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

Livea Cichito Esteves

Anel de inteiros algébricos e discriminante de uma família de corpos de números cujo grau é uma potência de 2

São José do Rio Preto
2024

Livea Cichito Esteves

Anel de inteiros algébricos e discriminante de uma família de corpos de números cujo grau é uma potência de 2

Tese apresentada como parte dos requisitos para obtenção do título de Doutor 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

São José do Rio Preto
2024

E79a

Esteves, Livea Cichito
Anel de inteiros algébricos e discriminante de uma família de corpos de números cujo grau é uma potência de 2 / Livea Cichito Esteves. -- São José do Rio Preto, 2024
187 p.

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

1. Corpo de números. 2. Corpos puros. 3. Anel de inteiros algébricos. 4. Base integral. 5. Discriminante. 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.

Livea Cichito Esteves

Anel de inteiros algébricos e discriminante de uma família de corpos de números cujo grau é uma potência de 2

Tese apresentada como parte dos requisitos para obtenção do título de Doutor 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.

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
Orientador

Prof. Dr. Agnaldo J. Ferrari
F. C. - Unesp, Bauru - SP

Prof. Dr. Trajano P. da Nóbrega Neto
Ibilce - Unesp, S. J. Rio Preto - SP

Prof. Dr. Edson D. de Carvalho
Feis - Unesp, Ilha Solteira - SP

Prof. Dr. Robson R. de Araujo
IFSP, Catanduva - SP

São José do Rio Preto
07 de março de 2024

Às pessoas mais importantes da minha vida:
João Carlos, Maria Ines, Murilo e Rafael,
dedico.

AGRADECIMENTOS

Durante os quatro anos em que realizei o curso de Doutorado e a elaboração desta tese, tive o apoio de várias pessoas que foram fundamentais para realização deste sonho e, por isso, quero expressar aqui a minha gratidão.

Agradeço primeiramente a Deus, por me dar saúde, força e sabedoria para superar os momentos de dificuldade.

Aos meus pais, João Carlos e Maria Ines, e ao meu irmão, Rafael, por todo amor, apoio e carinho em todos os momentos.

Ao meu namorado, Murilo, por todo amor e cuidado, por me incentivar e me encorajar a prosseguir nos estudos, além de toda paciência e ajuda nos mais diversos momentos.

À minha amiga e parceira de pesquisa, Linara, por todo o conhecimento compartilhado durante a realização deste trabalho e a todos os amigos com quem compartilhei momentos de aprendizado e de diversão.

Ao meu orientador, Toninho, por toda paciência e dedicação em me orientar e pelos valiosos ensinamentos.

Aos professores titulares da banca examinadora, Prof. Dr. Trajano Pires da Nóbrega Neto (Unesp - São José do Rio Preto), Prof. Dr. Robson Ricardo de Araujo (IFSP - Catanduva), Prof. Dr. Agnaldo José Ferrari (Unesp - Bauru), Prof. Dr. Edson Donizete de Carvalho (Unesp - Ilha Solteira), e aos professores suplentes da banca examinadora, Prof. Dr. Everton Luiz de Oliveira (UFMS - Campo Grande), Profa. Dra. Cintya Wink De Oliveira Benedito (Unesp - São João da Boa Vista) e Prof. Dr. Leandro Bezerra de Lima (UFMS - Campo Grande), por aceitarem o convite e pelas valiosas contribuições ao trabalho.

À Capes, pelo apoio financeiro.

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

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

A beleza da matemática só se mostra
aos seguidores mais pacientes.
Maryam Mirzakhani

RESUMO

O objetivo deste trabalho é apresentar a estrutura do anel de inteiros algébricos e o discriminante do anel de inteiros algébricos de corpos de números do tipo $\mathbb{L} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[2^k]{d}$ e $d \neq 1$ é um inteiro livre de quadrados. Inicialmente, apresentamos a estrutura dos anéis de inteiros algébricos dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ com $d \equiv 2, 3 (mod\ 4)$ onde, nesse caso, $\mathbb{L}$ é monogênico. Na sequência, apresentamos bases integrais e os respectivos discriminantes para alguns corpos da forma $\mathbb{Q}(\sqrt[2^k]{d})$, para $k = 2, 3, 4, 5$, onde exploramos as estruturas dos anéis de inteiros algébricos de acordo com os valores de d. Posteriormente, como resultados principais desta tese, generalizamos essas bases e, com isso, também determinamos uma fórmula para o discriminante do anel de inteiros algébricos desses corpos $\mathbb{L}$. Nessa linha, apresentamos essas generalizações da seguinte forma: quando $d \equiv 5 (mod\ 8)$, quando $d \equiv 9 (mod\ 16)$ e, por fim, englobando todos os casos, apresentamos uma base integral e o discriminante do anel de inteiros algébricos dos corpos puros $\mathbb{Q}(\sqrt[2^k]{d})$ para $d \equiv 2^l + 1 (mod\ 2^{l+1})$ onde $2 \leq l \leq k-1$ e para $d \equiv 1 (mod\ 2^{k+1})$.

Palavras-chave: Corpo de números. Corpos puros. Anel de inteiros algébricos. Base integral. Discriminante.

ABSTRACT

The objective of this work is to present an integral basis and the discriminant of algebraic number fields of the type $\mathbb{L} = \mathbb{Q}(\theta)$, *where* $\theta = \sqrt[2^k]{d}$ *and* $d \neq 1$ *is a square-free integer. Initially, we present the rings of algebraic integers of fields* $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ *with* $d \equiv 2, 3 (mod\ 4)$ *where, in this case,* $\mathbb{L}$ *is monogenic. Afterwards, we present integral bases and the respective discriminants for some fields of the form* $\mathbb{Q}(\sqrt[2^k]{d})$*, for* $k = 2, 3, 4, 5$*, exploring their algebraic integer rings according to the values of* d*. Subsequently, as the main results of this thesis, comprising the main part of this work, we generalize these bases and, with this, we also determine a formula for the discriminant of these fields* $\mathbb{L}$*. Along these lines, we present these generalizations as follows: when* $d \equiv 5 (mod\ 8)$*, when* $d \equiv 9 (mod\ 16)$*, and finally, encompassing all cases, we present an integral basis and the discriminant of pure fields* $\mathbb{Q}(\sqrt[2^k]{d})$ *for* $d \equiv 2^l + 1 (mod\ 2^{l+1})$ *where* $2 \leq l \leq k-1$ *and for* $d \equiv 1 (mod\ 2^{k+1})$*.*

Keywords: Number field. Pure fields. Ring of algebraic integers. Integral bases. Discriminant.

Lista de Símbolos

$\equiv$	Equivalência
$\mathbb{N}$	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
$\mathbb{L}$	Corpo de números $\mathbb{L}$
$\mathcal{O}_{\mathbb{L}}$	anel de inteiros algébricos do corpo $\mathbb{L}$
$Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$	Traço do elemento $\alpha \in \mathbb{L}$ na extensão $\mathbb{L}/\mathbb{K}$
$N_{\mathbb{L}/\mathbb{K}(\alpha)}$	Norma do elemento $\alpha \in \mathbb{L}$ na extensão $\mathbb{L}/\mathbb{K}$
$N_{\mathbb{L}}(I)$	Norma do ideal $I \subset \mathcal{O}_{\mathbb{L}}$
$D(\mathbb{L})$	discriminante do anel de inteiros algébricos do corpo $\mathbb{L}$
det[A]	Determinante da matriz A

Sumário

Introdução

A Teoria dos Números é uma das clássicas linhas de pesquisas da matemática na qual o estudo está centrado no conceito de números inteiros e objetos relacionados como, por exemplo, a quantidade de números primos contidos no conjunto dos números inteiros, além da resolução de equações diofantinas. Podemos citar como um clássico problema dessa área o Último Teorema de Fermat, cujas tentativas de demonstrá-lo, que perduraram mais de três séculos, trouxeram diversos avanços em linhas de pesquisas distintas da matemática.

Um dos ramos dentro da Teoria dos Números é a Teoria Algébrica dos Números, cujo foco é a expansão do conceito de número inteiro. Mais precisamente, consiste no estudo de números complexos que são raízes de polinômios cujos coeficientes são racionais, os quais são chamados números algébricos. Além disso, se os polinômios em questão são mônicos e seus coeficientes são inteiros, suas raízes são conhecidas como inteiros algébricos e o conjunto formado por esses elementos de um corpo $\mathbb{L}$ de extensão finita sobre $\mathbb{Q}$ formam um anel, o qual recebe o nome de anel de inteiros algébricos do corpo $\mathbb{L}$.

O estudo desses anéis de inteiros algébricos de um corpo $\mathbb{L}$ possui grande relevância na Álgebra, principalmente na parte de aplicações. Dentre elas, destacam-se as construções de reticulados algébricos de boa densidade de centro, os quais são muito utilizados no estudo de códigos e criptografia, como pode ser visto, por exemplo, em [1] e [2]. De forma geral, essas construções são realizadas a partir do chamado Homomorfismo de Minkowski (canônico), o qual consiste em uma função aplicada sobre um $\mathbb{Z}$-módulo do anel de inteiros algébricos de um corpo de números de dimensão n sobre $\mathbb{Q}$ que resulta em um reticulado no espaço $\mathbb{R}^n$. Quando falamos na densidade de centro de um reticulado algébrico, no caso do homomorfismo canônico, um dos parâmetros necessários para seu cálculo é o discriminante do anel de inteiros algébricos do corpo $\mathbb{L}$, que destaca-se por sua dificuldade.

Além dos reticulados de alta densidade, outro tipo tem sido muito relevante nos últimos anos: os reticulados bem arredondados (*well-rounded*), que são aqueles em que o conjunto de vetores de norma mínima do reticulado gera o $\mathbb{R}^n$ (para mais detalhes, veja, por

exemplo, [3]). As aplicações envolvendo esses tipos de reticulados incluem problemas referentes ao número de contato (*kissing number*) e à diversidade de reticulados (para detalhes veja, por exemplo, [4] e [5]). A vantagem de obter reticulados desse modo reside na possibilidade de identificar os pontos do reticulado no $\mathbb{R}^n$ com os elementos do corpo de números $\mathbb{L}$. Com isso em vista, determinar quais reticulados algébricos são bem arredondados tem sido tópico de estudo de vários pesquisadores e, para determiná-los, também se faz necessário o conhecimento do anel de inteiros algébricos do corpo. Inclusive, em [6] foi provado que a imagem do anel de inteiros algébricos de um corpo quadrático via homomorfismo de Minkowski é um reticulado bem arredondado para apenas dois corpos imaginários, $\mathbb{L} = \mathbb{Q}(i)$ e $\mathbb{L} = \mathbb{Q}(\sqrt{-3})$. Nesse sentido, é de grande importância conhecer o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos de um corpo de números (veja as Definições 1.14 e 1.35) para a utilização dessas ferramentas. Além disso, esses fatores também podem ser úteis no estudo recente de Criptografia pós-quântica, cujos detalhes podem ser vistos em [7].

A procura do anel de inteiros algébricos de corpos de números tem sido objeto de estudo de vários matemáticos nos últimos anos, e resultados significativos têm surgido acerca desse assunto, principalmente abordando os corpos monogênicos, isto é, os corpos cuja base integral é potente (veja [8], por exemplo). Em particular, no início de 2015, Hameed [9] publicou um trabalho no qual apresentou um resultado onde analisou valores de d tais que os corpos do tipo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é inteiro livre de quadrados e $k \in \mathbb{N}$ são monogênicos. Para isso, o autor utilizou o conceito de índice de um inteiro algébrico (para mais detalhes veja Capítulo 2).

Também em 2015, Hameed [10] publicou um outro trabalho que consiste em determinar mais bases integrais além das potentes para o corpo de grau $2^k = 8$. A estratégia adotada por Hameed foi a de utilizar uma base integral do corpo de grau 4 conhecida de outros trabalhos como, por exemplo, [11] e [12], e explorar a extensão $\mathbb{Q}(\sqrt[4]{d}) \subset \mathbb{Q}(\sqrt[8]{d})$, a qual possui grau 2. Vale destacar que determinar uma base integral de um corpo não monogênico é um trabalho complexo, justificando assim a escolha do autor em restringir-se ao corpo de grau $2^k = 8$ nesses trabalhos. Os resultados presentes nos artigos [9] e [10] também podem ser encontrados em [13], sua tese de doutorado.

Dentro do mesmo escopo, outros trabalhos também foram publicados recentemente. Em fevereiro de 2021, Yakkou e Fadil exploraram os corpos cujo grau é uma potência de 3, no trabalho "On power integral bases of certain pure number fields definied by $x^{3^r} - m$", encontrado em [14]. Também em 2021, tivemos a contribuição de Facini em sua dissertação de mestrado [15] "Uma introdução aos corpos não abelianos de grau menor ou igual a 6", onde usando o polinômio característico, foi dado o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos dos corpos do tipo $\mathbb{Q}(\sqrt[n]{d})$, onde $2 \leq n \leq 6$

e $d \neq 1$ é um inteiro livre de quadrados. Em 2022, Yakkou publicou um trabalho focado em corpos não monogênicos [16], onde dado um corpo de números gerado pelo trinômio $x^n + ax^m + b$, o autor estabelece condições para a, b e n de modo que a base não seja a potente. Mais recentemente, em 2023, Fadil e Kchital no trabalho [17], intitulado "On monogenity of certain pure number fields defined by $x^{2^r 7^s} - m$", analisam em quais casos os corpos de grau $2^r 7^s$ e $m \neq 1$ livre de quadrados são monogênicos utilizando a teoria de polígonos de Newton. Fugindo um pouco dos casos tradicionais em que são considerados m livre de quadrados, o trabalho [18] explora os corpos cúbicos do tipo $\mathbb{Q}(\sqrt[3]{m})$ tal que $m \neq 1$ é livre de cubos e não livre de quadrados, apresentando uma base integral e o discriminante do anel de inteiros algébricos para esses corpos.

Embora os corpos monogênicos sejam muito importantes para as aplicações, principalmente devido à sua simplicidade, os anéis de inteiros algébricos dos demais corpos também podem ser aplicados a diversos contextos e, contudo, têm sido bem menos explorados, de modo que seu estudo, geralmente, se limita em abordar apenas casos particulares, como, por exemplo, em [19] e [20]. Um dos motivos que justificam esse fato é a falta de uma ferramenta imediata para facilitar este trabalho, como o índice de um inteiro algébrico que favorece esse estudo para os corpos monogênicos. Tendo em vista os avanços realizados nos últimos anos, a importância para algumas aplicações e a menor exploração para os casos não monogênicos, o presente trabalho tem como principal objetivo determinar o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos associado aos corpos de números do tipo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e $k \in \mathbb{N}$, os quais são chamados de corpos puros (*pure fields*) de grau 2^k, explorando o caso monogênico, já apresentado por Hameed, mas também as demais bases possíveis. Para isso, o texto está organizado em seis capítulos, sendo o primeiro dedicado aos conceitos preliminares da teoria algébrica dos números e os demais, que em conjunto abordam casos particulares e gerais, constituem o nosso resultado principal.

No Capítulo 1 retomamos alguns conceitos básicos da Teoria dos Números, como traço e norma de elementos do corpo, anel de inteiros algébricos, base integral e discriminante do anel de inteiros algébricos do corpo de números, que constituem uma base da teoria aqui desenvolvida. Além disso, também foi retomada algumas definições e propriedades envolvendo anel de Dedekind e ramificação de ideais, pois esses conceitos serão necessários para provar uma das proposições fundamentais para o desenvolvimento do trabalho. Na última seção, também exploramos alguns fatos a respeito do corpo $\mathbb{Q}(\sqrt[n]{d})$, o qual será nosso prinicipal objeto de estudo.

No Capítulo 2, baseado no artigo de Hameed, [9], apresentamos uma base integral e o discriminante do anel de inteiros algébricos dos corpos de números da forma $\mathbb{Q}(\sqrt[2^k]{d})$, com $d \neq 1$ um inteiro livre de quadrados e $d \equiv 2, 3 (mod\ 4)$, por meio do conceito de índice

de um inteiro algébrico. Esse tipo de corpo tem uma importância particular, pois, como veremos no decorrer do capítulo, o mesmo é monogênico, ou seja, uma base de seu anel de inteiros algébricos é potente.

No Capítulo 3, apresentamos as bases integrais e os discriminantes do anel de inteiros algébricos dos corpos de números da forma $\mathbb{Q}(\sqrt[2^k]{d})$, para $k = 2, 3, 4, 5$, com $d \neq 1$ um inteiro e livre de quadrados. O objetivo desse capítulo é apresentar a estrutura dos anéis de inteiros algébricos explicitamente além de apresentar as demonstrações em detalhes, a fim de que o leitor possa criar familiaridade com os passos e estratégias utilizados, pois os mesmos serão generalizados posteriormente. Além disso, embora esse capítulo trate apenas de casos particulares, o mesmo será essencial para a conclusão do resultado final da presente tese.

Nos Capítulos 4 e 5, damos os primeiros passos rumo à generalização dos resultados apresentados no Capítulo 3, onde, no Capítulo 4 o estudo se centraliza no caso em que $d \equiv 5(mod\ 8)$ ou, equivalentemente, $d \equiv 1(mod\ 4)$ e 4 é a maior potência de 2 que divide $d-1$. Fixando essa família de valores de $d \neq 1$, apresentamos uma base integral e o discriminante do anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, para todo $k \geq 1$. Já no Capítulo 5, nos concentramos no caso em que $d \equiv 9(mod\ 16)$ ou, equivalentemente, $d \equiv 1(mod\ 8)$ e 8 é a maior potência de 2 que divide $d-1$ e, utilizando de raciocínio análogo, apresentamos uma base e o discriminante do anel de inteiros algébricos dos corpos de números da forma $\mathbb{Q}(\sqrt[2^k]{d})$, para todo $k \geq 2$, destacando as semelhanças e diferenças entre as duas demonstrações.

No Capítulo 6, que contém nossa principal contibuição deste trabalho, apresentamos as bases integrais dos corpos de números da forma $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é inteiro livre de quadrados. Para isso, levamos em consideração o grau do corpo em questão e também o valor de d, pois as potências de 2 em que vale $d \equiv 1 \pmod{2^l}$ também são cruciais para a determinação da base integral. Analisando esses dois fatores foi possível determinar as estruturas das bases que geram estruturas de anéis de inteiros algébricos distintas para cada corpo de acordo com o grau e o valor de d e descrevê-las explicitamente. Para isso, enunciamos e demonstramos um teorema que descreve uma base integral de $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e $d \equiv 1 \pmod{2^l}$, para todo $k \geq 1$ e $l \geq 2$. Uma vez que o anel de inteiros algébricos é conhecido, também calculamos todos os discriminantes associados a essas bases.

Vale destacar ainda que os resultados obtidos na Seção 3.3 do Capítulo 3 assim como os resultados apresentados nos Capítulos 4, 5 e 6 são originais deste trabalho.

1 Resultados básicos de teoria algébrica dos números

Neste capítulo, introduzimos alguns conceitos básicos sobre teoria algébrica dos números necessários para a compreensão e para o desenvolvimento do trabalho. Para isso, apresentamos resultados sobre o traço e a norma de um elemento, norma de ideais, base integral, anel de Dedekind, discriminante e, para finalizar, fazemos uma análise do corpo $\mathbb{Q}(\sqrt[n]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados, destacando uma proposição, em particular, que visa estender um resultado conhecido da teoria dos números e que será fundamental no desnvolvimento dos capítulos seguintes. Para obter mais detalhes e se aprofundar nos tópicos que abordamos neste capítulo de maneira concisa, o leitor pode consultar as referências [21] e [22].

1.1 Traço e norma

Nesta seção abordamos conceitos relacionados ao traço e à norma de elementos de um corpo. Seja $\mathbb{K}$ um corpo de números, isto é, uma extensão finita dos racionais, e seja $\mathbb{L}$ um corpo tal que $\mathbb{K} \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{K}] = n$. Sejam $\sigma_1, \ldots, \sigma_n$ os n $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{C}$.

Definição 1.1. Seja $\alpha \in \mathbb{L}$.

1. O **traço** de α na extensão $\mathbb{L}/\mathbb{K}$ é definido por

$$Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha). \tag{1.1}$$

2. A **norma** de α na extensão $\mathbb{L}/\mathbb{K}$ é definida por

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha). \tag{1.2}$$

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

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = x^n - Tr_{\mathbb{L}/\mathbb{K}}(\alpha)x^{n-1} + \cdots + (-1)^n N_{\mathbb{L}/\mathbb{K}}(\alpha). \tag{1.3}$$

Proposição 1.2. *[21, Teor. 5, Cap. 2] Se $\alpha, \beta \in \mathbb{L}$ e $a \in \mathbb{K}$, então*

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta)$;
2. $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha) = a\,Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$;
3. $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$;
4. $N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\beta)$;
5. $N_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^n N_{\mathbb{L}/\mathbb{K}}(\alpha)$;
6. $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$.

Além disso, se $\mathbb{M}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$, então

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(\alpha))$;
2. $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\alpha))$.

Teorema 1.3. *[22, Prop. 1, Cap. II, Sec. 2.6] Se $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{K}$, então*

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

Observação 1.4. Quando consideramos $\mathbb{L}$ um corpo de números, para a norma e o traço de $\mathbb{L}$ sobre $\mathbb{Q}$, usamos a seguinte notação, respectivamente, $Tr_{\mathbb{L}}(\alpha)$ e $N_{\mathbb{L}}(\alpha)$, onde $\alpha \in \mathbb{L}$.

1.2 Anel de inteiros algébricos

Nesta seção, introduzimos dois conceitos que serão muito utilizados em todo o texto: inteiro algébrico e anel de inteiros algébricos. Para isso, sejam $A \subseteq B$ anéis comutativos com unidade e $\alpha \in B$.

Definição 1.5. 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. Em particular, quando $B \subseteq \mathbb{C}$ e $A = \mathbb{Z}$, o elemento α é chamado um **inteiro algébrico**.

Proposição 1.6. *[22, Cor. 1, Cap. II, Sec. 2.1] Se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha + \beta$, $\alpha - \beta$ e $\alpha\beta$ são inteiros sobre A.*

Proposição 1.7. *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_α são inteiros sobre A. Em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são inteiros sobre A.*

O conjunto formado pelos elementos inteiros de A sobre B formam um anel que contém A, descrito na próxima definição.

Definição 1.8. O conjunto

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

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

Definição 1.9. O anel A é chamado integralmente fechado em B quando $\mathcal{O}_B = A$. Se A é um domínio e $\mathbb{L}$ é o seu corpo de frações, o anel A é chamado integralmente fechado se $\mathcal{O}_{\mathbb{L}} = A$.

Definição 1.10. Seja $\mathbb{L} \subseteq \mathbb{C}$ um corpo de números.

1. Os elementos de $\mathbb{L}$ que são inteiros sobre $\mathbb{Z}$ são chamados de **inteiros algébricos** de $\mathbb{L}$.

2. O conjunto dos elementos $\mathbb{L}$ que são inteiros algébricos é chamado de **anel de inteiros algébricos** de $\mathbb{L}$, ou simplesmente, de **anel de inteiros algébricos** de $\mathbb{L}$, o qual denotamos por $\mathcal{O}_{\mathbb{L}}$.

1.3 Base integral

Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações e $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n.

Teorema 1.11. *[22, Teor. 1, Cap. II, Sec. 2.7] Se $\mathcal{O}_{\mathbb{L}}$ é o anel de inteiros algébricos de $\mathbb{L}$ sobre A, então $\mathcal{O}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre finitamente gerado de posto n.*

Corolário 1.12. *[22, Cor., Cap. II, Sec. 2.7] Se A um anel principal, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

Corolário 1.13. *[23, Teor. 6.5.2] Seja $\mathbb{L}$ um corpo de números de grau n. Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{L}}$ é um ideal, então $\mathcal{I}$ é um A-módulo livre de posto n.*

Definição 1.14. Seja $\mathbb{L}$ um corpo de números. Uma base do $\mathbb{Z}$-módulo livre $\mathcal{O}_{\mathbb{L}}$ é chamada de **base integral** de $\mathbb{L}$.

Definição 1.15. Seja $\mathbb{L} = \mathbb{Q}(\alpha)$ um corpo de números de grau n, com $\alpha \in \mathbb{L}$. Se o conjunto $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, então chamamos B de **base de potências** de $\mathbb{L}$ (ou **base potente**).

