estudo do discriminante, em alguns casos bem particulares podemos determinar a base integral apenas com as propriedades de discriminante. Além do mais, conhecemos algumas propriedades desses corpos que os tornam fascinantes tal como a padronização dos casos de acordo com graus. Para os trabalhos futuros instigamos o estudo: para o grau 3, dos polinômios minimais $p(x) = x^3+ax+b \in \mathbb{Z}[x]$; para o grau 4, dos polinômios minimais $p(x) = x^4+ax+b \in \mathbb{Z}[x]$, $p(x) = x^4 - d$, com d livre de cubos; e para os demais graus as mesmas indagações, buscando via polinômio característico o anel dos inteiros algébricos dessas extensões. Também, estimulamos o estudo dos graus como $n = p^k$ potência de primos, com $k \in \mathbb{N}$ ou $n = pq$ produto de primos.

Via homomorfismo de Minkowski, foi possível a definição dos reticulados algébricos e a identificação de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ como tal. Assim, coube uma minuciosa exploração de exemplos para obter reticulados de densidade ótima, mas, somente via $\mathcal{O}_{\mathbb{K}}$, não se permitiu ter exemplos bons e por este motivo desperta-se a curiosidade para estudar os reticulados algébricos sobre os $\mathbb{Z}$-módulos contidos no corpo $\mathbb{K}$.

As perspectivas futuras englobam a padronização dos graus e generalização dos casos em conjuntos com o estudo dos reticulados sobre os $\mathbb{Z}$-módulos contidos no corpo $\mathbb{K}$. Com isso, imagina-se que objetivamente podemos conseguir reticulados com dimensão ótima.

Referências

[1] PASTORELLI, M. *As 6 Direções de Gandhi: não se esqueça de olhar para elas todos os dias*. 2020. Acesso em: 20 de agosto de 2021. Disponível em: <https://www.bonsfluidos.com.br/espiritualidade/as-6-direcoes-de-gandhi-nao-se-esqueca-de-olhar-para-elas-todos-os-dias.phtml>.

[2] TEORIA dos números: a rainha da Matemática. Acesso em: 27 de agosto de 2021. Disponível em: <https://www.somatematica.com.br/coluna/gisele/25052001.php>.

[3] ARAUJO, R. R. de. *Anéis de inteiros de corpos de números e aplicações*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2015.

[4] VIANA, M. *Viana explica a descoberta da teoria da informação*. 2020. Acesso em: 27 de agosto de 2021. Disponível em: <https://impa.br/noticias/marcelo-viana-explica-a-descoberta-da-teoria-da-informacao/>.

[5] ANDRADE, A. A. de. *Uma introdução a teoria algébrica dos números*. 1. ed. São José do Rio Preto - SP: Amazon.com, 2021.

[6] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 5. ed. São Paulo: Saraiva, 2018.

[7] VICENTE, J. P. G. *Reticulados de Posto 3 em Corpos de Números*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2000.

[8] RODRIGUES, V. C. da S. *Reticulados de Posto 4 em Corpos de Números*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2001.

[9] RIBEIRO, A. C. *Reticulados Sobre Corpos de Números*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2003.

[10] ULHOA, F. C.; LOURENÇO, M. L. *Um Curso de Álgebra Linear*. São Paulo: EDUSP, 2005.

[11] JÚNIOR, C. F. B. *Notas de aula de álgebra comutativa (doutorado - UFPB e UFCG)*. [S.l.: s.n.], 2019.

[12] ATIYAH, M. F.; MACDONALD, I. G. *Introduction to Commutative Algebra*. Reading, Massachusetts: Addison-Wesley, 1969.

[13] SAMUEL, P. *Algebraic Theory of Numbers*. Paris: Hermann, 1970.

[14] ALVES, C.; ANDRADE, A. A. de. *Reticulados via Corpos Ciclotômicos*. São Paulo: UNESP, 2014.

[15] SAUTER, E.; AZEVEDO, F. S. de. *Análise de Fourier*. [S.l.]: UFRGS, 2020.

[16] BENEVIDES, F. S.; NETO, A. C. M. *Radiciação de números complexos no plano de Argand-Gauss*. [S.l.], 2020.

[17] NEBE, G.; SLOANE, N. J. A. *Table of Densest Packings Presently Known*. 2012. Acesso em: 20 de agosto de 2021. Disponível em: <http://www.math.rwth-aachen.de/ Gabriele.Nebe/LATTICES/density.html>.

Índice Remissivo