Definição 1.16. Seja $\mathbb{L}$ um corpo de números. Se o anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ possui uma base de potências, dizemos que o corpo $\mathbb{L}$ é **monogênico.**

1.4 Anel de Dedekind

Nesta seção, apresentamos algumas definições, lemas e propriedades com o objetivo final de enunciar o teorema que garante que em um domínio de Dedekind, um ideal não nulo pode ser fatorado como produto de primos de maneira única. O caso particular em que estamos interessados, é a validade desse resultado para o anel de inteiros algébricos de um corpo de números, o qual veremos que é um anel de Dedekind.

Definição 1.17. Sejam A um anel e M um A-módulo. O módulo M é chamado um **A-módulo Noetheriano** se satisfaz uma das seguintes condições:

1. Todo conjunto não vazio de submódulos de M possui um elemento maximal.
2. Toda sequência crescente de submódulos de M é estacionária.
3. Todo submódulo de M é finitamente gerado.

Um anel A é chamado Noetheriano se quando considerado como um A-módulo for Noetheriano.

Definição 1.18. Um anel A é chamado um **anel de Dedekind** se A é noetheriano, integralmente fechado e se todo ideal primo não nulo de A é maximal.

Teorema 1.19. *[22, Teor. 1, Cap. III, Sec. 3.4] Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de $\mathbb{K}$. Se $\mathcal{O}_{\mathbb{L}}$ é o fecho integral de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind e um A-módulo finitamente gerado.*

Como consequência desse teorema, podemos concluir que o anel de inteiros algébricos de qualquer corpo de números é um anel de Dedekind.

Definição 1.20. Seja A um domínio e $\mathbb{K}$ seu corpo de frações. Um ideal fracionário de A é um A-submódulo I de $\mathbb{K}$ tal que $dI \subset A$ para algum $d \in A$, com $d \neq 0$.

Teorema 1.21. *[22, Teor. 3, Cap. 3, Sec. 3.4] Seja A um domínio de Dedekind. Se I é um ideal fracionário não nulo de A, então I é expresso de maneira única como*

$$I = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

onde $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ são ideais primos de A e $e_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, g$.

Agora, consideramos $\mathbb{L}$ um corpo de números e $\mathcal{O}_\mathbb{L}$ o seu anel de inteiros algébricos, o qual é um domínio de Dedekind.

Definição 1.22. Sejam $\mathcal{A}$ e $\mathcal{B}$ ideais fracionários de $\mathcal{O}_\mathbb{L}$. O ideal $\mathcal{A}$ divide $\mathcal{B}$ quando existe um ideial inteiro $\mathcal{C}$ de $\mathcal{O}_\mathbb{L}$ tal que $\mathcal{B} = \mathcal{A}\mathcal{C}$. Nesse caso, denotamos $\mathcal{A}|\mathcal{B}$.

Definição 1.23. Seja $\mathcal{A}$ um ideal de $\mathcal{O}_\mathbb{L}$. A norma do ideal $\mathcal{A}$ é definida como sendo o número de elementos do anel quociente $\frac{\mathcal{O}_\mathbb{L}}{\mathcal{A}}$, ou seja,

$$N_\mathbb{L}(\mathcal{A}) = \#\frac{\mathcal{O}_\mathbb{L}}{\mathcal{A}}.$$

Proposição 1.24. *[22, pag. 52] A norma $N_\mathbb{L}(\mathcal{A})$ é finita.*

Proposição 1.25. *[22, Prop. 2, Sec. 3.5, Cap. III] Se $\mathcal{A}$ e $\mathcal{B}$ são ideais não nulos de $\mathcal{O}_\mathbb{L}$, então $N_\mathbb{L}(\mathcal{A}\mathcal{B}) = N_\mathbb{L}(\mathcal{A})N_\mathbb{L}(\mathcal{B})$.*

Agora, considerando uma extensão de corpos $\mathbb{L}/\mathbb{K}$ de grau n e P um ideal primo em $\mathcal{O}_\mathbb{K}$, segue que o ideal $I = P\mathcal{O}_\mathbb{L}$ pode não ser primo em $\mathcal{O}_\mathbb{L}$, entretanto, pode ser fatorado como no Teorema 1.21. Cada $\mathfrak{P}_i$ desta fatoração é chamado de **ideal primo acima** de P, enquanto P é um **ideal primo abaixo** de $\mathfrak{P}_i$. A partir disso, podemos concluir que para i satisfazendo $1 \leq i \leq g$, vale a igualdade $\mathfrak{P}_i \cap \mathcal{O}_\mathbb{K} = P$. Ademais, o expoente e_i na fatoração de $P\mathcal{O}_\mathbb{L}$ é chamado de **índice de ramificação** de $\mathfrak{P}_i$ sobre $\mathcal{O}_\mathbb{K}$ e a dimensão do espaço vetorial $\mathcal{O}_\mathbb{L}/\mathfrak{P}_i$ sobre o corpo $\mathcal{O}_\mathbb{K}/P$ é chamada de **grau residual** (ou grau inercial) de $\mathfrak{P}_i$ sobre $\mathcal{O}_\mathbb{K}$ e é denotada por f_i.

Proposição 1.26. *[22, Prop. 1, Sec. 2, Cap. V] Os ideais $\mathfrak{P}_i's$ são os ideais primos de $\mathfrak{B}$ de $\mathcal{O}_\mathbb{L}$ tal que $\mathfrak{B} \cap \mathcal{O}_\mathbb{L} = P$.*

A *Igualdade Fundamental* garante que $\sum_{i=1}^{g} e_i f_i = n$ [22, Teor. 1, Sec. 2, Cap. V]. Se $\mathbb{L}/\mathbb{K}$ é uma extensão galoisiana, então, devido ao fato de que todos os ideais primos acima de P são conjugados com relação aos automorfismos do grupo de Galois $Gal(\mathbb{L}/\mathbb{K})$, segue

que todos os graus residuais são iguais e denotados por f e todos os índices de ramificação são iguais e denotados por e. Assim, neste caso, a Igualdade Fundamental garante que $n = efg$. Com relação à fatoração de um ideal primo $P \subseteq \mathcal{O}_{\mathbb{K}}$ em $\mathcal{O}_{\mathbb{L}}$ segundo a expressão dada no Teorema 1.21, temos ainda as seguintes classificações:

1. O ideal P *se ramifica* em $\mathcal{O}_{\mathbb{L}}$ se $e_i > 1$ para algum $i \in \{1, 2, \ldots, g\}$. Caso contrário, P é chamado *não ramificado* em $\mathcal{O}_{\mathbb{L}}$.

2. O ideal P é *totalmente decomposto* em $\mathcal{O}_{\mathbb{L}}$ se $e_i = f_i = 1$, para todo $i \in \{1, 2, \ldots, g\}$.

3. O ideal P é *inerte* em $\mathcal{O}_{\mathbb{L}}$ se $e_i = 1$ e $f_i = n$, para algum $i \in \{1, 2, \ldots, g\}$.

4. O ideal P é *totalmente ramificado* em $\mathcal{O}_{\mathbb{L}}$ se $e_i = n$ e $f_i = 1$, para algum $i \in \{1, 2, \ldots, g\}$.

Em particular, se $\mathcal{P} \subset \mathcal{O}_{\mathbb{L}}$ é um ideal primo, então o corpo $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$ é um espaço vetorial sobre $\mathbb{Z}/\langle p \rangle$ de grau residual f, onde p é o único número primo abaixo de $\mathcal{P}$.

Proposição 1.27. *[24, Prop. 3.7.5] Se $\mathcal{P}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$, então $N_{\mathbb{L}}(\mathcal{P}) = p^f$, onde f é o grau residual de $\mathcal{P}$. Além disso, se $\mathcal{P}$ é um múltiplo do ideal $\mathcal{Q}$ e $N_{\mathbb{L}}(\mathcal{P}) = N_{\mathbb{L}}(\mathcal{Q})$, então $\mathcal{P} = \mathcal{Q}$.*

1.5 Discriminante

Nesta seção, apresentamos o conceito de discriminante de uma extensão de anéis. Para isso, sejam A e B anéis tais que $A \subseteq B$ e B é um A-módulo livre de posto finito n.

Definição 1.28. 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

$$D_{B/A}(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(Tr_{B/A}(\alpha_i \alpha_j)) \in A,$$

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

Proposição 1.29. *[22, Prop. 1, Cap. II, Sec. 2.7] Se $\{\beta_1, \ldots, \beta_n\}$ 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 $i = 1, \ldots, n$, então*

$$D_{B/A}(\beta_1, \ldots, \beta_n) = (\det(a_{ij}))^2 D_{B/A}(\alpha_1, \ldots, \alpha_n).$$

Corolário 1.30. *[23, Teor. 6.5.4] Seja A um domínio. Se $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ são bases de B sobre A, então $D_{B/A}(\alpha_1, \ldots, \alpha_n) = D_{B/A}(\beta_1, \ldots, \beta_n)$.*

Definição 1.31. O discriminante de B sobre A é definido como o ideal de A, gerado por $D_{B/A}(\alpha_1, \ldots, \alpha_n)$, onde $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de B sobre A, e denotamos $D(B/A)$.

Agora, apresentamos alguns resultados envolvendo discriminante do anel de inteiros algébricos de corpos de números. O Corolário 1.13 da Seção 1.3, afirma que o anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ é um $\mathbb{Z}$-módulo livre finitamente gerado de posto n. Este fato nos motiva a definir o discriminante do anel de inteiros algébricos dos corpos de números através da base integral.

Definição 1.32. Seja $\mathbb{L}$ um corpo de números. O discriminante do anel de inteiros algébricos de $\mathbb{L}$ é definido como o discriminante de uma base de seu anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ e é denotado por $D(\mathbb{L})$.

Proposição 1.33. *[23, Teor. 7.1.9] Sejam $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números de grau n e $\theta \in \mathbb{L}$ o seu elemento primitivo. Se $p(x)$ é o polinômio minimal de θ, então*

$$D_{\mathbb{L}}(\theta) = D_{\mathbb{L}}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{L}}(p'(\theta)), \tag{1.4}$$

onde $p'(x)$ é a derivada de $p(x)$.

Corolário 1.34. *Seja $\mathbb{L} = \mathbb{Q}(\theta)$ 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*

$$D_{\mathbb{L}}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n^2+n+2}{2}} (n^n d^{n-1}). \tag{1.5}$$

Proposição 1.35. *[23, Teor. 7.1.8] Seja $\mathbb{L}$ um corpo de números de grau n e seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$ contida no anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$. Se o discriminante $D_{\mathbb{L}}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é livre de quadrados, então $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{Z}$.*

A próxima definição, a qual será fortemente utilizada no capítulo seguinte, nos dá a ideia de índice de um inteiro algébrico.

Definição 1.36. Sejam θ um inteiro algébrico de grau n e $\mathbb{L} = \mathbb{Q}(\theta)$. O índice de θ é definido como sendo o índice da extensão $\mathbb{Z}[\theta] \subset \mathcal{O}_{\mathbb{L}}$ como grupos abelianos aditivos, ou seja,

$$Ind(\theta) = [\mathcal{O}_{\mathbb{L}} : \mathbb{Z}[\theta]].$$

Com base na Proposição 1.29, se $\mathbb{L}$ é um corpo de números de grau n e θ é seu elemento primitivo, então

$$D_{\mathbb{L}}(1, \theta, \ldots, \theta^{n-1}) = Ind(\theta)^2 D(\mathbb{L}).$$

Neste caso, se $Ind(\theta) = \pm 1$, então $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\theta]$.

1.6 O corpo $\mathbb{Q}(\sqrt[n]{d})$, com $d \neq 1$ um inteiro livre de quadrados

Nesta seção, veremos algumas propriedades e proposições a respeito dos corpos de números do tipo $\mathbb{L} = \mathbb{Q}(\sqrt[n]{d})$, com $d \neq 1$ um inteiro e livre de quadrados, uma vez que este corpo será nosso principal objeto de estudo, em particular, para $n = 2^k$.

Primeiramente, podemos afirmar que o elemento $\sqrt[n]{d}$ é um inteiro algébrico, pois é raiz do polinômio $p(x) = x^n - d$ que, por sua vez, é polinômio minimal de $\sqrt[n]{d}$ em $\mathbb{Z}$. Além disso, a extensão $\mathbb{Q}(\sqrt[n]{d}) \supset \mathbb{Q}$ tem grau n e um elemento primitivo de $\mathbb{Q}(\sqrt[n]{d})$ é o próprio $\sqrt[n]{d}$. Vale também ressaltar que, embora essa extensão $\mathbb{Q}(\sqrt[n]{d}) \supset \mathbb{Q}$ seja separável, já que o corpo $\mathbb{Q}$ possui característica zero, nem sempre ela é normal e, consequentemente, nem sempre é de Galois.

A próxima proposição será muito utilizada nos demais capítulos, pois fornece os traços dos elementos do tipo $(\sqrt[n]{d})^k$, valores que aparecerão ao calcular o discriminante do anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[n]{d})$.

Proposição 1.37. *[15, Prop. 2.6.8] Se $\mathbb{L} = \mathbb{Q}(\theta)$ é um corpo de números, onde $\theta = \sqrt[n]{d}$ com $d \in \mathbb{Z}$ livre de quadrados, então*

$$Tr_{\mathbb{L}}(\theta^k) = \begin{cases} nd^s, & \text{se } n|k \\ 0, & \text{caso contrário.} \end{cases} \tag{1.6}$$

A proposição seguinte traz um resultado bem conhecido da Teoria dos Números, onde o nosso próximo objetivo é generalizá-lo para um caso de nosso interesse.

Proposição 1.38. *[15, Prop. 2.6.9] Sejam $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[n]{d}$ com $d \in \mathbb{Z}$ livre de quadrados e $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \in \mathbb{L}$, com $a_0, a_1, a_2, \ldots, a_{n-1} \in \mathbb{Q}$. Se α é um inteiro algébrico, então $na_0, na_1, na_2, \ldots, na_{n-1} \in \mathbb{Z}$.*

Baseando-se na Proposição 1.38, o próximo resultado visa estendê-la para uma extensão quadrática $\mathbb{L} \supset \mathbb{K}$.

Proposição 1.39. *[10, Lema 3] Sejam $\mathbb{L} = \mathbb{Q}(\theta)$ e $\mathbb{K} = \mathbb{Q}(\theta^2)$, com $\theta = \sqrt[n]{d}$. Se $\eta = \alpha + \beta\theta \in \mathcal{O}_{\mathbb{L}}$ com $\alpha, \beta \in \mathbb{K}$, então $2\alpha, 2\beta \in \mathcal{O}_{\mathbb{K}}$.*

Demonstração. Dado um inteiro η contido no corpo $\mathbb{L}$, existem α, $\beta \in \mathbb{K}$ tais que $\eta = \alpha + \beta\theta$, uma vez que $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$. Sendo η inteiro em $\mathbb{L}$, segue pela Proposição 1.7 que seu traço e sua norma são inteiros em $\mathbb{K}$, ou seja, $Tr_{\mathbb{L}/\mathbb{K}}(\eta) = 2\alpha \in \mathcal{O}_{\mathbb{K}}$ e $N_{\mathbb{L}/\mathbb{K}}(\eta) = \alpha^2 - \beta^2\theta^2 \in \mathcal{O}_{\mathbb{K}}$. Agora, tomando a norma de ambos os lados em $2\eta = 2\alpha + 2\beta\theta$, obtemos $4N_{\mathbb{L}/\mathbb{K}}(\eta) = (2\alpha)^2 - (2\beta)^2\theta^2 \in \mathcal{O}_{\mathbb{K}}$, e logo, $(2\beta)^2\theta^2 \in \mathcal{O}_{\mathbb{K}}$. Como $2\beta \in \mathbb{K}$ e $\mathbb{K}$ é

um domínio de integridade, o ideal principal (2β) é um ideal fracionário, de acordo com a Definição 1.20. Desse modo, pelo Teorema 1.21 existem ideais primos $P_i \subset \mathcal{O}_{\mathbb{K}}$ e inteiros e_i tais que

$$(2\beta) = {P_1}^{e_1}{P_2}^{e_2}\dots{P_n}^{e_n},$$

onde se $e_i < 0$, então $P_i^{e_i} = (P_i^{-1})^{-e_i}$. Dessa forma, tomando $\mathcal{P}$ como a parte em que e_i são positivos e $\mathcal{Q}$ como a parte em que e_i são negativos, podemos escrever $(2\beta) = \mathcal{P}/\mathcal{Q}$, com $\text{mdc}(\mathcal{P}/\mathcal{Q}) = 1$. Se $\mathcal{Q} = 1$, pelo fato de que $\mathcal{P} \subset \mathcal{O}_{\mathbb{K}}$, poderíamos inferir que $(2\beta) \subset \mathcal{O}_{\mathbb{K}}$ e, consequentemente, $2\beta \in \mathcal{O}_{\mathbb{K}}$, de onde concluiríamos a prova. Por essa razão, vamos supor que $\mathcal{Q} \neq 1$. Assim, existe um fator primo Q de $\mathcal{Q}$. Como $(2\beta)^2\theta^2 = \frac{\mathcal{P}^2}{\mathcal{Q}^2}\theta^2 \in \mathcal{O}_{\mathbb{K}}$, segue que Q divide θ^2, isto é, $\theta^2 = Q^2 I$, para algum ideal I. Tomando a norma de ideais com respeito a $\mathbb{K}/\mathbb{Q}$ em ambos os lados, segue que

$$\begin{aligned} d &= \theta^2(\theta\zeta_n^2)^2(\theta\zeta_n^4)^2(\theta\zeta_n^6)^2\dots(\theta\zeta_n^{n-2})^2 = \theta^2\sigma_2(\theta^2)\sigma_4(\theta^2)\dots\sigma_{n-2}(\theta^2) \\ &= N(\theta^2) = (N_{\mathbb{K}}(Q))^2 N_{\mathbb{K}}(I) = (p^f)^2 N_{\mathbb{K}}(I). \end{aligned}$$

onde σ_i são os automorfismos, ζ_n é a raiz da unidade e f denota o grau residual de Q sobre $\mathcal{O}_{\mathbb{K}}$. Pela Proposição 1.27, segue que $f > 1$ e, assim, d é divisível por p^2, o que é um absurdo, pois d é livre de quadrados. Logo, $\mathcal{Q} = 1$ e, portanto, $2\beta \in \mathcal{O}_{\mathbb{K}}$. □

Essa proposição será o ponto inicial para provar vários resultados dos capítulos seguintes, uma vez que em nossas construções sempre iremos considerar extensões de grau 2.

1.7 Considerações finais

O objetivo desse capítulo foi apresentar definições e resultados básicos da teoria algébrica dos números que serão utilizados no desenvolvimento dos demais capítulos. Neste sentido, apresentamos resultados sobre traço, norma, base integral, discriminante e destacamos alguns fatos a respeito do corpo $\mathbb{Q}(\sqrt[n]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. Também apresentamos um resultado (Proposição 1.39) que, embora não integre os conceitos básicos da teoria dos números, deriva de um resultado muito usual e será usado constantemente nos Capítulos 3, 4, 5 e 6. No próximo capítulo, nos restringiremos a um caso particular do corpo $\mathbb{Q}(\sqrt[n]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados, apresentando uma base integral e o discriminante do anel de inteiros algébricos para $n = 2^k$ e $d \equiv 2, 3 \pmod 4$.

2 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \equiv 2, 3 (mod\ 4)$

Uma consequência imediata do Teorema do Elemento Primitivo, é o fato de que todo corpo de números possui uma base potente. Além disso, usualmente nos deparamos com corpos cujos anéis de inteiros algébricos também possuem esse tipo de base. Nesse ponto, podemos nos perguntar se todo anel de inteiros algébricos de um corpo de números admite base potente, ou seja, se os anéis de inteiros algébricos possuem essa mesma propriedade que os corpos de números. Porém, a resposta para essa pergunta é negativa, pois nem sempre um anel de inteiros algébricos admitirá uma base potente. Sendo assim, dado um corpo $\mathbb{L}$, uma questão que surge naturalmente é: "Esse corpo é monogênico?" Isto é, existe $\alpha \in \mathcal{O}_{\mathbb{L}}$ tal que $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{L}}$? Responder a essa questão para $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ é um dos objetivos deste capítulo.

O interesse em solucionar esse problema se dá devido ao fato da base potente ser a mais trivial de modo que torna-se relevante determinar quais são os corpos monogênicos e o elemento gerador dessa base. Os corpos quadráticos fornecem um exemplo bem conhecido de corpo monogênico, onde se $\mathbb{L} = \mathbb{Q}(\theta)$, com $\theta = \sqrt{d}$ e $d \neq 1$ um inteiro e livre de quadrados, então seu anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ (para mais detalhes, veja [25]) é dado por

$$\begin{cases} \mathbb{Z}[\theta], & \text{se} \quad d \equiv 2, 3 (mod\ 4), \text{ e} \\ \mathbb{Z}\left[\frac{1+\theta}{2}\right] & \text{se} \quad d \equiv 1 (mod\ 4). \end{cases} \tag{2.1}$$

Outro exemplo bastante comum, que também pode ser visto em [25], são os corpos ciclotômicos $\mathbb{L} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade, cujo anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ é dado por $\mathbb{Z}[\zeta]$, e o mesmo ocorre para o corpo maximal real $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, o qual possui o anel de inteiros algébricos $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

Neste capítulo, determinamos uma base para o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \equiv 2, 3 (mod\ 4)$ é um inteiro e livre de quadrados, e veremos que uma base integral dos corpos quadráticos dada por (2.1) para o caso $d \equiv 2, 3 (mod\ 4)$ não se trata de um caso isolado, mas sim de uma propriedade que abrange todos os corpos puros cujo

grau é uma potência de 2. Além disso, calculamos o discriminante do anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[2^k]{d})$ a partir dessa base. Note que, quando trabalhamos com o caso $d \equiv 2, 3(mod\ 4)$ um inteiro e livre de quadrados, os únicos valores de d que não serão englobados são os valores tais que $d \equiv 1(mod\ 4)$, pois se tívessemos $d \equiv 0(mod\ 4)$, então d não seria livre de quadrados. Esse caso restante será analisado nos próximos capítulos.

2.1 Anel de inteiros algébricos

Inicialmente, baseado no que foi apresentado em [9], apresentamos uma base integral de $\mathbb{Q}(\sqrt[2^k]{d})$. Para isso, faremos uso do conceito de índice de um inteiro algébrico além de alguns resultados auxiliares. Os próximos dois lemas também serão cruciais no desenvolvimento da seção.

Lema 2.1. *[23, Teor. 7.1.7] Se $\mathbb{L} = \mathbb{Q}(\theta)$ é um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{L}}$, então $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ é uma base integral de $\mathbb{L}$ se, e somente se, $Ind(\theta) = 1$.*

Lema 2.2. *[26, Lema 2.17] Sejam θ um inteiro algébrico e $\mathbb{L} = \mathbb{Q}(\theta)$. Se o polinômio minimal de θ sobre $\mathbb{Q}$ é Eisenstein com respeito ao primo p (também dito p-Eisentein), ou seja, é da forma $x^n + a_{n-1}x^{n-1} + a \ldots + a_0$ onde $a_0, a_1, \ldots a_{n-1}$ são divisíveis por p e a_0 não é divisível por p^2, então $Ind(\theta)$ não é divisível por p.*

Devido ao Lema 2.2, para demonstrar que o corpo $\mathbb{L}$ é monogênico, basta mostrarmos que o polinômio $x^{2^k} - d$ é p-Eisenstein para todo primo p dividindo d, onde $d \equiv 2, 3(mod\ 4)$. Dessa forma, podemos concluir que o índice de θ é 1 e, portanto, pelo Lema 2.1, segue que uma base de $\mathcal{O}_{\mathbb{L}}$ é potente.

Teorema 2.3 ([9], Teor. 2.1)**.** *Seja $\mathbb{L} = \mathbb{Q}(\theta)$, onde θ é uma raiz do polinômio $f(x) = x^{2^k} - d$, com $d \neq 1$ inteiro e livre de quadrados. Se $d \equiv 2, 3(mod\ 4)$, então $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, onde $n = 2^k$ é uma base integral de $\mathbb{L}$, ou seja, $\mathbb{L}$ é monogênico.*

Demonstração. Para um inteiro livre de quadrados $d \neq 1$, o polinômio $f(x) = x^{2^k} - d$ é p-Eisenstein para todo primo p que divide d, uma vez que d é livre de quadrados. Assim, $f(x)$ é irredutível sobre $\mathbb{Q}$. Além disso, de acordo com o Corolário 1.34, segue que

$$D_{\mathbb{L}}(1, \theta, \ldots, \theta^{n-1}) = (-1)^{2^{k-1}+1}(2^k)^{2^k} d^{2^k-1}.$$

Por outro lado, pela Proposição 1.29, segue que

$$D_{\mathbb{L}}(1, \theta, \ldots, \theta^{n-1}) = Ind(\theta)^2 D(\mathbb{L}).$$

Agora, vamos analisar a fatoração do índice dos casos: $d \equiv 2(mod\ 4)$ e $d \equiv 3(mod\ 4)$.

1. $d \equiv 2(mod\ 4)$. Neste caso, $d = 2(2k' + 1)$, com $k' \in \mathbb{Z}$. Assim, podemos fatorar d como produto de primos em $\mathbb{Z}$ como

$$d = 2p_1p_2 \dots p_l,$$

onde cada p_i é um primo ímpar distinto (pois d é livre de quadrados), com $1 \leq i \leq l$. Portanto,

$$D_{\mathbb{L}}(1, \theta, \dots, \theta^{n-1}) = \pm(2^k)^{2^k}(2p_1p_2 \dots p_l)^{2^k-1} = Ind(\theta)^2 D(\mathbb{L}).$$

Pelo Lema 2.2, segue que $Ind(\theta)$ não é divisível por 2 e também não é divisível por p_i, para todo $1 \leq i \leq l$. Portanto, $Ind(\theta) = 1$ e, assim, $D_{\mathbb{L}}(1, \theta, \dots, \theta^{n-1}) = D(\mathbb{L})$. Consequentemente, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\theta]$, isto é, $\mathbb{L}$ é monogênico.

2. $d \equiv 3(mod\ 4)$. Neste caso, $d = 4k' + 3$, com $k' \in \mathbb{Z}$. Como o critério de Eisenstein também pode ser aplicado a um polinômio depois de uma transformação, faremos uma mudança de variável no polinômio $f(x)$, transformando x em $x - 1$, de onde obtemos a seguinte expressão

$$g(x) = f(x - 1) = (x - 1)^{2^k} - d = x^{2^k} + a_{2^k-1}x^{2^k-1} + \dots + (1 - d),$$

onde cada a_i, com $1 \leq i \leq 2^k - 1$, é divisível por 2 e por $1 - d$. Mas $1 - d = 1 - (4k' + 3) = -4k' - 2 = -2(2k' + 1)$, de modo que $1 - d$ é divisível por 2 e não por 2^2. Assim, $g(x)$ é 2-Eisenstein, implicando que $g(x)$ é irredutível sobre $\mathbb{Q}$ e, desta forma, $f(x) = x^{2^k} - d$ também o é. Portanto, nenhum dos fatores primos de $D_{\mathbb{L}}(\theta) = D_{\mathbb{L}}(\theta - 1)$ divide $Ind(\theta)$ e, deste modo, $Ind(\theta) = 1$ e $D_{\mathbb{L}}(\theta) = D(\mathbb{L})$. Consequentemente, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\theta]$, ou seja, $\mathbb{L}$ é monogênico.

Portanto, em ambos os casos, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\theta]$. □

2.2 Discriminante

Uma vez que conhecemos uma base integral de um corpo, é natural o interesse em calcular o seu discriminante. Neste caso, por se tratar do corpo monogênico, o seu discriminante é facilmente calculado, pois coincide com o discriminante do seu polinômio minimal, conforme o próximo Teorema e cujos resultados podem ser encontrados em [9] para $k \geq 2$ e em [25] para $k = 1$.

Teorema 2.4. *Seja o corpo de números $\mathbb{L} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[n]{d}$, com d livre de quadrados e $n = 2^k$, $k > 1$. Se $d \equiv 2, 3(mod\ 4)$, então o discriminante do anel de inteiros algébricos*

$\mathcal{O}_{\mathbb{L}}$ de $\mathbb{L}$ é dado por

$$D(\mathbb{L}) = \begin{cases} 4d, & se \quad k = 1 \ e \\ -n^n d^{n-1} & se \quad k \geq 2. \end{cases}$$

Demonstração. Como uma base de $\mathcal{O}_{\mathbb{L}}$ é uma base potente $\{1, \theta, \theta^2, \ldots, \theta^{n-2}, \theta^{n-1}\}$, segue que podemos calcular o discriminante do anel de inteiros algébricos do corpo de números $\mathbb{L} = \mathbb{Q}(\theta)$ utilizando o Corolário 1.34, através do polinômio minimal $p(x) = x^{2^k} - d$ do elemento primitivo $\theta = \sqrt[2^k]{d}$. Assim,

$$D_{\mathbb{L}}(\theta) = D_{\mathbb{L}}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n^2+n+2}{2}}(n^n d^{n-1}).$$

Se $n = 2$, segue que $D_{\mathbb{L}}(\theta) = 4d$. Agora, se $k \geq 2$, sendo $n = 2^k$ segue que

$$(-1)^{\frac{n^2+n+2}{2}} = (-1)^{\frac{2^{2k}+2^k+2}{2}} = (-1)^{\frac{2(2^{2k-1}+2^{k-1}+1)}{2}} = (-1)^{2^{2k-1}+2^{k-1}+1} = -1,$$

visto que $2^{2k-1} + 2^{k-1} + 1$ é ímpar para $k \geq 2$. Portanto, $D_{\mathbb{L}}(\theta) = -n^n d^{n-1}$, o que prova o teorema. □

2.3 Considerações finais

Reconhecer quais são os corpos monogênicos tem grande relevância na Teoria de Números, como mencionado acima. Todavia, determinar os corpos que não são monogênicos também tem sido um grande desafio, e determinar explicitamente suas respectivas bases integrais configura um problema ainda maior. Outro fato que tem incentivado a busca por esses corpos é o fato de que bons reticulados algébricos podem vir a ser gerados por ideais fornecidos por esses anéis de inteiros algébricos. Diante disso, determinar bases integrais para corpos além do monogênico será o objetivo dos capítulos seguintes.

3 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $2 \leq k \leq 5$

Este capítulo é dedicado a apresentação do anel de inteiros algébricos e do discriminante do anel de inteiros algébricos de certos corpos puros de grau 4, 8, 16 e 32, explorando tanto os corpos monogênicos como os corpos que fornecem bases distintas. No caso de grau 4, tal abordagem já foi desenvolvida e pode ser encontrada em [15] e [12], sendo a estratégia utilizada na prova do anel de inteiros algébricos a análise do polinômio característico, estudando todos os seus coeficientes. Já para o grau 8, veja [10], por exemplo, no qual a estratégia utilizada na prova foi distinta. Para obter o anel de inteiros algébricos do corpo puro de grau 8, Hameed, em [10], recorreu à base integral do corpo de grau 4 e trabalhou com essa extensão de grau 2. Aqui, apresentamos uma versão para a demonstração da base integral de grau 4 por meio da estratégia utilizada por Hameed, ou seja, fazendo o uso da base integral conhecida para o corpo quadrático. Ademais, apresentamos uma demonstração sutilmente diferente da feita em [10] para o corpo puro de grau 8, pois embora a técnica utilizada seja a mesma, tomamos algumas igualdades e congruências no decorrer da prova diferentes das tomadas por ele tendo em vista a futura generalização do resultado. No caso do grau 16, utilizamos o mesmo raciocínio, enquanto que para o grau 32 apresentamos uma base e omitimos a demonstração, uma vez que é semelhante ao caso de grau 16 e aos demais casos.

3.1 Base integral e discriminante do corpo puro de grau 4

Os corpos quárticos $\mathbb{L}$ são corpos de números cujo grau da extensão é quatro, ou seja, $[\mathbb{L} : \mathbb{Q}] = 4$. O objetivo deste capítulo é apresentar o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos do corpo quártico $\mathbb{L} = \mathbb{Q}(\sqrt[4]{d})$ que tem $p(x) = x^4 - d$ como polinômio minimal, com a restrição de que $d \neq 1$ seja inteiro livre de quadrados. Outras versões dessa base podem ser obersavadas, por exemplo, em [27], [28],

[12],[29] e [15].

3.1.1 Anel de inteiros algébricos

Nesta seção, apresentamos uma base integral do corpo quártico $\mathbb{Q}(\sqrt[4]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. O valor de d, mais precisamente sua congruência módulos 4 e 8, é o fator que determina a estrutura do anel de inteiros algébricos, o qual é dado pelo próximo teorema.

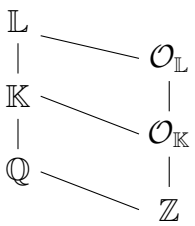
Teorema 3.1. *Seja* $\mathbb{L} = \mathbb{Q}(\theta)$ *um corpo de números, onde* $\theta = \sqrt[4]{d}$ *com* $d \neq 1$ *um inteiro e livre de quadrados. O anel de inteiros algébricos* $\mathcal{O}_{\mathbb{L}}$ *de* $\mathbb{L}$ *é dado por*

$$\mathcal{O}_{\mathbb{L}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3, \text{ se } d \not\equiv 1 (mod\ 4) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{1+\theta^2}{2}\right) + \mathbb{Z}\left(\frac{\theta+\theta^3}{2}\right), \text{ se } d \equiv 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{1+\theta^2}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Demonstração. Faremos a demonstração analisando as congruências de d.

1. O primeiro caso, $d \equiv 2, 3 (mod\ 4)$, é uma consequência direta do Teorema 2.3.

2. Agora, para os demais casos, $d \equiv 5 (mod\ 8)$ ou $d \equiv 1 (mod\ 8)$, baseando-se na prova que consta em [10], vamos utilizar uma base integral dos corpos quadráticos, resultado bastante conhecido da Teoria dos Números e, trabalhando a partir dessa base, obtemos o anel de inteiros algébricos dos corpos quárticos. Se $\theta = \sqrt[4]{d}$, com $d \neq 1$ inteiro livre de quadrados e $d \equiv 1 (mod\ 4)$, que engloba ambos os casos, $d \equiv 5 (mod\ 8)$ e $d \equiv 1 (mod\ 8)$, então segue que $\{1, \frac{1+\theta^2}{2}\}$ é uma base integral de $\mathbb{Q}(\sqrt[2]{d}) = \mathbb{Q}(\theta^2)$. Chamando $\mathbb{K} = \mathbb{Q}(\sqrt[2]{d}) = \mathbb{Q}(\theta^2)$, $\mathbb{L} = \mathbb{Q}(\sqrt[4]{d}) = \mathbb{Q}(\theta)$, e $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$ seus respectivos anéis de inteiros algébricos, obtemos as seguintes sequências:



onde $\{1, \theta^2\}$ é base de $\mathbb{K}$ sobre $\mathbb{Q}$, $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$ e $\{1, \frac{1+\theta^2}{2}\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Utilizando esses fatos, provaremos a validade do resultado. Por facilidade de notação, denotemos $\omega_1 = \frac{1+\theta^2}{2}$ e $\omega_2 = \frac{1+\theta+\theta^2+\theta^3}{4}$. Assim, nosso objetivo é mostrar que $\{1, \theta, \omega_1, \omega_1\theta\}$ é base integral de $\mathbb{L}$ se $d \equiv 5 (mod\ 8)$ ou,

equivalentemte, $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$, e $\{1, \theta, \omega_1, \omega_2\}$ é base integral de $\mathbb{L}$ se $d \equiv 1(mod\ 8)$. Note que, para o caso $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$, porquanto $\{1, \frac{1+\theta^2}{2}\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, a prova se resume em mostrar a igualdade $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$. Começamos por esse caso, verificando as duas inclusões.

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Assim, uma vez que $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que existem $\alpha', \beta' \in \mathbb{K}$ tal que $\eta = \alpha' + \beta'\theta$. Pela Proposição 1.39, segue que $2\alpha', 2\beta' \in \mathcal{O}_{\mathbb{K}}$, de modo que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tais que $\alpha' = \frac{\alpha}{2}$ e $\beta' = \frac{\beta}{2}$. Logo, $2\eta = \alpha + \beta\theta$. Tomando a norma de ambos os lados na extensão $\mathbb{L}/\mathbb{K}$ e usando as propriedades contidas na Proposição 1.2, segue que

$$N(2\eta) = N(\alpha+\beta\theta) \Rightarrow\ 4N(\eta) = \alpha^2 - \beta^2\theta^2 \Rightarrow \alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \quad (3.1)$$

Como $\alpha,\ \beta \in \mathcal{O}_{\mathbb{K}}$ e $\{1, \omega_1\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ tais que $\alpha = a_0 + a_1\omega_1$ e $\beta = b_0 + b_1\omega_1$. Substituindo essas igualdades na Equação (3.1), segue que

$$\alpha^2 - \beta^2\theta^2 = a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1 - (b_0^2 + b_1^2\omega_1^2 + 2b_0b_1\omega_1)\theta^2 \equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}). \quad (3.2)$$

Reescrevendo a Equação (3.2) em termos da congruência módulo 2, segue que

$$\alpha^2 - \beta^2\theta^2 = a_0^2 + a_1^2\omega_1^2 - (b_0^2 + b_1^2\omega_1^2)\theta^2 \equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}). \quad (3.3)$$

Nesse corpo, são válidas as congruências $\omega_1^2 \equiv \omega_1 + 1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e $\theta^2 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$. De fato, como $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$, segue que existe $m \in \mathbb{Z}$ ímpar tal que $d - 1 = 4m$ e, logo, $\frac{d-1}{4} = m$. Assim,

$$\begin{aligned} \omega_1^2 &= \left(\tfrac{1+\theta^2}{2}\right)^2 = \tfrac{1+2\theta^2+\theta^4}{4} = \tfrac{1+2\theta^2+d}{4} = \tfrac{2+2\theta^2}{4} + \tfrac{d-1}{4} = \tfrac{1+\theta^2}{2} + m = \omega_1 + m \\ &\equiv \omega_1 + 1(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Para a segunda congruência, uma vez que $2\omega_1 \in 2\mathcal{O}_{\mathbb{K}}$, da igualdade $\omega_1 = \frac{1+\theta^2}{2}$, segue que $\theta^2 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$. Além disso, para todo $x \in \mathbb{Z}$, verifica-se que $x^2 \equiv x(mod\ 2)$. Efetuando essas substituições na Equação (3.3), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0 + a_1\omega_1 + a_1 - b_0 - b_1\omega_1 - b_1 \\ &= (a_0 + a_1 - b_0 - b_1) + (a_1 - b_1)\omega_1 \\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Como $\{1, \omega_1\}$ é base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e os coeficientes da combinação linear

acima são inteiros, segue que

$$\begin{cases} (a_0 + a_1 - b_0 - b_1) \equiv 0 \ (mod\ 2) \\ (a_1 - b_1) \equiv 0 \ (mod\ 2). \end{cases}$$

Assim,

$$\begin{cases} a_0 \equiv b_0 \ (mod\ 2) \\ a_1 \equiv b_1 \ (mod\ 2) \\ a_0^2 \equiv b_0^2 \ (mod\ 4) \\ a_1^2 \equiv b_1^2 \ (mod\ 4) \\ 2b_0b_1 \equiv 2a_0a_1 (mod\ 4). \end{cases} \tag{3.4}$$

Substituindo as congruências módulo 4 contidas no Sistema (3.4) na Equação (3.2), segue que

$$\alpha^2 - \beta^2\theta^2 = a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1 - (a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1)\theta^2 \equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}).$$

Colocando $1 - \theta^2$ em evidência, obtemos

$$\alpha^2 - \beta^2\theta^2 = (1 - \theta^2)(a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1) \equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}).$$

Mas, $1 - \theta^2 = 1 - 2\theta^2 + \theta^2 = 2\omega_1 - 2\theta^2$, donde segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= (a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1)(2\omega_1 - 2\theta^2) \\ &= 2a_0^2\omega_1 - 2a_0^2\theta^2 + 2a_1^2\omega_1^3 - 2a_1^2\omega_1^2\theta^2 + 4a_0a_1\omega_1^2 - 4a_0a_1\omega_1\theta^2 \\ &\equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Utilizando o fato que $2x \equiv 0 \ (mod\ 4) \Rightarrow x \equiv 0 \ (mod\ 2)$ e, em seguida, usando novamente as congruências $\omega_1^2 \equiv \omega_1 + 1 (mod\ 2\mathcal{O}_{\mathbb{K}})$, $\omega_1^3 \equiv 1 (mod\ 2\mathcal{O}_{\mathbb{K}}), \theta^2 \equiv 1 (mod\ 2\mathcal{O}_{\mathbb{K}})$ e $x^2 \equiv x (mod\ 2)$, para todo $x \in \mathbb{Z}$, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0\omega_1 - a_0 + a_1 - a_1\omega_1 - a_1 \\ &= -a_0 + (a_0 - a_1)\omega_1 \\ &\equiv 0 \ (mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Assim,

$$\begin{cases} -a_0 \equiv 0 \ (mod\ 2) \\ a_0 - a_1 \equiv 0 \ (mod\ 2). \end{cases}$$

A única solução desse sistema é $a_0, a_1 \equiv 0 (mod\ 2)$ e, substituindo-as no Sistema

(3.4), segue que $b_0, b_1 \equiv 0(mod\ 2)$, ou seja, a_0, a_1, b_0 e b_1 são todos pares. Por conseguinte, $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$ e, portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ e ω_1 são inteiros algébricos em $\mathbb{L}$, uma vez que pertencem a $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$, segue que

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \omega_1][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto,

$$\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta].$$

3. Utilizando raciocínio análogo, agora, provaremos o resultado para $d \equiv 1(mod\ 8)$. Neste caso, diferentemente do caso exposto no item 2, a igualdade $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$ não é válida, de forma que é necessário mostrar que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \omega_1, \omega_2]$.

a) $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[1, \theta, \omega_1, \omega_2]$. Como no caso anterior, tomando $\eta \in \mathcal{O}_{\mathbb{L}}$, existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tal que $2\eta = \alpha + \beta\theta$ e, logo,

$$\alpha^2 - \beta^2\theta^2 \equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{3.5}$$

Como $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$, existem $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ tais que $\alpha = a_0 + a_1\omega_1$ e $\beta = b_0 + b_1\omega_1$. Note que estamos utilizando a mesma base de $\mathcal{O}_{\mathbb{K}}$ adotada no caso anterior, $\{1, \omega_1\}$, visto que para esta família de valores de $d \neq 1$ na qual $d \equiv 1 \pmod 8$, claramente se verifica $d \equiv 1 \pmod 4$. Assim, substituindo esses valores de α e β na Equação (3.5), segue que

$$\alpha^2 - \beta^2\theta^2 = a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1 - (b_0^2 + b_1^2\omega_1^2 + 2b_0b_1\omega_1)\theta^2 \equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{3.6}$$

Reescrevendo a Equação (3.6) utilizando a congruência módulo 2, segue que

$$\alpha^2 - \beta^2\theta^2 = a_0^2 + a_1^2\omega_1^2 - (b_0^2 + b_1^2\omega_1^2)\theta^2 \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \tag{3.7}$$

Observe que, exatamente como no caso anterior, nesse corpo é válido que $\theta^2 \equiv 1 \pmod 2$ e, além disso, também verifica-se que $\omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$, pois como $d \equiv 1(mod\ 8)$, segue que existe $m \in \mathbb{Z}$ tal que $d - 1 = 8m$ e, logo, $\frac{d-1}{4} = 2m$. Assim,

$$\begin{aligned} \omega_1^2 &= \left(\tfrac{1+\theta^2}{2}\right)^2 = \tfrac{1+2\theta^2+\theta^4}{4} = \tfrac{1+2\theta^2+d}{4} = \tfrac{2+2\theta^2}{4} + \tfrac{d-1}{4} = \tfrac{1+\theta^2}{2} + 2m \\ &= \omega_1 + 2m \quad \equiv \quad \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Efetuando essas substituições na Equação (3.7), obtemos

$$\alpha^2 - \beta^2\theta^2 = a_0 + a_1\omega_1 - b_0 - b_1\omega_1 \equiv 0 \ (mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Como $\{1, \omega_1\}$ é base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e os coeficientes da combinação linear acima são inteiros, segue que

$$\begin{cases} (a_0 - b_0) \equiv 0 \ (mod\ 2) \\ (a_1 - b_1) \equiv 0 \ (mod\ 2). \end{cases}$$

Assim,

$$\begin{cases} a_0 \equiv b_0 \ (mod\ 2) \\ a_1 \equiv b_1 \ (mod\ 2) \\ a_0^2 \equiv b_0^2 \ (mod\ 4) \\ a_1^2 \equiv b_1^2 \ (mod\ 4) \\ 2b_0b_1 \equiv 2a_0a_1 (mod\ 4). \end{cases} \tag{3.8}$$

Substituindo esses valores na Equação (3.6), segue que

$$\alpha^2 - \beta^2\theta^2 = a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1 - (a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1)\theta^2 \equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}).$$

Colocando $1 - \theta^2$ em evidência, obtemos

$$\alpha^2 - \beta^2\theta^2 = (1 - \theta^2)(a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1) \equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}).$$

Mas $1 - \theta^2 = 1 - 2\theta^2 + \theta^2 = 2\omega_1 - 2\theta^2$, donde segue que

$$\alpha^2 - \beta^2\theta^2 = 2(\omega_1 - \theta^2)(a_0^2 + a_1^2\omega_1^2 + 2a_0a_1\omega_1) \equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}).$$

Aplicando o fato que $2x \equiv 0 \ (mod\ 4) \Rightarrow x \equiv 0 \ (mod\ 2)$, obtemos

$$\alpha^2 - \beta^2\theta^2 = (\omega_1 - \theta^2)(a_0^2 + a_1^2\omega_1^2) \equiv 0 \ (mod\ 2\mathcal{O}_{\mathbb{K}})$$

Agora, fazendo uso novamente das congruências $\omega_1^2 \equiv \omega_1 (mod\ 2\mathcal{O}_{\mathbb{K}}), \theta^2 \equiv 1 (mod\ 2\mathcal{O}_{\mathbb{K}})$ e $x^2 \equiv x (mod\ 2)$, para todo $x \in \mathbb{Z}$, segue que

$$\alpha^2 - \beta^2\theta^2 = a_0\omega_1 - a_0 \equiv 0 \ (mod\ 2\mathcal{O}_{\mathbb{K}}). \tag{3.9}$$

Vale ressaltar que a diferença entre os valores da congruência módulo $2\mathcal{O}_{\mathbb{K}}$ de ω_1^2 entre esse caso e o expresso no item 2, é o que vai resultar na obtenção de uma base diferente para $\mathcal{O}_{\mathbb{L}}$, ainda que ambas provenham da mesma base

de $\mathcal{O}_{\mathbb{K}}$. Desse modo, na Equação (3.9), obtemos novamente uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$, donde segue que $a_0 \equiv 0(mod\ 2)$ e, substituindo essa congruência no Sistema (3.8), segue que $b_0 \equiv 0(mod\ 2)$. Sobre a_1 e b_1, a única conclusão que podemos tirar é que ambos possuem a mesma paridade, conforme o Sistema (3.8). Assim, analisaremos as duas possibilidades: a_1 e b_1 ambos pares e a_1 e b_1 ambos ímpares. Na primeira situação, teríamos

$$\begin{cases} a_0 = 2a_0' \\ a_1 = 2a_1' \\ b_0 = 2b_0' \\ b_1 = 2b_1', \end{cases}$$

onde $a_0', a_1', b_0', b_1' \in \mathbb{Z}$. Assim,

$$\begin{aligned} \eta &= \tfrac{\alpha}{2} + \tfrac{\beta}{2}\theta = \tfrac{a_0+a_1\omega_1}{2} + \tfrac{(b_0+b_1\omega_1)\theta}{2} = \tfrac{2a_0'+2a_1'\omega_1}{2} + \tfrac{(2b_0'+2b_1'\omega_1)\theta}{2} \\ &= a_0' + a_1'\omega_1 + (b_0' + b_1\omega_1)\theta = a_0' + b_0'\theta + a_1'\omega_1 + b_1'\omega_1\theta, \end{aligned}$$

ou seja, $\eta \in \mathbb{Z}[1, \theta, \omega_1, \omega_1\theta]$, que recai no caso anterior, onde $d \equiv 1(mod\ 4)$. No segundo caso, a_1 e b_1 ambos ímpares, podemos escrever

$$\begin{cases} a_0 = 2a_0' \\ a_1 = 2a_1' + 1 \\ b_0 = 2b_0' \\ b_1 = 2b_1' + 1 \end{cases}$$

onde $a_0', a_1', b_0', b_1' \in \mathbb{Z}$. Assim,

$$\begin{aligned} \eta &= \tfrac{\alpha}{2} + \tfrac{\beta}{2}\theta = \tfrac{a_0+a_1\omega_1}{2} + \tfrac{(b_0+b_1\omega_1)\theta}{2} = \tfrac{2a_0'+(2a_1'+1)\omega_1}{2} + \tfrac{(2b_0'+(2b_1'+1)\omega_1)\theta}{2} \\ &= a_0' + a_1'\omega_1 + b_0'\theta + b_1'\omega_1\theta + \tfrac{(1+\theta)}{2}\omega_1. \end{aligned}$$

Como $\omega_2 = \frac{(1+\theta)}{2}\omega_1$, segue que $\eta \in \mathbb{Z}[1, \theta, \omega_1, \omega_1\theta, \omega_2]$. Mas $\omega_1\theta = 2\omega_2 - \omega_1$, de modo que $\eta \in \mathbb{Z}[1, \theta, \omega_1, \omega_2]$, donde segue a inclusão $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[1, \theta, \omega_1, \omega_2]$.

b) $\mathbb{Z}[1, \theta, \omega_1, \omega_2] \subset \mathcal{O}_{\mathbb{L}}$. Já é de nosso conhecimento que os elementos θ e ω_1 são inteiros em $\mathbb{L}$, de modo que só resta mostrar que ω_2 também é inteiro para chegarmos à conclusão final. Para isso, mostraremos que a norma e o traço de ω_2 estão em $\mathcal{O}_{\mathbb{K}}$, de acordo com a Proposição 1.7, pois o grau da extensão $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$ é 2 e, consequentemente, o polinômio minimal possui apenas esses 2 fatores.

I) $\mathrm{Tr}(\omega_2) = \omega_2 + \sigma_4(\omega_2) = \omega_1\left(\frac{1+\theta}{2}\right) + \omega_1\left(\frac{1-\theta}{2}\right) = \omega_1\left(\frac{1+\theta}{2} + \frac{1-\theta}{2}\right) = \omega_1 \in \mathcal{O}_{\mathbb{K}}$.

II) $\mathrm{N}(\omega_2) = \omega_2.\sigma_4(\omega_2) = \omega_1\left(\frac{1+\theta}{2}\right).\omega_1\left(\frac{1-\theta}{2}\right) = \frac{1}{2}\omega_1\left(\frac{1-\theta^2}{2}\right) = \frac{1}{2}\omega_1(-\omega_1+1) = k\omega_1 \in \mathcal{O}_{\mathbb{K}}$, pois

$$\omega_1(-\omega_1+1) = \frac{1+\theta^2}{2}\frac{1-\theta^2}{2} = \frac{1-\theta^4}{4} = \frac{1-d}{4} = -2k,$$

já que $d \equiv 1(mod\ 8)$ implica que $\frac{d-1}{4} = 2k$.

Desse fato, segue a inclusão $\mathbb{Z}[1, \theta, \omega_1, \omega_2] \subset \mathcal{O}_{\mathbb{L}}$.

Portanto, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \omega_1, \omega_2]$.

A partir dos itens 1, 2 e 3, finalizamos a prova do teorema. □

3.1.2 Discriminante

Uma vez que determinamos uma base integral de um corpo, o próximo passo é calcular o seu discriminante, cujas aplicações incluem o cálculo da densidade de centro de um reticulado algébrico, fato que confere grande relevância ao conhecimento desse valor. Cada corpo de números está associado a um único valor correspondente ao discriminante, visto que duas bases equivalentes de um mesmo corpo fornecem discriminantes iguais. Sendo assim, como para o corpo $\mathbb{Q}(\sqrt[4]{d})$ existem 3 possibilidades de estruturas do anel de inteiros algébricos (a depender do valor de d), também haverá 3 possibilidades de discriminantes diferentes, como segue no próximo teorema, onde consideramos $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números com $\theta = \sqrt[4]{d}$ e $d \neq 1$ um inteiro livre de quadrados.

Teorema 3.2. *O discriminante do anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ de $\mathbb{L}$ é dado por*

$$D(\mathbb{L}) = \begin{cases} -256d^3, \text{ se } d \not\equiv 1(mod\ 4) \\ -16d^3, \text{ se } d \equiv 5(mod\ 8) \\ -4d^3, \text{ se } d \equiv 1(mod\ 8). \end{cases}$$

Demonstração. Pela Proposição 2.4, segue que $D(\mathbb{L}) = -n^n d^{n-1}$, para $d \not\equiv 1(mod\ 4)$. Substituindo $n = 4$ na expressão, obtemos diretamente que $D(\mathbb{L}) = -256d^3$, se $d \not\equiv 1(mod\ 4)$. Para os demais casos, calculamos o discriminante do anel de inteiros algébricos através da Definição 1.32. Se $d \equiv 5(mod\ 8)$ segue pelo Teorema 3.1 que $\mathcal{O}_{\mathbb{L}} = \langle 1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2} \rangle$. Asssim, pela Definição 1.32 e sabendo que $d = \theta^4$, segue que o discriminante $D_{\mathbb{L}}\left(1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}\right)$ é dado por

$$D_{\mathbb{L}}\left(1,\theta,\frac{1+\theta^2}{2},\frac{\theta+\theta^3}{2}\right)=\det\begin{bmatrix} Tr(1) & Tr(\theta) & Tr\left(\frac{1+\theta^2}{2}\right) & Tr\left(\frac{\theta+\theta^3}{2}\right)\\ Tr(\theta) & Tr(\theta^2) & Tr\left(\frac{\theta+\theta^3}{2}\right) & Tr\left(\frac{\theta^2+d}{2}\right)\\ Tr\left(\frac{1+\theta^2}{2}\right) & Tr\left(\frac{\theta+\theta^3}{2}\right) & Tr\left(\frac{d+2\theta^2+1}{4}\right) & Tr\left(\frac{\theta+2\theta^3+\theta^5}{4}\right)\\ Tr\left(\frac{\theta+\theta^3}{2}\right) & Tr\left(\frac{\theta^2+d}{2}\right) & Tr\left(\frac{\theta+2\theta^3+\theta^5}{4}\right) & Tr\left(\frac{\theta^2+\theta^3+d+\theta^5}{4}\right)\end{bmatrix}.$$

Uilizando a Proposição 1.37 para calcular os traços que compõem as entradas da matriz, segue que

$$\begin{aligned} D_{\mathbb{L}}\left(1,\theta,\tfrac{1+\theta^2}{2},\tfrac{\theta+\theta^3}{2}\right) &= \det\begin{bmatrix} 4 & 0 & 2 & 0\\ 0 & 0 & 0 & 2d\\ 2 & 0 & d+1 & 0\\ 0 & 2d & 0 & d\end{bmatrix}\\ &= (-1)^{2+4}2d\det\begin{bmatrix} 4 & 0 & 2\\ 2 & 0 & d+1\\ 0 & 2d & 0\end{bmatrix}=-16d^3. \end{aligned}$$

Agora, se $d\equiv 1(mod\ 8)$, segue pelo Teorema 3.1 que $\mathcal{O}_{\mathbb{L}}=\langle 1,\theta,\frac{1+\theta^2}{2},\frac{1+\theta+\theta^2+\theta^3}{4}\rangle$ e, desse modo, pela Definição 1.32 segue que $D(\mathbb{L})=D_{\mathbb{L}}\left(1,\theta,\frac{1+\theta^2}{2},\frac{1+\theta+\theta^2+\theta^3}{4}\right)$ é expresso por

$$D(\mathbb{L})=\det\begin{bmatrix} Tr(1) & Tr(\theta) & Tr\left(\frac{1+\theta^2}{2}\right) & Tr\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right)\\ Tr(\theta) & Tr(\theta^2) & Tr\left(\frac{\theta+\theta^3}{2}\right) & Tr\left(\frac{\theta+\theta^2+\theta^3+d}{4}\right)\\ Tr\left(\frac{1+\theta^2}{2}\right) & Tr\left(\frac{\theta+\theta^3}{2}\right) & Tr\left(\frac{1+2\theta^2+d}{4}\right) & Tr\left(\frac{1+\theta+2\theta^2+2\theta^3+d+\theta^5}{8}\right)\\ Tr\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right) & Tr\left(\frac{\theta+\theta^2+\theta^3+d}{4}\right) & Tr\left(\frac{1+\theta+2\theta^2+2\theta^3+d+\theta^5}{8}\right) & Tr\left(\frac{1+2\theta+3\theta^2+3\theta^3+3d+2\theta^5+\theta^6}{16}\right)\end{bmatrix}.$$

Calculando os valores dos traços com o auxílio do Lema 1.37, segue que

$$\begin{aligned} D_{\mathbb{L}}\left(1,\theta,\tfrac{1+\theta^2}{2},\tfrac{1+\theta+\theta^2+\theta^3}{4}\right) &= \det\begin{bmatrix} 4 & 0 & 2 & 1\\ 0 & 0 & 0 & d\\ 2 & 0 & d+1 & \frac{1+d}{2}\\ 1 & d & \frac{1+d}{2} & \frac{1+3d}{4}\end{bmatrix}\\ &= (-1)^{2+4}d\begin{bmatrix} 4 & 0 & 2\\ 2 & 0 & d+1\\ 1 & d & \frac{1+d}{2}\end{bmatrix}=-4d^3, \end{aligned}$$

o que prova o teorema. □

3.2 Base integral e discriminante do corpo puro de grau 8

Em [10], Hameed determina as bases integrais e seus respectivos discriminantes para os corpos puros de grau 8 do tipo $\mathbb{L} = \mathbb{Q}(\sqrt[8]{d})$ cujo polinômio minimal é $p(x) = x^8 - d$ e $d \neq 1$ é inteiro livre de quadrados. Nesta seção, nós apresentaremos uma prova sutilmente diferente da feita em [10], mas utilizando da mesma ideia, cujo raciocínio é análogo ao que foi feito na seção anterior.

3.2.1 Anel de inteiros algébricos

Para o corpo $\mathbb{Q}(\sqrt{d})$, com $d \neq 1$ inteiro e livre de quadrados, sabemos que há 2 estruturas distintas para suas bases integrais, as quais variam conforme o valor de d e, pelo Teorema 3.1, constatamos que para o corpo $\mathbb{Q}(\sqrt[4]{d})$, esse número aumenta para 3 casos diferentes. Agora, no próximo teorema, iremos descrever o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[8]{d})$, o qual possui 4 estruturas distintas conforme o valor de d.

Teorema 3.3. *Seja $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[8]{d}$ com $d \neq 1$ um inteiro e livre de quadrados. Uma base integral de $\mathbb{L}$ é dada por*

1. $\{1, \theta, \theta^2, \ldots, \theta^7\}$, *se* $d \equiv 2, 3 (mod\ 4)$
2. $\{1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3\}$, *se* $d \equiv 5 (mod\ 8)$
3. $\{1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_2\theta\}$, *se* $d \equiv 9 (mod\ 16)$
4. $\{1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_3\}$, *se* $d \equiv 1 (mod\ 16)$,

onde $\omega_1 = \frac{1+\theta^4}{2}, \omega_2 = \frac{1+\theta^2+\theta^4+\theta^6}{4}$ *e* $\omega_3 = \frac{1+\theta+\theta^2+\theta^3+\theta^4+\theta^5+\theta^6+\theta^7}{8}$.

Demonstração. Faremos a prova para cada caso separadamente. Sendo $\mathbb{L} = \mathbb{Q}(\theta)$, consideramos $\mathbb{K} = \mathbb{Q}(\theta^2) = \mathbb{Q}(\sqrt[4]{d})$.

1. O primeiro caso, $d \equiv 2, 3 (mod\ 4)$, é uma consequência direta do Teorema 2.3.

2. Agora, para $d \equiv 5 (mod\ 8)$, vamos utilizar a base obtida na Seção 3.1. Pelo Teorema 3.1, segue que $\{1, \theta^2, \frac{1+\theta^4}{2}, \frac{1+\theta^4}{2}\theta^2\}$ é uma base integral de $\mathbb{Q}(\sqrt[4]{d}) = \mathbb{Q}(\theta^2)$. Além disso, como $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_1\theta + \mathbb{Z}\omega_1\theta^2 + \mathbb{Z}\omega_1\theta^3 = \mathcal{O}_{\mathbb{K}}[\theta]$, a prova se resume em mostrar que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$.

   a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Neste caso, seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Assim, uma vez que $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que existem $\alpha', \beta' \in \mathbb{K}$ tal que $\eta = \alpha' + \beta'\theta$. Pela Proposição (1.39), segue que $2\alpha', 2\beta' \in \mathcal{O}_{\mathbb{K}}$, de modo que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$

tais que $\alpha' = \frac{\alpha}{2}$ e $\beta' = \frac{\beta}{2}$. Logo, $2\eta = \alpha + \beta\theta$. Tomando a norma de ambos os lados e usando as propriedades contidas na Proposição 1.2, segue que

$$N(2\eta) = N(\alpha+\beta\theta) \Rightarrow\ 4N(\eta) = \alpha^2-\beta^2\theta^2 \Rightarrow \alpha^2-\beta^2\theta^2 \equiv 0(mod\, 4\mathcal{O}_{\mathbb{K}}). \quad (3.10)$$

Como $\alpha,\ \beta \in \mathcal{O}_{\mathbb{K}}$ e $\{1, \theta^2, \omega_1, \omega_1\theta^2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Z}$ tais que $\alpha = a_0 + a_1\theta^2 + a_2\omega_1 + a_3\omega_1\theta^2$ e $\beta = b_0 + b_1\theta^2 + b_2\omega_1 + b_3\omega_1\theta^2$. Substituindo na Equação (3.10), segue que

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_1^2\theta^4 + 2a_0a_1\theta^2 + 2a_0a_2\omega_1 + 2a_0a_3\omega_1\theta^2 \\
&\quad +2a_1a_2\theta^2\omega_1 + 2a_1a_3\omega_1\theta^4 + 2a_2a_3\omega_1^2\theta^2 - (b_0^2 + b_1^2\theta^4 + b_2^2\omega_1^2 \\
&\quad +b_3^2\omega_1^2\theta^4 + 2b_0b_1\theta^2 + 2b_0b_2\omega_1 + 2b_0b_3\omega_1\theta^2 \\
&\quad +2b_1b_2\theta^2\omega_1 + 2b_1b_3\omega_1\theta^4 + 2b_2b_3\omega_1^2\theta^2)\theta^2 \\
&\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned} \quad (3.11)$$

Se considerarmos a congruência módulo 2 ao invés da congruência módulo 4, podemos reescrever a Equação (3.11) como

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_1^2\theta^4 - (b_0^2 + b_1^2\theta^4 + b_2^2\omega_1^2 + b_3^2\omega_1^2\theta^4)\theta^2 \\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned} \quad (3.12)$$

Nesse corpo, são válidas as congruências

$$\begin{cases} \theta^4 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_1^2 \equiv \omega_1 + 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ x^2 \equiv x(mod\ 2), \end{cases}$$

para todo $x \in \mathbb{Z}$. De fato, de $\omega_1 = \frac{1+\theta^4}{2}$, segue que $\theta^4 = 2\omega_1 - 1 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e também,

$$\omega_1^2 = \left(\frac{1+\theta^4}{2}\right)^2 = \frac{1+2\theta^4+\theta^8}{4} = \frac{2+2\theta^4}{4} + \frac{d-1}{4} = \omega_1 + m \equiv \omega_1 + 1(mod\ 2\mathcal{O}_{\mathbb{K}}),$$

onde m é tal que, como $d \equiv 1(mod\ 4)$ e 4 é a maior potência de 2 que divide $d-1$, existe $m \in \mathbb{Z}$ ímpar tal que $d - 1 = 4m$. Substituindo-as na Equação (3.12), segue que

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &\equiv a_0 + a_1 + a_2\omega_1 + a_2 + a_3\omega_1 + a_3 \\ &\quad -(b_0 + b_1 + b_2\omega_1 + b_2 + b_3\omega_1 + b_3)\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Reagrupando, segue que

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= (a_0 + a_1 + a_2 + a_3) + (a_2 + a_3)\omega_1 + (-b_0 - b_1 - b_2 - b_3)\theta^2 \\ &\quad +(-b_2 - b_3)\omega_1\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})\end{aligned}.$$

Como $\{1, \theta^2, \omega_1, \omega_1\theta^2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $a_i, b_i \in \mathbb{Z}$, segue que os coeficientes que multiplicam os elementos da base devem ser congruentes a 0 módulo 2, ou seja, devemos ter

$$\begin{cases} a_0 + a_1 + a_2 + a_3 \equiv 0\ (mod\ 2) \\ a_2 + a_3 \equiv 0\ (mod\ 2) \\ -b_0 - b_1 - b_2 - b_3 \equiv 0(mod\ 2) \\ -b_2 - b_3 \equiv 0\ (mod\ 2). \end{cases}$$

E dessas congruências obtemos as seguintes relações

$$\begin{cases} a_0 \equiv -a_1\ (mod\ 2) \\ a_2 \equiv -a_3\ (mod\ 2) \\ b_0 \equiv -b_1\ (mod\ 2) \\ b_2 \equiv -b_3\ (mod\ 2). \end{cases} \tag{3.13}$$

Efetuando os produtos, as seguintes congruências módulo 4 são obtidas

$$\begin{cases} {a_0}^2 \equiv {a_1}^2\ (mod\ 4) \\ {a_2}^2 \equiv {a_3}^2\ (mod\ 4) \\ {b_0}^2 \equiv {b_1}^2(mod\ 4) \\ {b_2}^2 \equiv {b_3}^2\ (mod\ 4) \\ 2a_0a_1 \equiv 2(a_0)^2(mod\ 4) \\ 2a_0a_3 \equiv 2a_0a_2(mod\ 4) \\ 2a_1a_2 \equiv 2a_0a_2(mod\ 4) \end{cases} \quad \begin{cases} 2a_1a_3 \equiv 2a_0a_2(mod\ 4) \\ 2a_2a_3 \equiv 2(a_2)^2(mod\ 4) \\ 2b_0b_1 \equiv 2(b_0)^2(mod\ 4) \\ 2b_0b_3 \equiv 2b_0b_2(mod\ 4) \\ 2b_1b_2 \equiv 2b_0b_2(mod\ 4) \\ 2b_1b_3 \equiv 2b_0b_2(mod\ 4) \\ 2b_2b_3 \equiv 2(b_2)^2(mod\ 4). \end{cases} \tag{3.14}$$

Substituindo as congruências do Sistema (3.14) na Equação (3.11), segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= a_0^2+a_0^2\theta^4+a_2^2\omega_1^2+a_2^2\omega_1^2\theta^4-2a_0^2\theta^2+2a_0a_2\omega_1-2a_0a_2\omega_1\theta^2\\
&\quad -2a_0a_2\theta^2\omega_1+2a_0a_2\omega_1\theta^4-2a_2^2\omega_1^2\theta^2-(b_0^2+b_0^2\theta^4\\
&\quad +b_2^2\omega_1^2+b_2^2\omega_1^2\theta^4-2b_0^2\theta^2+2b_0b_2\omega_1-2b_0b_2\omega_1\theta^2-2b_0b_2\theta^2\omega_1\\
&\quad +2b_0b_2\omega_1\theta^4-2b_2^2\omega_1^2\theta^2)\theta^2\\
&= (1+\theta^4)(a_0^2+a_2^2\omega_1^2+2a_0a_2\omega_1)-2a_0^2\theta^2-2a_2^2\omega_1^2\theta^2\\
&\quad -[(1+\theta^4)(b_0^2+b_2^2\omega_1^2+2b_0b_2\omega_1)-2b_0^2\theta^2-2b_2^2\omega_1^2\theta^2]\theta^2\\
&\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Como $1+\theta^4=2\omega_1$, segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= 2\omega_1(a_0^2+a_2^2\omega_1^2+2a_0a_2\omega_1)-2a_0^2\theta^2-2a_2^2\omega_1^2\theta^2\\
&\quad -[2\omega_1(b_0^2+b_2^2\omega_1^2+2b_0b_2\omega_1)-2b_0^2\theta^2-2b_2^2\omega_1^2\theta^2]\theta^2\\
&\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Também, uma vez que $2x\equiv 0\ (mod\ 4)\Rightarrow x\equiv 0\ (mod\ 2)$, obtemos

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \omega_1(a_0^2+a_2^2\omega_1^2)-a_0^2\theta^2-a_2^2\omega_1^2\theta^2\\
&\quad -[\omega_1(b_0^2+b_2^2\omega_1^2)-b_0^2\theta^2-b_2^2\omega_1^2\theta^2]\theta^2\\
&\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Usando novamente as congruências $\theta^4\equiv 1\ (mod\ 2\mathcal{O}_{\mathbb{K}})$, $\theta^6\equiv\theta^2(mod\ 2\mathcal{O}_{\mathbb{K}})$, $\omega_1^2\equiv\omega_1+1(mod\ 2\mathcal{O}_{\mathbb{K}})$, $\omega_1^3\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e que $x^2\equiv x\ (mod\ 2)$, segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \omega_1a_0+a_2-a_0\theta^2-a_2\omega_1\theta^2-a_2\theta^2\\
&\quad -\omega_1b_0\theta^2-b_2\theta^2+b_0+b_2\omega_1+b_2\\
&= (a_2+b_0+b_2)+(-a_0-a_2-b_2)\theta^2+(a_0+b_2)\omega_1\\
&\quad +(-a_2-b_0)\omega_1\theta^2\\
&\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Como $\{1,\theta^2,\omega_1,\omega_1\theta^2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, os coeficientes dessa combinação linear devem congruentes a 0 módulo 2, fato que fornece as seguintes equações

$$\begin{cases} a_2 + b_0 + b_2 \equiv 0 \ (mod\ 2) \\ -a_0 - a_2 - b_2 \equiv 0 \ (mod\ 2) \\ a_0 + b_2 \equiv 0 \ (mod\ 2) \\ -a_2 - b_0 \equiv 0 \ (mod\ 2). \end{cases}$$

A única solução desse sistema é $a_0, a_2, b_0, b_2 \equiv 0(mod\ 2)$ e, substituindo-as no Sistema (3.14), segue que $a_1, a_3, b_1, b_3 \equiv 0(mod\ 2)$, ou seja, a_i, b_i são ambos pares, para todo $i = 0, 1, 2, 3$. Desse modo, $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$ e, consequentemente, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde concluímos que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como na Seção 3.1, essa inclusão verifica-se imediatamente do fato que θ e ω_1 são inteiros em $\mathbb{L}$, pois

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \omega_1, \omega_1\theta^2][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto,

$$\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \omega_1, \omega_1\theta^2][1, \theta].$$

3. Agora, utilizando raciocínio similar, provamos o caso em que $d \equiv 9(mod\ 16)$ ou, equivalentemente, $d \equiv 1(mod\ 8)$ e $d \not\equiv 1(mod\ 16)$. Neste caso, note que assim como no item 2, considerando uma base de $\mathcal{O}_{\mathbb{K}}$ correspondente a essa congruência, verifica-se a igualdade $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_1\theta + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_2\theta = \mathcal{O}_{\mathbb{K}}[\theta]$. Desse modo, é suficiente mostrar que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$.

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Neste caso, seguindo os mesmos passos utilizados anteriormente, tomando $\eta \in \mathcal{O}_{\mathbb{L}}$, existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ e $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Z}$ tais que $\alpha = a_0 + a_1\theta^2 + a_2\omega_1 + a_3\omega_2$ e $\beta = b_0 + b_1\theta^2 + b_2\omega_1 + b_3\omega_2$ e, assim,

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_2^2 + 2a_0a_1\theta^2 + 2a_0a_2\omega_1 + 2a_0a_3\omega_2 \\ &\quad +2a_1a_2\theta^2\omega + 2a_1a_3\omega_2\theta^2 + 2a_2a_3\omega_1\omega_2 - (b_0^2 + b_1^2\theta^4 + b_2^2\omega_1^2 \\ &\quad +b_3^2\omega_2^2 + 2b_0b_1\theta^2 + 2b_0b_2\omega_1 + 2b_0b_3\omega_2 + 2b_1b_2\theta^2\omega_1 \\ &\quad +2b_1b_3\omega_2\theta^2 + 2b_2b_3\omega_1\omega_2)\theta^2 \\ &\equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.15}$$

Reescrevendo utilizando a congruência módulo 2, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\omega^2 + a_3^2\omega_2^2 - (b_0^2 + b_1^2\theta^4 + b_2^2\omega^2 + b_3^2\omega_2^2)\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.16}$$

Ademais, as seguintes congruências são válidas nesse corpo

$$\begin{cases} \theta^4 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \theta^6 \equiv \theta^2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_1\theta^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2\theta^2 \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2^2 \equiv \omega_2 + \omega + 1 + \theta^2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ x^2 \equiv x(mod\ 2), \end{cases} \tag{3.17}$$

para todo $x \in \mathbb{Z}$. De fato, as congruências de θ^4 e θ^6 são imediatas da definição de ω_1 e, para as demais, como $d \equiv 1(mod\ 8)$ e 8 é a maior potência de 2 que divide $d-1$, existe $m \in \mathbb{Z}$ ímpar tal que $d-1 = 8m$, Assim,

I) Para ω_1, segue que

$$\omega_1^2 = \left(\frac{1+\theta^4}{2}\right)^2 = \frac{d-1}{4} + \omega_1 = 2m + \omega_1 = \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}).$$

$$\begin{aligned} \omega_1\theta^2 &= \left(\tfrac{1+\theta^4}{2}\right)\theta^2 = \tfrac{\theta^2+\theta^6}{2} = 2(\tfrac{1+\theta^2+\theta^4+\theta^6}{4}) - \tfrac{1+\theta^4}{2} \\ &= 2\omega_2 - \omega_1 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

II) Para ω_2, segue que

$$\begin{aligned} \omega_2^2 &= \omega_1^2\left(\tfrac{1+\theta^2}{2}\right)^2 = (\omega_1 + 2m)\left(\tfrac{1+2\theta^2+\theta^4}{4}\right) \\ &= \tfrac{1}{2}(\omega_1 + 2m)(\tfrac{\omega_1}{2} + \tfrac{\theta^2}{2}) = m(\omega_1 + \theta^2) + \tfrac{1}{2}(\omega_1^2 + \theta^2\omega_1) \\ &= m(\omega_1 + \theta^2) + \tfrac{1}{2}(\omega_1 + 2m + 2\omega_2 - \omega_1) \\ &= m(\omega_1 + \theta^2 + 1) + \omega_2 \\ &\equiv \omega_1 + \theta^2 + 1 + \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \end{aligned}$$

e

$$\begin{aligned} \omega_2\theta^2 &= \left(\tfrac{1+\theta^2+\theta^4+\theta^6}{4}\right)\theta^2 = \tfrac{\theta^2+\theta^4+\theta^6+\theta^8}{4} = \tfrac{1+\theta^2+\theta^4+\theta^6}{4} + \tfrac{\theta^8-1}{4} \\ &= \tfrac{1+\theta^2+\theta^4+\theta^6}{4} + \tfrac{d-1}{4} = \omega_2 + 2m \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Substituindo-as na Equação (3.16), segue que

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= (a_0 + a_1 + a_3 - b_3) + (a_2 + a_3 - b_2 - b_3)\omega_1 \\ &\quad +(a_3 - b_0 - b_1 - b_3)\theta^2 + (a_3 - b_3)\omega_2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $\{1, \theta^2, \omega, \omega_2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $a_i, b_i \in \mathbb{Z}$, segue que os coeficientes devem ser congruentes a 0 módulo 2, donde seguem as congruências

$$\begin{cases} a_0 + a_1 + a_3 - b_3 \equiv 0\ (mod\ 2) \\ a_2 + a_3 - b_2 - b_3 \equiv 0\ (mod\ 2) \\ a_3 - b_0 - b_1 - b_3 \equiv 0(mod\ 2) \\ a_3 - b_3 \equiv 0\ (mod\ 2). \end{cases}$$

Essas congruências fornecem as seguintes relações

$$\begin{cases} a_0 \equiv -a_1\ (mod\ 2) \\ a_2 \equiv b_2\ (mod\ 2) \\ b_0 \equiv -b_1\ (mod\ 2) \\ a_3 \equiv b_3\ (mod\ 2). \end{cases} \tag{3.18}$$

Assim, efetuando os produtos, obtemos

$$\begin{cases} {a_0}^2 \equiv {a_1}^2\ (mod\ 4) \\ {a_2}^2 \equiv {b_2}^2\ (mod\ 4) \\ {b_0}^2 \equiv {b_1}^2(mod\ 4) \\ {a_3}^2 \equiv {b_3}^2\ (mod\ 4) \\ 2a_0a_1 \equiv 2(a_0)^2(mod\ 4) \\ 2a_0a_3 \equiv 2a_0a_3(mod\ 4) \\ 2a_1a_2 \equiv 2a_0a_2(mod\ 4) \end{cases} \quad \begin{cases} 2a_1a_3 \equiv 2a_0a_3(mod\ 4) \\ 2a_2a_3 \equiv 2a_2a_3(mod\ 4) \\ 2b_0b_1 \equiv 2(b_0)^2(mod\ 4) \\ 2b_0b_3 \equiv 2b_0a_3(mod\ 4) \\ 2b_1b_2 \equiv 2b_0a_2(mod\ 4) \\ 2b_1b_3 \equiv 2b_0a_3(mod\ 4) \\ 2b_2b_3 \equiv 2a_2a_3(mod\ 4). \end{cases} \tag{3.19}$$

Substituindo as congruências do Sistema (3.19) na Equação (3.15), segue que

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= a_0^2 + a_0^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_2^2 - 2a_0^2\theta^2 + 2a_0a_2\omega_1 + 2a_0a_3\omega_2 \\ &\quad -2a_0a_2\theta^2\omega_1 - 2a_0a_3\omega_2\theta^2 + 2a_2a_3\omega_1\omega_2 - (b_0^2 + b_0^2\theta^4 + a_2^2\omega_1^2 \\ &\quad +a_3^2\omega_2^2 - 2b_0^2\theta^2 + 2b_0a_2\omega_1 + 2b_0a_3\omega_2 - 2b_0a_2\theta^2\omega_1 \\ &\quad -2b_0a_3\omega_2\theta^2 + 2a_2a_3\omega_1\omega_2)\theta^2 \\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Agrupando os termos semelhantes, obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= a_0^2(1+\theta^4)+a_2^2\omega_1^2(1+\theta^2)+a_3^2\omega_2^2(1+\theta^2)-2a_0^2\theta^2\\ &\quad -2a_0a_2\omega_1-2a_0a_3\omega_2+2a_0a_2\theta^2\omega_1+2a_0a_3\omega_2\theta^2\\ &\quad +2a_2a_3\omega_1\omega_2-(b_0^2(1+\theta^4)-2b_0^2\theta^2+2b_0a_2\omega_1 \qquad (3.20)\\ &\quad +2b_0a_3\omega_2-2b_0a_2\theta^2\omega_1-2b_0a_3\omega_2\theta^2+2a_2a_3\omega_1\omega_2)\theta^2\\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Usando as igualdades,

$$\begin{cases}1+\theta^4=2\omega_1\\ \omega_1^2(1+\theta^2)=2(m+m\theta^2+\omega_2)\\ \omega_2^2(1+\theta^2)=2(m+m\theta^2+\omega_1+\omega_2+m\omega_2),\end{cases}$$

onde $m\equiv 1(mod\ 2)$ e as quais são facilmente verificadas substituindo os valores correspondentes a ω_1 e ω_2, todas as parcelas da Equação (3.20) estariam multiplicadas por 2, de modo que podemos reduzir a congruência para módulo 2, uma vez que $2x\equiv 0\ (\text{mod } 4)\Rightarrow x\equiv 0\ (\text{mod } 2)$. Após reduzir a congruência, podemos usar novamente as congruências válidas módulo 2 expressas no Sistema (3.17): $x^2\equiv x(mod\ 2)$, para todo $x\in\mathbb{Z}$, $m\equiv 1(mod\ 2)$, $\omega_1\theta^2\equiv\omega_1$, $\omega_2\theta^2\equiv\omega_2$, $\omega_1\omega_2\theta^2\equiv\omega_1\omega_2$ e $\theta^4\equiv 1$, de onde segue a expressão

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= a_0\omega_1+a_2(1+\theta^2+\omega_2)+a_3(1+\theta^2+\omega_1)-a_0\theta^2-b_0\omega_1+b_0\\ &= (a_2+a_3+b_0)+(a_2+a_3-a_0)\theta^2+(a_0+a_3-b_0)\omega_1+(a_2)\omega_2\\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $\{1,\theta^2,\omega_1,\omega_2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2. Logo,

$$\begin{cases}a_2+b_0+b_2\equiv 0\ (mod\ 2)\\ -a_0-a_2-b_2\equiv 0\ (mod\ 2)\\ a_0+b_2\equiv 0\ (mod\ 2)\\ -a_2-b_0\equiv 0\ (mod\ 2).\end{cases}$$

Como a única solução desse sistema é $a_0,a_2,b_0,b_2\equiv 0(mod\ 2)$, substituindo-as no Sistema (3.13), segue que $a_1,a_3,b_1,b_3\equiv 0(mod\ 2)$, ou seja, a_i,b_i são todos pares, para todo $i=0,1,2,3$. Logo, $\alpha',\beta'\in\mathcal{O}_{\mathbb{K}}$ e, portanto, $\eta\in\mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}}\subset\mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ, ω_1 e ω_2 são inteiros em $\mathbb{L}$, segue que

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \omega_1, \omega_2][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto,

$$\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \omega_1, \omega_2][1, \theta] = \mathbb{Z}[1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_2\theta].$$

4. Finalmente, provamos o caso $d \equiv 1(mod\ 16)$. Neste caso, assim como no item 3 da Seção 3.1, não é válido que $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_1\theta + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3\theta = \mathcal{O}_{\mathbb{K}}[\theta]$, de modo que precisamos mostrar que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_3]$.
   a) $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_3]$. Como $d \equiv 1(mod\ 16)$, segue que $d \equiv 1(mod\ 8)$ e, assim, tomando $\eta \in \mathcal{O}_{\mathbb{L}}$, existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ e $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Z}$ tais que $\alpha = a_0 + a_1\theta^2 + a_2\omega_1 + a_3\omega_2$ e $\beta = b_0 + b_1\theta^2 + b_2\omega_1 + b_3\omega_2$, exatamente como no item 3, ou seja, partimos da mesma base de $\mathcal{O}_{\mathbb{K}}$, visto que referente ao corpo $\mathbb{K}$ não há diferença entre as bases integrais quando d satisfaz uma dessas congruências. Logo,

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_2^2 + 2a_0a_1\theta^2 + 2a_0a_2\omega_1 + 2a_0a_3\omega_2 \\ &\quad + 2a_1a_2\theta^2\omega_1 + 2a_1a_3\omega_2\theta^2 + 2a_2a_3\omega_1\omega_2 - (b_0^2 + b_1^2\theta^4 + b_2^2\omega^2 \\ &\quad + b_3^2\omega_2^2 + 2b_0b_1\theta^2 + 2b_0b_2\omega_1 + 2b_0b_3\omega_2 + 2b_1b_2\theta^2\omega_1 + 2b_1b_3\omega_2\theta^2 \\ &\quad + 2b_2b_3\omega_1\omega_2)\theta^2 \\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.21}$$

Reduzindo para módulo 2, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_2^2 - (b_0^2 + b_1^2\theta^4 + b_2^2\omega_1^2 + b_3^2\omega_2^2)\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.22}$$

De modo análogo aos casos anteriores, prova-se que nesse corpo são válidas as congruências

$$\begin{cases} \theta^4 \equiv 1(mod\ 2) \\ \theta^6 \equiv \theta^2(mod\ 2) \\ \omega_1^2 \equiv \omega_1(mod\ 2) \\ \omega_1\theta^2 \equiv \omega_1(mod\ 2) \\ \omega_2\theta^2 \equiv \omega_2(mod\ 2) \\ \omega_2^2 \equiv \omega_2(mod\ 2) \\ x^2 \equiv x(mod\ 2), \end{cases}$$

para todo $x \in \mathbb{Z}$. Note que algumas congruências são diferentes das obtidas no caso anterior, item 3, e é a partir dessa diferença que vamos obter um novo anel de inteiros algébricos, embora tenhamos partido da mesma base em ambos os casos. Substituindo essas congruências na Equação (3.22), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0 + a_1 + a_2\omega_1 + a_3\omega_2 - (b_0\theta^2 + b_1\theta^2 + b_2\omega_1 + b_3\omega_2) \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Como $\{1, \theta^2, \omega_1, \omega_2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $a_i, b_i \in \mathbb{Z}$, segue que os coeficientes devem ser congruentes a 0 módulo 2, donde segue o sistema

$$\begin{cases} a_0 + a_1 \equiv 0\ (mod\ 2) \\ a_2 - b_2 \equiv 0\ (mod\ 2) \\ -b_0 - b_1 \equiv 0(mod\ 2) \\ a_3 - b_3 \equiv 0\ (mod\ 2). \end{cases}$$

E dessas relaçoes, obtemos as congruências

$$\begin{cases} a_0 \equiv -a_1\ (mod\ 2) \\ a_2 \equiv b_2\ (mod\ 2) \\ b_0 \equiv -b_1\ (mod\ 2) \\ a_3 \equiv b_3\ (mod\ 2). \end{cases} \tag{3.23}$$

Como essas congruências são as mesmas obtidas no Sistema (3.13), elas fornecem as mesmas congruências módulo 4 do Sistema (3.19). Substituindo-as na Equação (3.21), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_0^2\theta^4 + a_2^2\omega_1^2 + a_3^2\omega_2^2 - 2a_0^2\theta^2 + 2a_0a_2\omega_1 + 2a_0a_3\omega_2 \\ &\quad -2a_0a_2\theta^2\omega_1 - 2a_0a_3\omega_2\theta^2 + 2a_2a_3\omega_1\omega_2 - (b_0^2 + b_0^2\theta^4 + a_2^2\omega_1^2 \\ &\quad +a_3^2\omega_2^2 - 2b_0^2\theta^2 + 2b_0a_2\omega_1 + 2b_0a_3\omega_2 - 2b_0a_2\theta^2\omega_1 - 2b_0a_3\omega_2\theta^2 \\ &\quad +2a_2a_3\omega_1\omega_2)\theta^2 \\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Agrupando os termos semelhantes, obtemos

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= a_0^2(1+\theta^4) + (1-\theta^2)(a_2^2\omega_1^2 + a_3^2\omega_2^2) - 2a_0^2\theta^2 + 2a_0a_2\omega_1 \\ &\quad +2a_0a_3\omega_2 - 2a_0a_2\theta^2\omega_1 - 2a_0a_3\omega_2\theta^2 + 2a_2a_3\omega_1\omega_2 - (b_0^2(1+\theta^4) \\ &\quad -2b_0^2\theta^2 + 2b_0a_2\omega_1 + 2b_0a_3\omega_2 - 2b_0a_2\theta^2\omega_1 - 2b_0a_3\omega_2\theta^2 \\ &\quad +2a_2a_3\omega_1\omega_2)\theta^2 \\ &\equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned} \tag{3.24}$$

Usando as igualdades

$$\begin{cases} 1+\theta^4 = 2\omega_1 \\ (1-\theta^2)(a_2^2\omega_1^2 + a_3^3\omega_2^2) = 2(a_2^2\omega_1 - a_2^2\omega_2), \end{cases}$$

todas as parcelas da Equação (3.24) estariam multiplicadas por 2. Daí, reduzindo a congruência para módulo 2 e usando o fato que $x^2 \equiv x(mod\ 2)$ para todo $x \in \mathbb{Z}$, e, em seguida, que $\omega_1\theta^2 \equiv \omega_1$, $\omega_2\theta^2 \equiv \omega_2$, $\omega_1\omega_2\theta^2 \equiv \omega_1\omega_2$ e $\theta^4 \equiv 1$, segue a expressão

$$\alpha^2 - \beta^2\theta^2 = a_0\omega_1 + a_2\omega_1 - a_2\omega_2 - a_0\theta^2 - b_0\omega_1 + b_0 \equiv 0 \ (mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Como $\{1, \theta^2, \omega_1, \omega_2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2. Logo,

$$\begin{cases} b_0 \equiv 0 \ (mod\ 2) \\ -a_0 \equiv 0 \ (mod\ 2) \\ a_0 + a_2 - b_0 \equiv 0 \ (mod\ 2) \\ -a_2 \equiv 0 \ (mod\ 2). \end{cases}$$

Como a única solução desse sistema é $a_0, a_2, b_0 \equiv 0(mod\ 2)$, substituindo-as no Sistema (3.13), segue que $a_1, b_1, b_2 \equiv 0(mod\ 2)$. Deste modo, repetindo o raciocínio desenvolvido para o corpo quártico, vamos analisar a paridade de a_3 e b_3 que, de acordo com o Sistema (3.13), é a mesma. A seguir, analisamos os dois casos: ambos pares e ambos ímpares.

I) a_3 e b_3 são pares. Neste caso, significa que todos os inteiros a_i e b_i são pares, de modo que existem inteiros a_i' e b_i' tais que $a_i = 2a_i'$ e $b_i = 2b_i'$, para todo $0 \leq i \leq 3$. Logo,

$$\begin{aligned}\eta &= \frac{\alpha}{2}+\frac{\beta}{2}\theta = \frac{a_0+a_1\theta^2+a_2\omega_1+a_3\omega_1\theta^2}{2}+\frac{(b_0+b_1\theta^2+b_2\omega_1+b_3\omega_2)\theta}{2}\\ &= \frac{2a'_0+2a'_1\theta^2+2a'_2\omega_1+2a'_3\omega_2}{2}+\frac{(2b'_0+2b'_1\theta^2+2b'_2\omega_1+2b'_3\omega_2)\theta}{2}\\ &= a'_0+a'_1\theta^2+a'_2\omega_1+a'_3\omega_2+b'_0\theta+b'_1\theta^3+b'_2\omega_1\theta+b'_3\omega_2\theta.\end{aligned}$$

Assim, $\eta \in \langle 1,\theta,\theta^2,\theta^3,\omega_1,\omega_1\theta,\omega_2,\omega_2\theta\rangle$, ou seja, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, e recaímos no caso anterior.

II) a_3 e b_3 são ímpares. Neste caso, significa que existem inteiros a'_i e b'_i tais que $a_i = 2a'_i$ e $b_i = 2b'_i$, para $0 \leq i \leq 2$, $a_3 = 2a'_3+1$ e $b_3 = 2b'_3+1$. Logo,

$$\begin{aligned}\eta &= \frac{\alpha}{2}+\frac{\beta}{2}\theta = \frac{a_0+a_1\theta^2+a_2\omega_1+a_3\omega_2}{2}+\frac{(b_0+b_1\theta^2+b_2\omega_1+b_3\omega_2)\theta}{2}\\ &= \frac{2a'_0+2a'_1\theta^2+2a'_2\omega_1+(2a'_3+1)\omega_2}{2}\\ &\quad+\frac{(2b'_0+2b'_1\theta^2+2b'_2\omega_1+(2b'_3+1)\omega_2)\theta}{2}\\ &= a'_0+a'_1\theta^2+a'_2\omega_1+a'_3\omega_2+b'_0\theta+b'_1\theta^3+b'_2\omega_1\theta+b'_3\omega_2\theta+\tfrac{(1+\theta)}{2}\omega_2.\end{aligned}$$

Como $\frac{(1+\theta)}{2}\omega_2 = \omega_3$, segue que $\eta \in \langle 1,\theta,\theta^2,\theta^3,\omega_1,\omega_1\theta,\omega_2,\omega_2\theta,\omega_3\rangle$. Mas $\omega_2\theta = 2\omega_3-\omega_2$ e , portanto, $\eta \in \langle 1,\theta,\theta^2,\theta^3,\omega_1,\omega_1\theta,\omega_2,\omega_3\rangle$, de onde segue a inclusão $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[1,\theta,\theta^2,\theta^3,\omega_1,\omega_1\theta,\omega_2,\omega_3]$.

b) $\mathbb{Z}[1,\theta,\theta^2,\theta^3,\omega_1,\omega_1\theta,\omega_2,\omega_3] \subset \mathcal{O}_{\mathbb{L}}$. Sabemos que os elementos θ, ω_1 e ω_2 são inteiros em $\mathbb{L}$, de modo que só falta mostrar o mesmo para ω_3. Faremos isso provando que a norma e o traço de ω_3 estão em $\mathcal{O}_{\mathbb{K}}$.

$$\begin{aligned}\mathrm{Tr}(\omega_3) &= \omega_3+\sigma_4(\omega_3) = \omega_1\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}\right)+\omega_1\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1-\theta}{2}\right)\\ &= \omega_1\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}+\tfrac{1-\theta}{2}\right) = \omega_2 \in \mathcal{O}_{\mathbb{K}}.\end{aligned}$$

Além disso,

$$\begin{aligned}\mathrm{N}(\omega_3) &= \omega_3.\sigma_4(\omega_3) = \omega_1\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}\right).\omega_1\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1-\theta}{2}\right)\\ &= \tfrac{1}{4}\omega_2\omega_1\left(\tfrac{1-\theta^4}{2}\right) = \tfrac{1}{4}\omega_2\omega_1(-\omega_1+1) = m\omega_2 \in \mathcal{O}_{\mathbb{K}},\end{aligned}$$

em consequência de

$$\left(\frac{1+\theta^2}{2}\right)\left(\frac{1+\theta}{2}\right)\left(\frac{1-\theta}{2}\right) = \frac{1-\theta^4}{8} = \frac{1}{4}(1-\omega_1)$$

e

$$\omega_1(-\omega_1+1) = \frac{1+\theta^4}{2}\frac{1-\theta^4}{2} = \frac{1-\theta^8}{4} = \frac{1-d}{4} = -4m,$$

já que $d \equiv 1(mod\ 16)$ implica que $\frac{d-1}{4} = 4m$. Desse fato, segue que

$$\mathbb{Z}[1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_3] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \theta^2, \theta^3, \omega_1, \omega_1\theta, \omega_2, \omega_3]$.

Através dos itens 1, 2, 3 e 4, concluímos a prova do teorema. □

3.2.2 Discriminante

A partir do Teorema 3.3 concluímos que existem 4 possibilidades de estruturas diferentes do anel de inteiros algébricos para o corpo $\mathbb{Q}(\sqrt[8]{d})$, com $d \neq 1$ um inteiro livre de quadrados. Assim, no próximo teorema, o qual descreve o seu discriminante, também existirão 4 casos distintos, onde consideramos $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[8]{d}$ com $d \in \mathbb{Z}$ livre de quadrados.

Teorema 3.4. *O discriminante do anel de inteiros algébricos* $\mathcal{O}_{\mathbb{L}}$ *de* $\mathbb{L}$ *é dado por*

$$D(\mathbb{L}) = \begin{cases} -8^8 d^7, \text{ se } d \not\equiv 1(mod\ 4) \\ -2^{16} d^3, \text{ se } d \equiv 5(mod\ 8) \\ -2^{12} d^3, \text{ se } d \equiv 9(mod\ 16) \\ -2^{10} d^3, \text{ se } d \equiv 1(mod\ 16). \end{cases}$$

Demonstração. O primeiro caso, $d \not\equiv 1(mod\ 4)$, segue diretamente da Proposição 2.4, pois para $n = 8$ a expressão obtida de $D(\mathbb{L}) = -n^n d^{n-1}$ é $D(\mathbb{L}) = -8^8 d^7$. Para os demais casos, como essa base não é potente, precisamos calcular o discriminante do anel de inteiros algébricos através da Definição 1.32, do mesmo modo que fizemos na prova do Teorema 3.2. Se $d \equiv 5(mod\ 8)$, segue pelo Teorema 3.3 que

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[1, \theta, \theta^2, \theta^3, \frac{1+\theta^4}{2}, \frac{\theta+\theta^5}{2}, \frac{\theta^2+\theta^6}{2}, \frac{\theta^3+\theta^7}{2}\right]$$

e, assim, pela Definição 1.32, considerando $d = \theta^8$ e substituindo os valores dos traços que constam no Lema 1.37, segue que

$$
\begin{aligned}
D(\mathbb{L}) &= D_{\mathbb{L}}\left(1,\theta,\theta^2,\theta^3,\tfrac{1+\theta^4}{2},\tfrac{\theta+\theta^5}{2},\tfrac{\theta^2+\theta^6}{2},\tfrac{\theta^3+\theta^7}{2}\right)\\
&= \det\begin{bmatrix}
8 & 0 & 0 & 0 & 4 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 4d\\
0 & 0 & 0 & 0 & 0 & 0 & 4d & 0\\
0 & 0 & 0 & 0 & 0 & 4d & 0 & 0\\
4 & 0 & 0 & 0 & 2(d+1) & 0 & 0 & 0\\
0 & 0 & 0 & 4d & 0 & 0 & 0 & 4d\\
0 & 0 & 4d & 0 & 0 & 0 & 4d & 0\\
0 & 4d & 0 & 0 & 0 & 4d & 0 & 0
\end{bmatrix}\\
&= -(4d)^6.\det\begin{bmatrix} 8 & 4\\ 4 & 2(d+1)\end{bmatrix} = -2^{12}d^6 2^4 d = 2^{16}d^7.
\end{aligned}
$$

Agora, se $d \equiv 9(mod\ 16)$, pelo Teorema 3.1, segue que

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[1,\theta,\theta^2,\theta^3\frac{1+\theta^2}{2},\frac{\theta+\theta^5}{2},\frac{1+\theta^2+\theta^4+\theta^6}{4},\frac{\theta+\theta^3+\theta^5+\theta^7}{4}\right]$$

e, assim, pela Definição 1.32, segue que

$$
\begin{aligned}
D(\mathbb{L}) &= D_{\mathbb{L}}\left(1,\theta,\theta^2,\theta^3,\tfrac{1+\theta^4}{2},\tfrac{\theta+\theta^5}{2},\tfrac{1+\theta^2+\theta^4+\theta^6}{4},\tfrac{\theta+\theta^3+\theta^5+\theta^7}{4}\right)\\
&= \det\begin{bmatrix}
8 & 0 & 0 & 0 & 4 & 0 & 2 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2d\\
0 & 0 & 0 & 0 & 0 & 0 & 2d & 0\\
0 & 0 & 0 & 0 & 0 & 4d & 0 & 2d\\
4 & 0 & 0 & 0 & 2(d+1) & 0 & d+1 & 0\\
0 & 0 & 0 & 4d & 0 & 0 & 0 & d\\
0 & 0 & 2d & 0 & d+1 & 0 & 3d+1 & 0\\
0 & 2d & 0 & 2d & 0 & d & 0 & 2d
\end{bmatrix}\\
&= -(2d)^4(4d)^2.\det\begin{bmatrix} 8 & 4\\ 4 & 2(d+1)\end{bmatrix} = -2^8 d^6 2^4 d = 2^{12}d^7.
\end{aligned}
$$

Por último, se $d \equiv 1(mod\ 16)$, segue pelo Teorema 3.1 que

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[1,\theta,\theta^2,\theta^3,\frac{1+\theta^4}{2},\frac{\theta+\theta^5}{2},\frac{1+\theta^2+\theta^4+\theta^6}{4},\frac{1+\theta+\theta^2+\theta^3+\theta^4+\theta^5+\theta^6+\theta^7}{8}\right],$$

desse modo, usando novamente a Definição 1.32, segue que

$$
\begin{aligned}
D(\mathbb{L}) &= D_{\mathbb{L}}\left(1, \theta, \theta^2, \theta^3, \tfrac{1+\theta^4}{2}, \tfrac{\theta+\theta^5}{2}, \tfrac{1+\theta^2+\theta^4+\theta^6}{4}, \tfrac{1+\theta+\theta^2+\theta^3+\theta^4+\theta^5+\theta^6+\theta^7}{8}\right) \\
&= \det \begin{bmatrix}
8 & 0 & 0 & 0 & 4 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d \\
0 & 0 & 0 & 0 & 0 & 0 & 2d & d \\
0 & 0 & 0 & 0 & 0 & 4d & 0 & d \\
4 & 0 & 0 & 0 & 2(d+1) & 0 & d+1 & \frac{d+1}{2} \\
0 & 0 & 0 & 4d & 0 & 0 & 0 & d \\
0 & 0 & 2d & 0 & d+1 & 0 & \frac{1+3d}{2} & \frac{1+3d}{4} \\
0 & d & d & d & \frac{d+1}{2} & d & \frac{1+3d}{4} & \frac{1+7d}{8}
\end{bmatrix} \\
&= -d^2(2d)^2(4d)^2 \det \begin{bmatrix} 8 & 4 \\ 4 & 2(d+1) \end{bmatrix} = -2^6 d^6 2^4 d = -2^{10} d^7,
\end{aligned}
$$

o que prova o teorema. □

3.3 Base integral e discriminante do corpo puro de grau 16

Nas seções anteriores deste capítulo, apresentamos versões diferentes para resultados já demonstrados em outros trabalhos. Agora, nesta seção, apresentamos o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos do corpo puro de grau 16, resultado que até então não consta na literatura. No entanto, veremos que a construção dessa base representa uma extensão natural dos casos anteriores, e realizar a sua demonstração foi o impulso inicial para pensarmos a respeito de uma generalização envolvendo esse raciocínio.

3.3.1 Anel de inteiros algébricos

Pelo Teorema 3.3, conhecemos uma base integral do corpo $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[8]{d}$, com $d \neq 1$ um inteiro livre de quadrados. Porém, podemos escrever essa base de outra forma, a qual será mais conveniente para o nosso objetivo, utilizando $\theta = \sqrt[16]{d}$. Nesse caso, como $(\sqrt[16]{d})^2 = \sqrt[8]{d}$, uma base integral de $\mathbb{K}$ se apresenta como

1. $\{1, \theta^2, \theta^4, \theta^6, \theta^8, \theta^{10}, \theta^{12}, \theta^{14}\}$ se $d \equiv 2, 3 (mod\ 4)$
2. $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_1\theta^4, \omega_1\theta^6\}$, se $d \equiv 5 (mod\ 8)$
3. $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_2\theta^2, \}$, se $d \equiv 9 (mod\ 16)$

4. $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_3\}$, se $d \equiv 1(mod\ 16)$.

Esse fato será essencial para a demonstração do próximo teorema.

Teorema 3.5. *Seja* $\mathbb{L} = \mathbb{Q}(\theta)$, *onde* $\theta = \sqrt[16]{d}$, *com* $d \neq 1$ *um inteiro e livre de quadrados. Uma base do anel de inteiros algébricos de* $\mathbb{L}$, *denotado por* $\mathcal{O}_{\mathbb{L}}$, *é dada por*

1. $\{1, \theta, \theta^2, \ldots, \theta^{15}\}$ *se* $d \equiv 2, 3(mod\ 4)$

2. $\{1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^7\}$, *se* $d \equiv 5(mod\ 8)$

3. $\{1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_2\theta^2, \omega_2\theta^3\}$, *se* $d \equiv 9(mod\ 16)$

4. $\{1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_3\theta\}$, *se* $d \equiv 17(mod\ 32)$

5. $\{1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_4\}$, *se* $d \equiv 1(mod\ 32)$, *onde* $\omega_1 = \frac{1+\theta^8}{2}, \omega_2 = \frac{1+\theta^4+\theta^8+\theta^{12}}{4}$, $\omega_3 = \frac{1+\theta^2+\theta^4+\theta^6+\theta^8+\theta^{10}+\theta^{12}+\theta^{14}}{8}$ *e* $\omega_4 = \frac{1+\theta+\theta^2+\theta^3+\theta^4+\theta^5+\theta^6+\theta^7+\theta^8+\theta^9+\theta^{10}+\theta^{11}+\theta^{12}+\theta^{13}+\theta^{14}+\theta^{15}}{16}$.

Demonstração. Faremos a prova de cada item separadamente.

1. Para o caso $d \equiv 2, 3(mod\ 4)$, pelo Teorema 2.3, segue que

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\theta].$$

   Agora, pela forma que as bases integrais de $\mathbb{L}$ nos casos $d \equiv 5(mod\ 8), d \equiv 9(mod\ 16)$ e $d \equiv 17(mod\ 32)$ foram descritas acima, provar que esse conjunto é uma base de $\mathcal{O}_{\mathbb{L}}$, resume-se em provar que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$, onde $\mathbb{K} = \mathbb{Q}(\theta^2)$. Portanto, seguimos esse raciocínio para cada uma dessas congruências e, por fim, faremos a prova para o caso em que $d \equiv 1(mod\ 32)$, que se difere dos demais por não valer a igualdade $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$. No que segue, faremos a prova de cada um desses casos.

2. Seja $d \equiv 5(mod\ 8)$ ou, equivalentemente, $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$. Mostremos que

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \ldots, \omega_1\theta^7] = \mathcal{O}_{\mathbb{L}}[\theta].$$

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Uma vez que $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, existem $\alpha', \beta' \in \mathbb{K}$ tal que $\eta = \alpha' + \beta'\theta$. Pela Proposição (1.39), $2\alpha', 2\beta' \in \mathcal{O}_{\mathbb{K}}$, de modo que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tais que $\alpha' = \frac{\alpha}{2}$ e $\beta' = \frac{\beta}{2}$. Logo, $2\eta = \alpha + \beta\theta$. Tomando a norma de ambos os lados e usando as propriedades de norma contidas na Proposição 1.2, segue que

$$N(2\eta) = N(\alpha + \beta\theta) \Rightarrow\ 4N(\eta) = \alpha^2 - \beta^2\theta^2.$$

Assim,

$$\alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{3.25}$$

Como α, $\beta \in \mathcal{O}_{\mathbb{K}}$ e, pelo Teorema 3.3, $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_1\theta^4, \omega_1\theta^6\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7 \in \mathbb{Z}$ tais que

$$\begin{cases} \alpha = a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + a_4\omega_1 + a_5\omega_1\theta^2 + a_6\omega_1\theta^4 + a_7\omega_1\theta^6 \\ \beta = b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + b_4\omega_1 + b_5\omega_1\theta^2 + b_6\omega_1\theta^4 + b_7\omega_1\theta^6. \end{cases}$$

Substituindo esses valores na Equação (3.25), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\omega^2 + a_5^2\omega_1^2\theta^4 + a_6^2\omega_1^2\theta^8 + a_7^2\omega_1^2\theta^{12} \\ &\quad +2(a_0a_1\theta^2 + a_0a_2\theta^4 + a_0a_3\theta^6 + a_0a_4\omega_1 + a_0a_5\omega_1\theta^2 + a_0a_6\omega_1\theta^4 \\ &\quad +a_0a_7\omega_1\theta^6 + a_1a_2\theta^6 + a_1a_3\theta^8 + a_1a_4\omega_1\theta^2 + a_1a_5\omega_1\theta^4 + a_1a_6\omega_1\theta^6 \\ &\quad +a_1a_7\omega_1\theta^8 + a_2a_3\theta^{10} + a_2a_4\omega_1\theta^4 + a_2a_5\omega_1\theta^6 + a_2a_6\omega_1\theta^8 \\ &\quad +a_2a_7\omega_1\theta^{10} + a_3a_4\omega_1\theta^6 + a_3a_5\omega_1\theta^8 + a_3a_6\omega_1\theta^{10} + a_3a_7\omega_1\theta^{12} \\ &\quad +a_4a_5\omega_1^2\theta^2 + a_4a_6\omega_1^2\theta^4 + a_4a_7\omega_1^2\theta^6 + a_5a_6\omega_1^2\theta^6 + a_5a_7\omega_1^2\theta^8 \\ &\quad +a_6a_7\omega_1^2\theta^{10}) - (b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^12 + b_4^2\omega_1^2 + b_5^2\omega_1^2\theta^4 + b_6^2\omega_1^2\theta^8 \\ &\quad +b_7^2\omega_1^2\theta^12 + 2(b_0b_1\theta^2 + b_0b_2\theta^4 + b_0b_3\theta^6 + b_0b_4\omega + b_0b_5\omega\theta^2 + b_0b_6\omega_1\theta^4 \\ &\quad +b_0b_7\omega_1\theta^6 + b_1b_2\theta^6 + b_1b_3\theta^8 + b_1b_4\omega_1\theta^2 + b_1b_5\omega_1\theta^4 + b_1b_6\omega_1\theta^6 \\ &\quad +b_1b_7\omega_1\theta^8 + b_2b_3\theta^{10} + b_2b_4\omega_1\theta^4 + b_2b_5\omega_1\theta^6 + b_2b_6\omega_1\theta^8 + b_2b_7\omega_1\theta^{10} \\ &\quad +b_3b_4\omega_1\theta^6 + b_3b_5\omega_1\theta^8 + b_3b_6\omega_1\theta^{10} + b_3b_7\omega_1\theta^{12} + b_4b_5\omega_1^2\theta^2 + b_4b_6\omega_1^2\theta^4 \\ &\quad +b_4b_7\omega_1^2\theta^6 + b_5b_6\omega_1^2\theta^6 + b_5b_7\omega_1^2\theta^8 + b_6b_7\omega_1^2\theta^{10})\theta^2 \\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.26}$$

Reeescrevendo a Equação (3.25) partir da congruência módulo 2, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\omega_1^2 + a_5^2\omega_1^2\theta^4 + a_6^2\omega_1^2\theta^8 + a_7^2\omega_1^2\theta^{12} \\ &\quad -(b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^{12} + b_4^2\omega_1^2 + b_5^2\omega_1^2\theta^4 + b_6^2\omega_1^2\theta^8 \\ &\quad +b_7^2\omega_1^2\theta^{12})\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.27}$$

Em $\mathcal{O}_{\mathbb{K}}$, são válidas as congruências:

$$\begin{cases} \theta^8 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}), \\ \theta^{12} \equiv \theta^4(mod\ 2\mathcal{O}_{\mathbb{K}}), \\ \omega_1^2 \equiv \omega_1 + 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \text{ e} \\ x^2 \equiv x(mod\ 2), \end{cases}$$

para todo $x \in \mathbb{Z}$. De fato, de $\omega_1 = \frac{1+\theta^8}{2}$, vem a primeira congruência, pois, $\theta^8 = 2\omega_1 - 1$, e do mesmo fato também vem a segunda congruência, pois $\theta^{12} = 2\omega_1\theta^4 - \theta^4$, e $\omega_1\theta^4 \in \mathcal{O}_{\mathbb{K}}$. Para a terceira congruência, fazemos

$$\omega_1^2 = \left(\frac{1+\theta^8}{2}\right)^2 = \frac{1+2\theta^8+\theta^{16}}{4} = \frac{d-1}{4} + \frac{2+2\theta^8}{4} = \frac{d-1}{4} + \omega_1 = m + \omega_1,$$

pois $d \equiv 1(mod\ 4)$ e, logo, $\frac{d-1}{4} = m$. Além disso, m é ímpar, ou seja, $m \equiv 1(mod\ 2)$, pois caso contrário iria contradizer o fato que $d \not\equiv 1(mod\ 8)$. Logo, $\omega_1^2 \equiv \omega_1 + 1(mod\ 2\mathcal{O}_{\mathbb{K}})$. Substituindo esses valores na Equação (3.27), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0 + a_1\theta^4 + a_2 + a_3\theta^4 + a_4\omega + a_4 + a_5\omega\theta^4 + a_5\theta^4 + a_6\omega + a_6 \\ &\quad + a_7\omega\theta^4 + a_7\theta^4 - (b_0 + b_1\theta^4 + b_2 + b_3\theta^4 + b_4\omega_1 + b_4 + b_5\omega_1\theta^4 \\ &\quad + b_5\theta^4 + b_6\omega_1 + b_6 + b_7\omega_1\theta^4 + b_7\theta^4)\theta^2 \\ &= (a_0 + a_2 + a_4 + a_6) + (a_4 + a_6)\omega_1 + (a_1 + a_3 + a_5 + a_7)\theta^4 \\ &\quad + (a_5 + a_7)\omega_1\theta^4 + (-b_0 - b_2 - b_4 - b_6)\theta^2 + (-b_4 - b_6)\omega_1\theta^2 \\ &\quad + (b_1 + b_3 + b_5 + b_7)\theta^6 + (b_5 + b_7)\omega_1\theta^6 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Como $\{1, \theta^2, \theta^4, \theta^6\omega_1, \omega_1\theta^2, \omega_1\theta^4, \omega_1\theta^6\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $a_i, b_i \in \mathbb{Z}$, segue que $\{1, \theta^2, \theta^4, \theta^6\omega_1, \omega_1\theta^2, \omega_1\theta^4, \omega_1\theta^6\}$ é linearmente independente. Logo, os coeficientes devem ser congruentes a 0 módulo 2, donde seguem as congruências

$$\begin{cases} a_0 + a_2 + a_4 + a_6 \equiv 0\ (mod\ 2) \\ a_4 + a_6 \equiv 0\ (mod\ 2) \\ a_1 + a_3 + a_5 + a_7 \equiv 0\ (mod\ 2) \\ a_5 + a_7 \equiv 0\ (mod\ 2) \\ -b_0 - b_2 - b_4 - b_6 \equiv 0(mod\ 2) \\ -b_4 - b_6 \equiv 0\ (mod\ 2) \\ -b_1 - b_3 - b_5 - b_7 \equiv 0(mod\ 2) \\ -b_5 - b_7 \equiv 0\ (mod\ 2). \end{cases}$$

Essas congruências fornecem as seguintes relações

$$\begin{cases} a_0 \equiv -a_2 \ (mod\ 2) \\ a_1 \equiv -a_3 \ (mod\ 2) \\ a_4 \equiv -a_6 \ (mod\ 2) \\ a_5 \equiv -a_7 \ (mod\ 2) \\ b_0 \equiv -b_2 \ (mod\ 2) \\ b_1 \equiv -b_3 \ (mod\ 2) \\ b_4 \equiv -b_6 \ (mod\ 2) \\ b_5 \equiv -b_7 \ (mod\ 2). \end{cases} \tag{3.28}$$

Assim,

$$\begin{cases} {a_0}^2 \equiv {a_2}^2 \ (mod\ 4) \\ {a_1}^2 \equiv {a_3}^2 \ (mod\ 4) \\ {a_4}^2 \equiv {a_6}^2 \ (mod\ 4) \\ {a_5}^2 \equiv {a_7}^2 \ (mod\ 4) \\ {b_0}^2 \equiv {b_2}^2 (mod\ 4) \\ {b_1}^2 \equiv {b_3}^2 \ (mod\ 4) \\ {b_4}^2 \equiv {b_6}^2 (mod\ 4) \\ {b_5}^2 \equiv {b_7}^2 \ (mod\ 4) \end{cases} \quad \begin{cases} 2a_0a_2 \equiv -2(a_0)^2 (mod\ 4) \\ 2a_1a_3 \equiv -2(a_1)^2 (mod\ 4) \\ 2a_4a_6 \equiv -2(a_4)^2 (mod\ 4) \\ 2a_5a_7 \equiv -2(a_5)^2 (mod\ 4) \\ 2b_0b_2 \equiv -2(b_0)^2 (mod\ 4) \\ 2b_1b_3 \equiv -2(b_1)^2 (mod\ 4) \\ 2b_4b_6 \equiv -2(b_4)^2 (mod\ 4) \\ 2b_5b_7 \equiv -2(b_5)^2 (mod\ 4). \end{cases} \tag{3.29}$$

Observação 3.6. Por se tratar de uma demonstração similar à feita na Subseção 3.2.1, os demais valores dos produtos $2a_ia_j$ e $2b_ib_j$ já foram omitidos, uma vez que, utilizando o mesmo argumento, esses termos irão todos se anular, restando apenas os que estão descritos no sistema acima.

Substituindo as congruências contidas no Sistema (3.29) na Equação (3.26), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_0^2\theta^8 + a_1^2\theta^{12} + a_4^2\omega_1^2 + a_5^2\omega_1^2\theta^4 + a_4^2\omega_1^2\theta^8 + a_5^2\omega_1^2\theta^{12} \\ &\quad -2a_0^2\theta^4 - 2a_1^2\theta^8 - 2a_4^2\omega_1^2\theta^4 - 2a_5^2\omega_1^2\theta^8 - (b_0^2 + b_1^2\theta^4 + b_0^2\theta^8 + b_1^2\theta^{12} \\ &\quad +b_4^2\omega_1 a^2 + b_5^2\omega_1^2\theta^4 + b_4^2\omega_1^2\theta^8 + b_5^2\omega_1^2\theta^{12} - 2b_0^2\theta^4 - 2b_1^2\theta^8 - 2b_4^2\omega_1^2\theta^4 \\ &\quad -2b_5^2\omega_1^2\theta^8)\theta^2 \\ &\equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Note que alguns termos dessa soma estão multiplicados simultaneamente por 1 e por θ^8, de modo que podemos colocar $(1 + \theta^8)$ em evidência, donde obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= (1+\theta^8)(a_0^2+a_1^2\theta^4+a_4^2\omega_1^2+a_5^2\omega_1^2\theta^4)-2a_0^2\theta^4-2a_1^2\theta^8-2a_4^2\omega_1^2\theta^4\\ &\quad -2a_5^2\omega_1^2\theta^8-[(1+\theta^8)(b_0^2+b_1^2\theta^4+b_4^2\omega_1^2+b_5^2\omega_1^2\theta^4)-2b_0^2\theta^4-2b_1^2\theta^8\\ &\quad -2b_4^2\omega_1^2\theta^4-2b_5^2\omega_1^2\theta^8]\theta^2\\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $1+\theta^8=2\omega_1$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= 2a_0^2\omega_1+2a_1^2\omega_1\theta^4+2a_4^2\omega_1^3+2a_5^2\omega_1^3\theta^4-2a_0^2\theta^4-2a_1^2\theta^8-2a_4^2\omega_1^2\theta^4\\ &\quad -2a_5^2\omega_1^2\theta^8-[2b_0^2\omega_1+2b_1^2\omega_1\theta^4+2b_4^2\omega_1^3+2b_5^2\omega_1^3\theta^4-2b_0^2\theta^4-2b_1^2\theta^8\\ &\quad -2b_4^2\omega_1^2\theta^4-2b_5^2\omega_1^2\theta^8]\theta^2\\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Em razão de todos os termos estarem multiplicando por 2, podemos usar o fato que $2x\equiv 0\ (mod\ 4)\Rightarrow x\equiv 0\ (mod\ 2)$ e, em seguida, as congruências $\omega_1^2\equiv\omega_1+1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e $\omega_1^3\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$, donde segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= a_0^2\omega_1+a_1^2\omega_1\theta^4+a_4^2+a_5^2\theta^4-a_0^2\theta^4-a_1^2\theta^8-a_4^2\omega_1\theta^4-a_4^2\theta^4-a_5^2\omega_1\theta^8\\ &\quad -a_5^2\theta^8-[b_0^2\omega_1+b_1^2\omega_1\theta^4+b_4^2+b_5^2\theta^4-b_0^2\theta^4-b_1^2\theta^8-b_4^2\omega_1\theta^4-b_4^2\theta^4\\ &\quad -b_5^2\omega_1\theta^8-b_5^2\theta^8]\theta^2\\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Usando novamente que $\theta^8\equiv 1\ (mod\ 2)$ e que $x^2\equiv x\ (mod\ 2)$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= a_0\omega_1+a_1\omega_1\theta^4+a_4+a_5\theta^4-a_0\theta^4-a_1-a_4\omega_1\theta^4-a_4\theta^4-a_5\omega_1-a_5\\ &\quad -[b_0\omega_1+b_1\omega_1\theta^4+b_4+b_5\theta^4-b_0\theta^4-b_1-b_4\omega_1\theta^4-b_4\theta^4-b_5\omega-b_5]\theta^2\\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Mais uma vez obtemos uma combinação linear dos elementos da base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, donde segue que os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2, resultando no sistema abaixo.

$$\begin{cases} a_4 - a_1 - a_5 \equiv 0 \ (mod\ 2) \\ -b_4 + b_1 + b_5 \equiv 0 \ (mod\ 2) \\ a_5 - a_0 - a_4 \equiv 0 \ (mod\ 2) \\ -b_5 + b_0 + b_4 \equiv 0 \ (mod\ 2) \\ a_0 - a_5 \equiv 0 \ (mod\ 2) \\ -b_0 + b_5 \equiv 0 \ (mod\ 2) \\ a_1 - a_4 \equiv 0 \ (mod\ 2) \\ -b_1 + b_4 \equiv 0 \ (mod\ 2). \end{cases} \tag{3.30}$$

Como a única solução possível que satisfaça simultaneamente os Sistemas (3.30) e (3.28) é $a_i, b_i \equiv 0(mod\ 2)$, ou seja, todos pares, segue que $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$ e, portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ e ω_1 são inteiros em $\mathbb{L}$, é imediato que

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_1\theta^4, \omega_1\theta^6][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto, $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$.

3. Seja $d \equiv 9(mod\ 16)$ ou, equivalentemente, $d \equiv 1(mod\ 8)$ e $d \not\equiv 1(mod\ 16)$. Mostremos que

$$\mathcal{O}_{\mathbb{L}} = \{1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_2\theta^2, \omega_2\theta^3\} = \mathcal{O}_{\mathbb{K}}[\theta].$$

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Neste caso, o raciocínio é análogo ao utilizado no caso anterior, e será o mesmo para os demais casos também. Seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Uma vez que $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, existem $\alpha', \beta' \in \mathbb{K}$ tal que $\eta = \alpha' + \beta'\theta$. Pela Proposição (1.39), $2\alpha', 2\beta' \in \mathcal{O}_{\mathbb{K}}$, de modo que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tal que $\alpha' = \frac{\alpha}{2}$ e $\beta' = \frac{\beta}{2}$. Logo, $2\eta = \alpha + \beta\theta$. Tomando a norma de ambos os lados e usando suas propriedades, segue que

$$N(2\eta) = N(\alpha + \beta\theta) \Rightarrow\ 4N(\eta) = \alpha^2 - \beta^2\theta^2.$$

Assim,

$$\alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{3.31}$$

Como α, $\beta \in \mathcal{O}_{\mathbb{K}}$ e, pelo Teorema 3.3, $\{1, \theta^2, \theta^4, \theta^6\omega_1, \omega_1\theta^2, \omega_2, \omega_2\theta^2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7 \in \mathbb{Z}$

tais que

$$\begin{cases} \alpha = a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + a_4\omega_1 + a_5\omega_1\theta^2 + a_6\omega_2 + a_7\omega_2\theta^2 \quad \text{e} \\ \beta = b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + b_4\omega_1 + b_5\omega_1\theta^2 + b_6\omega_2 + b_7\omega_2\theta^2. \end{cases}$$

Substituindo esses valores na Equação (3.37), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\omega^2 + a_5^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_7^2\omega_2^2\theta^4 \\ &\quad +2(a_0a_1\theta^2 + a_0a_2\theta^4 + a_0a_3\theta^6 + a_0a_4\omega_1 + a_0a_5\omega_1\theta^2 + a_0a_6\omega_2 \\ &\quad +a_0a_7\omega_2\theta^2 + a_1a_2\theta^6 + a_1a_3\theta^8 + a_1a_4\omega_1\theta^2 + a_1a_5\omega_1\theta^4 + a_1a_6\omega_2\theta^2 \\ &\quad +a_1a_7\omega_2\theta^4 + a_2a_3\theta^{10} + a_2a_4\omega_1\theta^4 + a_2a_5\omega_1\theta^6 + a_2a_6\omega_2\theta^4 \\ &\quad +a_2a_7\omega_2\theta^6 + a_3a_4\omega_1\theta^6 + a_3a_5\omega_1\theta^8 + a_3a_6\omega_2\theta^6 + a_3a_7\omega_2\theta^8 \\ &\quad +a_4a_5\omega_1^2\theta^2 + a_4a_6\omega_1\omega_2 + a_4a_7\omega_1\omega_2\theta^2 + a_5a_6\omega_1\omega_2\theta^2 + a_5a_7\omega_1\omega_2\theta^4 \\ &\quad +a_6a_7\omega_2^2\theta^2) - (b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^12 + b_4^2\omega_1^2 + b_5^2\omega_1^2\theta^4 + b_6^2\omega_2^2 \\ &\quad +b_7^2\omega_2^2\theta^4 + 2(b_0b_1\theta^2 + b_0b_2\theta^4 + b_0b_3\theta^6 + b_0b_4\omega_1 + b_0b_5\omega_1\theta^2 + b_0b_6\omega_2 \\ &\quad +b_0b_7\omega_2\theta^2 + b_1b_2\theta^6 + b_1b_3\theta^8 + b_1b_4\omega_1\theta^2 + b_1b_5\omega_1\theta^4 + b_1b_6\omega_2\theta^2 \\ &\quad +b_1b_7\omega_2\theta^4 + b_2b_3\theta^{10} + b_2b_4\omega_1\theta^4 + b_2b_5\omega_1\theta^6 + b_2b_6\omega_2\theta^4 + b_2b_7\omega_2\theta^6 \\ &\quad +b_3b_4\omega_1\theta^6 + b_3b_5\omega_1\theta^8 + b_3b_6\omega_2\theta^6 + b_3b_7\omega_2\theta^8 + b_4b_5\omega_1^2\theta^2 + b_4b_6\omega_1\omega_2 \\ &\quad +b_4b_7\omega_1\omega_2\theta^2 + b_5b_6\omega_1\omega_2\theta^2 + b_5b_7\omega_1\omega_2\theta^4 + b_6b_7\omega_2^2\theta^6)\theta^2 \\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.32}$$

Reescreevendo utilizando a congruência módulo 2, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\omega_1^2 + a_5^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_7^2\omega_2^2\theta^4 \\ &\quad -(b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^{12} + b_4^2\omega_1^2 + b_5^2\omega_1^2\theta^4 + b_6^2\omega_2^2 + b_7^2\omega_2^2\theta^4)\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{3.33}$$

Nesse corpo, são válidas as congruências:

$$\begin{cases} \theta^8 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}), \\ \theta^{12} \equiv \theta^4(mod\ 2\mathcal{O}_{\mathbb{K}}), \\ \omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2^2 \equiv 1 + \theta^4 + \omega_1 + \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \end{cases} \qquad \begin{cases} \omega_1\theta^4 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2\theta^4 \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ x^2 \equiv x(mod\ 2), \end{cases} \tag{3.34}$$

para todo $x \in \mathbb{Z}$. De fato, $\omega_1\theta^4 = 2\omega_2 - \omega_1 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$, pois

$$2\omega_2 - \omega_1 = 2\left(\frac{1+\theta^4+\theta^8+\theta^{12}}{4}\right) - \frac{1+\theta^8}{2} = \frac{\theta^4+\theta^{12}}{2} = \omega_1\theta^4$$

e

$$\omega_1^2 = \left(\frac{1+\theta^8}{2}\right)^2 = \frac{d-1}{4} + \omega_1 = 2m + \omega_1 \equiv \omega_1 (mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Como $d \equiv 1(mod\ 8)$, segue que existe $m \in \mathbb{Z}$ tal que $d-1 = 8m$, e logo, $\frac{d-1}{4} = 2m$. Assim,

$$\begin{aligned}
\omega_2^2 &= \omega_1^2\left(\tfrac{1+\theta^4}{2}\right)^2 = (\omega_1+2m)\left(\tfrac{1+2\theta^4+\theta^8}{4}\right) = (\omega_1+2m)(\tfrac{\omega_1}{2}+\tfrac{\theta^4}{2}) \\
&= m(\omega_1+\theta^4) + \tfrac{1}{2}(\omega_1^2+\theta^4\omega_1) \\
&= m(\omega_1+\theta^4) + \tfrac{1}{2}(\omega_1+2m+2\omega_2-\omega_1) = m(\omega_1+\theta^4+1)+\omega_2 \\
&\equiv 1+\theta^4+\omega_1+\omega_2 (mod\ 2\mathcal{O}_{\mathbb{K}}),
\end{aligned}$$

pois m é ímpar. Por fim,

$$\omega_1^2 = \left(\frac{1+\theta^8}{2}\right)^2 = \frac{d-1}{4} + \omega_1 = 2m + \omega_1 \equiv \omega_1 (mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Como $d \equiv 1(mod\ 8)$, segue que existe $m \in \mathbb{Z}$ tal que $d-1 = 8m$, e logo, $\frac{d-1}{4} = 2m$. Assim,

$$\begin{aligned}
\omega_2^2 &= \omega_1^2\left(\tfrac{1+\theta^4}{2}\right)^2 = (\omega_1+2m)\left(\tfrac{1+2\theta^4+\theta^8}{4}\right) = (\omega_1+2m)(\tfrac{\omega_1}{2}+\tfrac{\theta^4}{2}) \\
&= m(\omega_1+\theta^4) + \tfrac{1}{2}(\omega_1^2+\theta^4\omega_1) \\
&= m(\omega_1+\theta^4) + \tfrac{1}{2}(\omega_1+2m+2\omega_2-\omega_1) = m(\omega_1+\theta^4+1)+\omega_2 \\
&\equiv 1+\theta^4+\omega_1+\omega_2 (mod\ 2\mathcal{O}_{\mathbb{K}}),
\end{aligned}$$

pois m é ímpar. Por fim,

$$\begin{aligned}
\omega_2\theta^4 &= \omega_1\left(\tfrac{1+\theta^4}{2}\right)\theta^4 = \omega_1\left(\tfrac{\theta^4+\theta^8}{2}\right) = \tfrac{\omega_1\theta^4}{2} + \tfrac{\omega_1\theta^8}{2} = \tfrac{2\omega_2-\omega_1}{2} + \tfrac{\omega_1(2\omega_1-1)}{2} \\
&= \omega_2 - \tfrac{\omega_1}{2} + \omega_1^2 - \tfrac{\omega_1}{2} = \omega_2 - \omega_1 + 2m + \omega_1 = \omega_2 + 2m \\
&\equiv \omega_2 (mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Utilizando essas congruências na Equação (3.33), segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= a_0+a_1\theta^4+a_2+a_3\theta^4+a_4\omega_1+a_5\omega_1+a_6(1+\theta^4+\omega_1+\omega_2)\\ &\quad +a_7(1+\theta^4+\omega_1+\omega_2)-(b_0+b_1\theta^4+b_2+b_3\theta^4+b_4\omega_1+b_5\omega_1\theta^4)\theta^2\\ &\quad -(b_6(1+\theta^4+\omega_1+\omega_2)+b_7(1+\theta^4+\omega_1+\omega_2))\theta^2=a_0+a_2+a_6\\ &\quad +a_7+(a_4+a_5+a_6+a_7)\omega_1+(a_1+a_3+a_6+a_7)\theta^4+(a_6+a_7)\omega_2\\ &\quad +(-b_0-b_2-b_6-b_7)\theta^2+(-b_4-b_5)\omega_1\theta^2+(-b_1-b_3-b_6-b_7)\theta^6\\ &\quad -(b_6+b_7)\omega_2\theta^2\\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $\{1,\theta^2,\theta^4,\theta^6\omega_1,\omega_1\theta^2,\omega_2,\omega_2\theta^2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $a_i,b_i\in\mathbb{Z}$, segue que os coeficientes devem ser congruentes a 0 módulo 2, donde seguem as congruências

$$\begin{cases} a_0+a_2+a_6+a_7\equiv 0\ (mod\ 2)\\ a_4+a_5+a_6+a_7\equiv 0\ (mod\ 2)\\ a_1+a_3+a_6+a_7\equiv 0\ (mod\ 2)\\ a_6+a_7\equiv 0\ (mod\ 2)\\ -b_0-b_2-b_6-b_7\equiv 0(mod\ 2)\\ -b_4-b_5-b_6-b_7\equiv 0\ (mod\ 2)\\ -b_1-b_3-b_6-b_7\equiv 0(mod\ 2)\\ -b_6-b_7\equiv 0\ (mod\ 2).\end{cases}$$

E essas congruências fornecem as seguintes relações

$$\begin{cases} a_0\equiv -a_2\ (mod\ 2)\\ a_1\equiv -a_3\ (mod\ 2)\\ a_4\equiv -a_5\ (mod\ 2)\\ a_6\equiv -a_7\ (mod\ 2)\end{cases}\qquad\begin{cases} b_0\equiv -b_2\ (mod\ 2)\\ b_1\equiv -b_3\ (mod\ 2)\\ b_4\equiv -b_5\ (mod\ 2)\\ b_6\equiv -b_7\ (mod\ 2).\end{cases}\tag{3.35}$$

Assim,

$$\begin{cases} {a_0}^2\equiv {a_2}^2\ (mod\ 4)\\ {a_1}^2\equiv {a_3}^2\ (mod\ 4)\\ {a_4}^2\equiv {a_5}^2\ (mod\ 4)\\ {a_6}^2\equiv {a_7}^2\ (mod\ 4)\\ {b_0}^2\equiv {b_2}^2(mod\ 4)\\ {b_1}^2\equiv {b_3}^2\ (mod\ 4)\\ {b_4}^2\equiv {b_5}^2(mod\ 4)\\ {b_6}^2\equiv {b_7}^2\ (mod\ 4)\end{cases}\qquad\begin{cases} 2a_0a_2\equiv -2(a_0)^2(mod\ 4)\\ 2a_1a_3\equiv -2(a_1)^2(mod\ 4)\\ 2a_4a_5\equiv -2(a_4)^2(mod\ 4)\\ 2a_6a_7\equiv -2(a_6)^2(mod\ 4)\\ 2b_0b_2\equiv -2(b_0)^2(mod\ 4)\\ 2b_1b_3\equiv -2(b_1)^2(mod\ 4)\\ 2b_4b_5\equiv -2(b_4)^2(mod\ 4)\\ 2b_6b_7\equiv -2(b_6)^2(mod\ 4).\end{cases}$$

Nesse sistema vale o mesmo que foi visto na Observação 3.6. Substituindo essas congruências na Equação (3.32), segue que

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_0^2\theta^8 + a_1^2\theta^{12} + a_4^2\omega_1^2 + a_4^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_6^2\omega_2^2\theta^4 \\ &\quad -2a_0^2\theta^4 - 2a_1^2\theta^8 - 2a_4^2\omega_1^2\theta^2 - 2a_6^2\omega_2^2\theta^2 - (b_0^2 + b_1^2\theta^4 + b_0^2\theta^8 + b_1^2\theta^{12} \\ &\quad +b_4^2\omega_1^2 + b_4^2\omega_1^2\theta^4 + b_6^2\omega_2^2 + b_6^2\omega^2\theta^4 - 2b_0^2\theta^4 - 2b_1^2\theta^8 - 2b_4^2\omega_1^2\theta^2 \\ &\quad -2b_6^2\omega_2^2\theta^2)\theta^2 \\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Colocando os termos que multiplicam os mesmos valores de a_i e b_i em evidência, obtemos

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= (1+\theta^8)(a_0^2 + a_1^2\theta^4) + \omega_1^2(1+\theta^4)a_4^2 + \omega_2^2(1+\theta^4)a_6^2 - 2a_0^2\theta^4 - 2a_1^2\theta^8 \\ &\quad -2a_4^2\omega^2\theta^4 - 2a_5^2\omega^2\theta^8 - [(1+\theta^8)(b_0^2 + b_1^2\theta^4 + b_4^2\omega^2 + b_5^2\omega^2\theta^4) - 2b_0^2\theta^4 \\ &\quad -2b_1^2\theta^8 - 2b_4^2\omega^2\theta^4 - 2b_5^2\omega^2\theta^8]\theta^2 \\ &\quad \equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned} \tag{3.36}$$

Nesse corpo, são válidas as igualdades

$$\begin{cases} 1 + \theta^8 = 2\omega_1, \\ \omega_1^2(1+\theta^4) = 2m + 2m\theta^4 + 2\omega_2 \text{ e} \\ \omega_2^2(1+\theta^4) = 2m + 2m\theta^4 + 2m\omega_1 + 2m\omega_2 + 2\omega_2. \end{cases}$$

De fato, a primeira é imediata e, para as demais,

$$\begin{aligned}\omega_1^2(1+\theta^4) &= (2m+\omega_1)(1+\theta^4) = 2m + 2m\theta^4 + \omega_1 + \omega_1\theta^4 \\ &= 2m + 2m\theta^4 + \omega_1 + 2\omega_2 - \omega_1 \\ &= 2(m + m\theta^4 + \omega_2)\end{aligned}$$

e

$$\begin{aligned}\omega_2^2(1+\theta^4) &= (m + m\theta^4 + m\omega_1 + \omega_2)(1+\theta^4) \\ &= m + m\theta^4 + m\theta^4 + m\theta^8 + m\omega_1 + m\omega_1\theta^4 + \omega_2 + \omega_2\theta^4 \\ &= m + 2m\theta^4 + m(2\omega_1 - 1) + m\omega_1 + m(2\omega_2 - \omega_1) + \omega_2 + (\omega_2 + 2m) \\ &= 2m + 2m\theta^4 + 2m\omega_1 + 2m\omega_2 + 2\omega_2,\end{aligned}$$

onde m é tal que $d - 1 = 8m$.

Realizando essas substituições na Equação (3.36), obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= 2\omega_1(a_0^2+a_1^2\theta^4)+2(m+m\theta^4+\omega_2)a_4^2\\ &\quad +2(m+m\theta^4+m\omega_1+m\omega_2+\omega_2)a_6^2\\ &\quad -2(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^4+a_6^2\omega_2^2\theta^8)\\ &\quad -[2\omega_1(b_0^2+b_1^2\theta^4)+2(m+m\theta^4+\omega_2)b_4^2\\ &\quad +2(m+m\theta^4+m\omega_1+m\omega_2+\omega_2)b_5^2\\ &\quad -2(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^4+b_6^2\omega_2^2\theta^8]\theta^2\\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como todos os termos estão multiplicando por 2, podemos usar que $2x \equiv 0\ (mod\ 4) \Rightarrow x \equiv 0\ (mod\ 2)$ e, em seguida, que $m \equiv 1\pmod 2$, de onde obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega_1(a_0^2+a_1^2\theta^4)+(1+\theta^4+\omega_2)a_4^2+(1+\theta^4+\omega_1)a_6^2\\ &\quad -(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^2+a_6^2\omega_2^2\theta^2)\\ &\quad -[\omega_1(b_0^2+b_1^2\theta^4)+(1+\theta^4+\omega_2)b_4^2+(1+\theta^4+\omega_1)b_5^2\\ &\quad -(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^2+b_6^2\omega_2^2\theta^2]\theta^2\\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Usando novamente as congruências módulo 2 contidas no Sistema (3.34), segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega_1(a_0+a_1\theta^4)+(1+\theta^4+\omega_2)a_4+(1+\theta^4+\omega_1)a_6\\ &\quad -(a_0\theta^4+a_1+a_4\omega_1\theta^2+a_6\theta^2(1+\theta^4+\omega_1+\omega_2))\\ &\quad -[\omega_1(b_0+b_1\theta^4)+(1+\theta^4+\omega_2)b_4+(1+\theta^4+\omega_1)b_5\\ &\quad -(b_0\theta^4+b_1+b_4\omega_1\theta^2+b_6\theta^2(1+\theta^4+\omega_1+\omega_2)]\theta^2\\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Realizando mais algumas substituições das congruências módulo 2 contidas no Sistema (3.34) e colocando alguns termos em evidência, obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega_1(a_0+a_1)+(1+\theta^4+\omega_2)a_4+(1+\theta^4+\omega_1)a_6\\ &\quad -[a_0\theta^4+a_1+a_4\omega_1\theta^2+a_6(\theta^2+\theta^6+\omega_1\theta^2+\omega_2\theta^2)]\\ &\quad -[\omega_1\theta^2(b_0+b_1)+(\theta^2+\theta^6+\omega_2\theta^2)b_4+(\theta^2+\theta^6+\omega_1\theta^2)b_5\\ &\quad -(b_0\theta^6+b_1\theta^2+b_4\omega_1+b_6(1+\theta^4+\omega_1+\omega_2)]\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_2\theta^2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2. Logo,

$$\begin{cases} a_4 - a_1 + a_6 + b_6 \equiv 0 \ (mod\ 2) \\ -b_4 - b_1 - b_6 - a_6 \equiv 0 \ (mod\ 2) \\ a_4 - a_0 + a_6 + b_6 \equiv 0 \ (mod\ 2) \\ -b_4 + b_0 - b_6 - a_6 \equiv 0 \ (mod\ 2) \\ a_0 + a_1 + a_6 + b_4 + b_6 \equiv 0 \ (mod\ 2) \\ -b_0 - b_1 - b_6 - a_4 - a_6 \equiv 0 \ (mod\ 2) \\ a_4 + b_6 \equiv 0 \ (mod\ 2) \\ -b_4 - a_6 \equiv 0 \ (mod\ 2). \end{cases}$$

Como a única solução é $a_i, b_i \equiv 0(mod\ 2)$, ou seja, todos pares, segue que $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$ e, portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ, ω_1 e ω_2 são inteiros em $\mathbb{L}$, segue que

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_2\theta^2][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto, $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$

4. Seja $d \equiv 17(mod\ 32)$ ou, equivalentemente, $d \equiv 1(mod\ 16)$ e $d \not\equiv 1(mod\ 32)$. Mostremos que

$$\mathcal{O}_{\mathbb{L}} = \{1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_3\theta\} = \mathcal{O}_{\mathbb{K}}[\theta].$$

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Neste caso, mais uma vez tomando $\eta \in \mathcal{O}_{\mathbb{L}}$ chegamos em

$$N(2\eta) = N(\alpha + \beta\theta) \Rightarrow\ 4N(\eta) = \alpha^2 - \beta^2\theta^2,$$

e, assim,

$$\alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{3.37}$$

Como α, $\beta \in \mathcal{O}_{\mathbb{K}}$ e $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_3\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7 \in \mathbb{Z}$ tais que

$$\begin{cases} \alpha = a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + a_4\omega_1 + a_5\omega_1\theta^2 + a_6\omega_2 + a_7\omega_3 \\ \beta = b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + b_4\omega_1 + b_5\omega_1\theta^2 + b_6\omega_2 + b_7\omega_3. \end{cases}$$

Substituindo esses valores na Equação (3.37), segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= a_0^2+a_1^2\theta^4+a_2^2\theta^8+a_3^2\theta^{12}+a_4^2\omega_1^2+a_5^2\omega_1^2\theta^4+a_6^2\omega_2^2+a_7^2\omega_3^2\\
&\quad +2(a_0a_1\theta^2+a_0a_2\theta^4+a_0a_3\theta^6+a_0a_4\omega_1+a_0a_5\omega_1\theta^2+a_0a_6\omega_2\theta^4\\
&\quad +a_0a_7\omega_3\theta^6+a_1a_2\theta^6+a_1a_3\theta^8+a_1a_4\omega_1\theta^2+a_1a_5\omega_1\theta^4+a_1a_6\omega_2\theta^6\\
&\quad +a_1a_7\omega_3\theta^8+a_2a_3\theta^{10}+a_2a_4\omega_1\theta^4+a_2a_5\omega_1\theta^6+a_2a_6\omega_2\theta^8\\
&\quad +a_2a_7\omega_3\theta^{10}+a_3a_4\omega_1\theta^6+a_3a_5\omega_1\theta^8+a_3a_6\omega_2\theta^{10}+a_3a_7\omega_3\theta^{12}\\
&\quad +a_4a_5\omega_1^2\theta^2+a_4a_6\omega_1\omega_2+a_4a_7\omega_1\omega_3+a_5a_6\omega_1\omega_2\theta^2+a_5a_7\omega_1\omega_3\theta^2\\
&\quad +a_6a_7\omega_2\omega_3)-(b_0^2+b_1^2\theta^4+b_2^2\theta^8+b_3^2\theta^{12}+b_4^2\omega_1^2+b_5^2\omega_1^2\theta^4+b_6^2\omega_2^2\\
&\quad +b_7^2\omega_3^2+2(b_0b_1\theta^2+b_0b_2\theta^4+b_0b_3\theta^6+b_0b_4\omega_1+b_0b_5\omega_1\theta^2+b_0b_6\omega_2\\
&\quad +b_0b_7\omega_3+b_1b_2\theta^6+b_1b_3\theta^8+b_1b_4\omega_1\theta^2+b_1b_5\omega_1\theta^4+b_1b_6\omega_2\theta^2\\
&\quad +b_1b_7\omega_3\theta^2+b_2b_3\theta^{10}+b_2b_4\omega_1\theta^4+b_2b_5\omega_1\theta^6+b_2b_6\omega_2\theta^4+b_2b_7\omega_3\theta^4\\
&\quad +b_3b_4\omega_1\theta^6+b_3b_5\omega_1\theta^8+b_3b_6\omega_2\theta^{12}+b_3b_7\omega_3\theta^{12}+b_4b_5\omega_1^2\theta^2\\
&\quad +b_4b_6\omega_1\omega_2+b_4b_7\omega_1\omega_3+b_5b_6\omega_1\omega_2\theta^2+b_5b_7\omega_1\omega_3\theta^2+b_6b_7\omega_2\omega_3)\theta^2\\
&\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned} \tag{3.38}$$

Reescrevendo a Equação (3.38) em termos da congruência módulo 2, segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= a_0^2+a_1^2\theta^4+a_2^2\theta^8+a_3^2\theta^{12}+a_4^2\omega_1^2+a_5^2\omega_1^2\theta^4+a_6^2\omega_2^2+a_7^2\omega_3^2\\
&\quad -(b_0^2+b_1^2\theta^4+b_2^2\theta^8+b_3^2\theta^{12}+b_4^2\omega_1^2+b_5^2\omega_1^2\theta^4+b_6^2\omega_2^2+b_7^2\omega_3^2)\theta^2\\
&\quad \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned} \tag{3.39}$$

Nesse corpo, são válidas as congruências:

$$\begin{cases}
\theta^8\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}),\\
\theta^{12}\equiv\theta^4(mod\ 2\mathcal{O}_{\mathbb{K}}),\\
\omega_1^2\equiv\omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_2^2\equiv\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_3^2\equiv\omega_3+1+\theta^2+\theta^4+\theta^6+\omega_1+\omega_1\theta^2+\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_1\theta^4\equiv\omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_2\theta^2\equiv\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_3\theta^2\equiv\omega_3(mod\ 2\mathcal{O}_{\mathbb{K}})\\
x^2\equiv x(mod\ 2),
\end{cases} \tag{3.40}$$

para todo $x\in\mathbb{Z}$. De fato, $\theta^8\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e $\theta^{12}\equiv\theta^4(mod\ 2\mathcal{O}_{\mathbb{K}})$ são imediatas.

As demais são demonstradas a seguir.

(I) Para ω_1, segue que

$$\omega_1^2 = \left(\frac{1+\theta^8}{2}\right)^2 = \frac{d-1}{4} + \omega_1 = 4m + \omega_1 \equiv \omega_1 (mod\ 4\mathcal{O}_{\mathbb{K}}).$$

(II) Para ω_2, segue que

$$\begin{aligned}
\omega_2^2 &= \omega_1^2 \left(\tfrac{1+\theta^4}{2}\right)^2 = (\omega_1 + 4m)\left(\tfrac{1+2\theta^4+\theta^8}{4}\right) = (\omega_1 + 4m)(\tfrac{\omega_1}{2} + \tfrac{\theta^4}{2}) \\
&= 2m(\omega_1 + \theta^4) + \tfrac{1}{2}(\omega_1^2 + \theta^4\omega_1) \\
&= 2m(\omega_1 + \theta^4) + \tfrac{1}{2}(\omega_1 + 4k + 2\omega_2 - \omega_1) = 2m(\omega_1 + \theta^4 + 1) + \omega_2 \\
&\equiv \omega_2 (mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

(III) Para ω_3, segue que

$$\begin{aligned}
\omega_3^2 &= \omega_2^2 \left(\tfrac{1+\theta^2}{2}\right)^2 = \omega_1^2 \left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right) \\
&= (\omega_1 + 4m)\left(\tfrac{1+2\theta^4}{2} - \tfrac{1-\theta^8}{2}\right)\left(\tfrac{1+\theta^2}{2} - \tfrac{1-\theta^4}{4}\right) = (\omega_1 + 4m)(\tfrac{1+\theta^4}{2} + \tfrac{1+\theta^2}{2}) \\
&\quad +(4m + \omega_1)\left[\left(\tfrac{1+\theta^4}{2}\right)\left(-\tfrac{1-\theta^4}{4}\right) + \left(-\tfrac{1-\theta^8}{4}\right)\left(\tfrac{1+\theta^2}{2}\right) + \left(\tfrac{1-\theta^8}{4}\right)\left(\tfrac{1-\theta^4}{4}\right)\right] \\
&= m(1+\theta^4)(1+\theta^2) + \omega_3 + (4m + \omega_1)\left[-\left(\tfrac{1}{4}\right)\omega_1^* - \left(\tfrac{1+\theta^2}{4}\right)\omega_1^* + \left(\tfrac{1-\theta^4}{8}\right)\omega_1^*\right] \\
&= m(1+\theta^4)(1+\theta^2) + \omega_3 + (-4m\omega_1)\left[-\left(\tfrac{1}{4}\right) - \left(\tfrac{1+\theta^2}{4}\right) + \left(\tfrac{1-\theta^4}{8}\right)\right] \\
&= m(1+\theta^4)(1+\theta^2) + \omega_3 + (m\omega_1)\left[1 + 1 + \theta^2 - \left(\tfrac{1}{2} - \tfrac{\theta^4}{2}\right)\right] \\
&= m(1+\theta^4)(1+\theta^2) + \omega_3 + (m\omega_1)\left(1 + \theta^2 - \tfrac{1+\theta^4}{2}\right) \\
&= m(1+\theta^2+\theta^4+\theta^6) + \omega_3 + m\left(\omega_1 + \omega_1\theta^2 + \omega_2\right) \\
&\equiv 1 + \theta^2 + \theta^4 + \theta^6 + \omega_1 + \omega_1\theta^2 + \omega_2 + \omega_3 (mod\ 2\mathcal{O}_{\mathbb{K}}),
\end{aligned}$$

onde $\omega_1^* = -\omega_1 + 1 = \frac{1-\theta^8}{2}$, por isso $(4m + \omega_1)\omega_1^* = -4m\omega_1$, e m é ímpar, senão, d seria congruente a 1 módulo 32.

(IV) $\omega_1\theta^4 = \frac{1+\theta^8}{2}\theta^4 = \frac{\theta^4+\theta^{12}}{2} = 2\left(\frac{1+\theta^4+\theta^8+\theta^{12}}{4}\right) - \frac{1+\theta^8}{2} = 2\omega_2 - \omega_1 \equiv \omega_1 (mod\ 2\mathcal{O}_{\mathbb{K}})$

(V) Analogamente ao item (IV), $\omega_2\theta^2 = 2\omega_3 - \omega_2 \equiv \omega_2 (mod\ 2\mathcal{O}_{\mathbb{K}})$

(VI) Para $\omega_3\theta^2$, segue que

$$\begin{aligned}
\omega_3\theta^2 &= \omega_1\left(\frac{1+\theta^4}{2}\right)\left(\frac{1+\theta^2}{2}\right)\theta^2 = \omega_1\left(\frac{\theta^2+\theta^4+\theta^6+\theta^8}{4}\right)\\
&= \frac{\omega_1\theta^2}{4}+\frac{\omega_1\theta^4}{4}+\frac{\omega_1\theta^6}{4}+\frac{\omega_1\theta^8}{4}\\
&= \frac{\omega_1\theta^2}{4}+\frac{2\omega_2-\omega_1}{4}+\frac{(2\omega_2\theta^2-\omega_1\theta^2)}{4}+\frac{\omega_1(2\omega_1-1)}{4}\\
&= \frac{\omega_1\theta^2}{4}+\frac{\omega_2}{2}-\frac{\omega_1}{4}+\frac{(\omega_2\theta^2}{2}-\frac{\omega_1\theta^2)}{4}+\frac{\omega_1^2}{2}-\frac{\omega_1}{4}\\
&= \frac{\omega_2}{2}-\frac{\omega_1}{2}+\frac{2\omega_3-\omega_2}{2}+\frac{\omega_1+4m}{2}\\
&= \tfrac{\omega_2}{2}-\tfrac{\omega_1}{2}+\omega_3-\tfrac{\omega_2}{2}+\tfrac{\omega_1}{2}+2m=\omega_3+2m\\
&\equiv \omega_3(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Substituindo essas congruências na Equação (3.39), segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= a_0+a_1\theta^4+a_2+a_3\theta^4+a_4\omega_1+a_5\omega_1+a_6\omega_2\\
&\quad +a_7(\omega_3+1+\theta^2+\theta^4+\theta^6+\omega_1+\omega_1\theta^2+\omega_2)-(b_0+b_1\theta^4\\
+ &\quad b_2+b_3\theta^4+b_4\omega_1+b_5\omega_1+b_6\omega_2+b_6+b_7(\omega_3+1+\theta^2+\theta^4\\
&\quad +\theta^6+\omega_1+\omega_1\theta^2+\omega_2))\theta^2\\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})
\end{aligned}$$

Substituindo novamente as congruências contidas no Sistema (3.40) na última equação, segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= a_0+a_1\theta^4+a_2+a_3\theta^4+a_4\omega_1+a_5\omega_1+a_6\omega_2\\
&\quad +a_7(\omega_3+1+\theta^2+\theta^4+\theta^6+\omega_1+\omega_1\theta^2+\omega_2)-b_0\theta^2\\
&\quad -b_1\theta^6b_2\theta^2-b_3\theta^6-b_4\omega_1\theta^2-b_5\omega_1\theta^2-b_6\omega_2\\
&\quad -b_7(\omega_3+1+\theta^2+\theta^4+\theta^6+\omega_1+\omega_1\theta^2+\omega_2)\\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})
\end{aligned}$$

Desse modo, obtemos uma combinação linear inteira dos elementos da base $\{1,\theta^2,\theta^4,\theta^6\omega,\omega\theta^2,\omega\theta^4,\omega\theta^6\}$ de $\mathcal{O}_{\mathbb{K}}$. Assim, os coeficientes devem ser congruentes a 0 módulo 2, donde seguem as congruências

$$\begin{cases} a_0 + a_2 + a_7 - b_7 \equiv 0 \ (mod\ 2) \\ -b_0 - b_2 - b_7 + a_7 \equiv 0 \ (mod\ 2) \\ a_1 + a_3 + a_7 - b_7 \equiv 0 \ (mod\ 2) \\ -b_1 - b_3 - b_7 + a_7 \equiv 0 \ (mod\ 2) \\ a_4 + a_5 + a_7 - b_7 \equiv 0 \ (mod\ 2) \\ -b_4 - b_5 - b_7 + a_7 \equiv 0 \ (mod\ 2) \\ a_6 + a_7 - b_6 - b_7 \equiv 0 \ (mod\ 2) \\ a_7 - b_7 \equiv 0 \ (mod\ 2). \end{cases}$$

Essas congruências fornecem as seguintes relações

$$\begin{cases} a_0 \equiv -a_2 \ (mod\ 2) \\ b_0 \equiv -b_2 \ (mod\ 2) \\ a_1 \equiv -a_3 \ (mod\ 2) \\ b_1 \equiv -b_3 \ (mod\ 2) \end{cases} \qquad \begin{cases} a_4 \equiv -a_5 \ (mod\ 2) \\ b_4 \equiv -b_5 \ (mod\ 2) \\ a_6 \equiv b_6 \ (mod\ 2) \\ a_7 \equiv b_7 \ (mod\ 2). \end{cases} \tag{3.41}$$

Assim,

$$\begin{cases} {a_0}^2 \equiv {a_2}^2 \ (mod\ 4) \\ {a_1}^2 \equiv {a_3}^2 \ (mod\ 4) \\ {a_4}^2 \equiv {a_5}^2 \ (mod\ 4) \\ {b_0}^2 \equiv {b_2}^2 (mod\ 4) \\ {b_1}^2 \equiv {b_3}^2 \ (mod\ 4) \\ {b_4}^2 \equiv {b_5}^2 (mod\ 4) \\ {a_6}^2 \equiv {b_6}^2 \ (mod\ 4) \\ {a_7}^2 \equiv {b_7}^2 \ (mod\ 4) \end{cases} \qquad \begin{cases} 2a_0a_2 \equiv -2(a_0)^2 (mod\ 4) \\ 2a_1a_3 \equiv -2(a_1)^2 (mod\ 4) \\ 2a_4a_5 \equiv -2(a_4)^2 (mod\ 4) \\ 2b_0b_2 \equiv -2(b_0)^2 (mod\ 4) \\ 2b_1b_3 \equiv -2(b_1)^2 (mod\ 4) \\ 2b_4b_5 \equiv -2(b_4)^2 (mod\ 4) \\ 2b_6b_7 \equiv 2a_6a_7 (mod\ 4), \end{cases} \tag{3.42}$$

onde mais uma vez é válida a Observação 3.6. Substituindo essas congruências na Equação (3.11), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_0^2\theta^8 + a_1^2\theta^{12} + a_4^2\omega_1^2 + a_4^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_7^2\omega_3^2 \\ &\quad -2(a_0^2\theta^4 + a_1^2\theta^8 + a_4^2\omega_1^2\theta^4 - a_6a_7\omega_2\omega_3) - (b_0^2 + b_1^2\theta^4 + b_0^2\theta^8 \\ &\quad +b_1^2\theta^{12} + b_4^2\omega_1^2 + b_4^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_7^2\omega_3^2 - 2(b_0^2\theta^4 + b_1^2\theta^8 \\ &\quad +b_4^2\omega_1^2\theta^4 - a_6a_7\omega_2\omega_3))\theta^2 \\ &\equiv 0 \ (mod\ 4\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Assim, agrupando os termos semelhantes, obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta &= (1+\theta^8)(a_0^2+a_1^2\theta^4)+\omega_1^2(1+\theta^4)a_4^2\\ &\quad +(1-\theta^2)a_6^2\omega_2^2+a_7^2\omega_3^2-2(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)\\ &\quad -[(1+\theta^8)(b_0^2+b_1^2\theta^4)+\omega_1^2(1+\theta^4)b_4^2-2(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^4\\ &\quad -a_6a_7\omega_2\omega_3)]\theta^2\\ &\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $1+\theta^8=2\omega_1$, $\omega_1^2(1+\theta^4)=2\omega_2$ e $(1-\theta^2)(a_6^2\omega_2^2+a_7^2\omega_3^2)=2(a_6^2-a_6^2\theta^2+a_6^2\theta^4-a_6^2\theta^6+a_6^2\omega_1-a_6^2\omega_1\theta^2+a_6^2\omega_2-a_6^2\omega_3-a_7^2\omega_3)$ e todos os termos estão multiplicados por 2, segue que podemos reduzir a congruência, pois $2x\equiv 0\ (mod\ 4)\Rightarrow x\equiv 0\ (mod\ 2)$. Desse modo, obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega_1(a_0^2+a_1^2\theta^4)+\omega_2a_4^2+a_6^2-a_6^2\theta^2+a_6^2\theta^4-a_6^2\theta^6+a_6^2\omega_1-a_6^2\omega_1\theta^2\\ &\quad +a_6^2\omega_2-a_6^2\omega_3-a_7^2\omega_3-(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)\\ &\quad -[\omega_1(b_0^2+b_1^2\theta^4)+\omega_2b_4^2-(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)]\theta^2\\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Usando novamente os fatos $\theta^8\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$, $\omega_1\theta^4\equiv\omega_1\ (mod\ 2\mathcal{O}_{\mathbb{K}})$, $\omega_2\theta^2\equiv\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})$, $\omega_3\theta^2\equiv\omega_3(mod\ 2\ \mathcal{O}_{\mathbb{K}})$, $\omega_2\omega_3\theta^2\equiv\omega_2\omega_3(mod\ 2\mathcal{O}_{\mathbb{K}})$ e $x^2\equiv x\ (mod\ 2)$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega_1(a_0+a_1)+a_4\omega_2+a_6-a_6\theta^2+a_6\theta^4-a_6\theta^6+a_6\omega_1\\ &\quad -a_6\omega_1\theta^2+a_6\omega_2-a_6\omega_3-a_7\omega_3-(a_0\theta^4+a_1+a_4\omega_1)\\ &\quad -[\omega_1(b_0+b_1\theta^4)+\omega_2b_4-(b_0\theta^4+b_1+b_4\omega_1]\theta^2\\ &= \omega_1(a_0+a_1)+a_4\omega_2+a_6-a_6\theta^2+a_6\theta^4-a_6\theta^6+a_6\omega_1-a_6\omega_1\theta^2\\ &\quad +a_6\omega_2-a_6\omega_3-a_7\omega_3-(a_0\theta^4+a_1+a_4\omega_1)-\omega_1\theta^2(b_0+b_1)\\ &\quad -\omega_2b_4+b_0\theta^6+b_1\theta^2+b_4\omega_1\theta^2\\ &\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Como $\{1,\theta^2,\theta^4,\theta^6,\omega_1,\omega_1\theta^2,\omega_2,\omega_3\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2. Logo, segue que

$$\begin{cases} -a_1 + a_6 \equiv 0(mod\ 2) \\ -b_1 - a_6 \equiv 0\ (mod\ 2) \\ -a_0 + a_6 \equiv 0\ (mod\ 2) \\ -b_0 - a_6 \equiv 0\ (mod\ 2) \\ a_0 + a_1 - a_4 + a_6 \equiv 0\ (mod\ 2) \\ -b_0 - b_1 + b_4 - a_6 \equiv 0\ (mod\ 2) \\ a_4 - b_4 + a_6 \equiv 0\ (mod\ 2) \\ a_6 - a_7 \equiv 0\ (mod\ 2). \end{cases}$$

Como a única solução possível é $a_i, b_i \equiv 0(mod\ 2)$, ou seja, todos pares, segue que $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$ e, portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ e ω_1, ω_2 e ω_3 são inteiros em $\mathbb{L}$, segue que

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_3][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto, $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$.

5. Seja $d \equiv 1(mod\ 32)$. Neste caso, vamos mostrar que

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_4].$$

a) $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_4]$. Como $d \equiv 1(mod\ 32)$, segue que $d \equiv 1(mod\ 16)$. Desse modo, tomando $\eta \in \mathcal{O}_{\mathbb{L}}$ existem α, $\beta \in \mathcal{O}_{\mathbb{K}}$ e $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7 \in \mathbb{Z}$ tais que

$$\begin{cases} \alpha = a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + a_4\omega_1 + a_5\omega_1\theta^2 + a_6\omega_2 + a_7\omega_3 \ \text{ e} \\ \beta = b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + b_4\omega_1 + b_5\omega_1\theta^2 + b_6\omega_2 + b_7\omega_3, \end{cases}$$

exatamente como no item 4, uma vez que uma base de $\mathcal{O}_{\mathbb{K}}$ é a mesma para ambas as congruências $d \equiv 17\ (\text{mod } 32)$ e $d \equiv 1\ (\text{mod } 32)$. Substituindo esses valores na Equação (3.37), segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 \ = \ & a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\omega_1^2 + a_5^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_7^2\omega_3^2 \\ & +2(a_0a_1\theta^2 + a_0a_2\theta^4 + a_0a_3\theta^6 + a_0a_4\omega_1 + a_0a_5\omega_1\theta^2 + a_0a_6\omega_2\theta^4 \\ & +a_0a_7\omega_3\theta^6 + a_1a_2\theta^6 + a_1a_3\theta^8 + a_1a_4\omega_1\theta^2 + a_1a_5\omega_1\theta^4 + a_1a_6\omega_2\theta^6 \\ & +a_1a_7\omega_3\theta^8 + a_2a_3\theta^{10} + a_2a_4\omega_1\theta^4 + a_2a_5\omega_1\theta^6 + a_2a_6\omega_2\theta^8 + a_2a_7\omega_3\theta^{10} \end{aligned}$$

$$
\begin{aligned}
&+a_3a_4\omega_1\theta^6 + a_3a_5\omega_1\theta^8 + a_3a_6\omega_2\theta^{10} + a_3a_7\omega_3\theta^{12} + a_4a_5\omega_1^2\theta^2\\
&+a_4a_6\omega_1\omega_2 + a_4a_7\omega_1\omega_3 + a_5a_6\omega_1\omega_2\theta^2 + a_5a_7\omega_1\omega_3\theta^2 + a_6a_7\omega_2\omega_3)\\
&-(b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^{12} + b_4^2\omega_1^2 + b_5^2\omega_1^2\theta^4 + b_6^2\omega_2^2 + b_7^2\omega_3^2 + 2(b_0b_1\theta^2\\
&+b_0b_2\theta^4 + b_0b_3\theta^6 + b_0b_4\omega_1 + b_0b_5\omega_1\theta^2 + b_0b_6\omega_2 + b_0b_7\omega_3 + b_1b_2\theta^6\\
&+b_1b_3\theta^8 + b_1b_4\omega_1\theta^2 + b_1b_5\omega_1\theta^4 + b_1b_6\omega_2\theta^2 + b_1b_7\omega_3\theta^2 + b_2b_3\theta^{10}\\
&+b_2b_4\omega_1\theta^4 + b_2b_5\omega_1\theta^6 + b_2b_6\omega_2\theta^4 + b_2b_7\omega_3\theta^4 + b_3b_4\omega_1\theta^6 + b_3b_5\omega_1\theta^8\\
&+b_3b_6\omega_2\theta^{12} + b_3b_7\omega_3\theta^{12} + b_4b_5\omega_1^2\theta^2 + b_4b_6\omega_1\omega_2 + b_4b_7\omega_1\omega_3 + b_5b_6\omega_1\omega_2\theta^2\\
&+b_5b_7\omega_1\omega_3\theta^2 + b_6b_7\omega_2\omega_3)\theta^2\\
\equiv\ & 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned}
\tag{3.43}
$$

Reescrevendo em termos da congruência módulo 2, segue que

$$
\begin{aligned}
\alpha^2 - \beta^2\theta^2 \ =\ & a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\omega_1^2 + a_5^2\omega_1^2\theta^4 + a_6^2\omega_2^2 + a_7^2\omega_3^2\\
&-(b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^{12} + b_4^2\omega_1^2\\
&+b_5^2\omega_1^2\theta^4 + b_6^2\omega_2^2 + b_7^2\omega_3^2)\theta^2 \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}
$$

Nesse corpo, são válidas as congruências:

$$
\begin{cases}
\theta^8 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}),\\
\theta^{12} \equiv \theta^4(mod\ 2\mathcal{O}_{\mathbb{K}}),\\
\omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_2^2 \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_3^2 = \omega_3 + 2m(1 + \theta^2 + \theta^4 + \theta^6 + \omega_1 + \omega_1\theta^2 + \omega_2) \equiv \omega_3(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_1\theta^4 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_2\theta^2 \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_3\theta^2 \equiv \omega_3(mod\ 2\mathcal{O}_{\mathbb{K}})\\
x^2 \equiv x(mod\ 2),
\end{cases}
$$

para todo $x \in \mathbb{Z}$. cujas demonstrações também são análogas às já feitas anteriormente. Utilizando-as, segue que

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= a_0 + a_1\theta^4 + a_2 + a_3\theta^4 + a_4\omega_1 + a_5\omega_1 + a_6\omega_2 + a_7\omega_3 \\
&\quad -(b_0 + b_1\theta^4 + b_2 + b_3\theta^4 + b_4\omega_1 + b_5\omega_1 + b_6\omega_2 + b_7\omega_2)\theta^2 \\
&= (a_0 + a_2) + (-b_0 - b_2)\theta^2 + (a_1 + a_3)\theta^4 + (-b_1 - b_3)\theta^6 \\
&\quad +(a_4 + a_5)\omega_1 + (-b_4 - b_5)\omega_1\theta^2 + (a_6 - b_6)\omega_2 + (a_7 - b_7)\omega_3 \\
&\equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}.
\end{aligned}$$

Como $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_3\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $a_i, b_i \in \mathbb{Z}$, segue que os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2, donde seguem as congruências

$$\begin{cases}
a_0 + a_2 \equiv 0 \pmod 2 \\
-b_0 - b_2 \equiv 0 \pmod 2 \\
a_1 + a_3 \equiv 0 \pmod 2 \\
-b_1 - b_3 \equiv 0 \pmod 2 \\
a_4 + a_5 \equiv 0 \pmod 2 \\
-b_4 - b_5 \equiv 0 \pmod 2 \\
a_6 - b_6 \equiv 0 \pmod 2 \\
a_7 - b_7 \equiv 0 \pmod 2
\end{cases}$$

E essas congruências fornece as seguintes relações

$$\begin{cases}
a_0 \equiv -a_2 \pmod 2 \\
b_0 \equiv -b_2 \pmod 2 \\
a_1 \equiv -a_3 \pmod 2 \\
b_1 \equiv -b_3 \pmod 2 \\
a_4 \equiv -a_5 \pmod 2 \\
b_4 \equiv -b_5 \pmod 2 \\
a_6 \equiv b_6 \pmod 2 \\
a_7 \equiv b_7 \pmod 2.
\end{cases} \tag{3.44}$$

Como o Sistema (3.44) contém as mesmas congruências módulo 2 que o Sistema (3.41), ao efetuar os produtos obteremos as congruências módulo 4 contidas no Sistema (3.42) onde é válida a Observação 3.6. Substituindo essas congruências na Equação (3.43), segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= a_0^2+a_1^2\theta^4+a_0^2\theta^8+a_1^2\theta^{12}+a_4^2\omega_1^2+a_4^2\omega_1^2\theta^4+a_6^2\omega_2^2+a_7^2\omega_3^2\\
&\quad -2(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)-(b_0^2+b_1^2\theta^4+b_0^2\theta^8+b_1^2\theta^{12}\\
&\quad +b_4^2\omega_1^2+b_4^2\omega_1^2\theta^4+a_6^2\omega_2^2+a_7^2\omega_3^2-2(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^4\\
&\quad -a_6a_7\omega_2\omega_3))\theta^2\\
&\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}})\\
&= (1+\theta^8)(a_0^2+a_1^2\theta^4)+\omega_1^2(1+\theta^4)a_4^2+(1-\theta^2)(a_6^2\omega_2^2+a_7^2\omega_3^2)\\
&\quad -2(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)-[(1+\theta^8)(b_0^2+b_1^2\theta^4)\\
&\quad +\omega_1^2(1+\theta^4)b_4^2-2(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)]\theta^2\\
&\equiv 0\ (mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Sabemos que $1+\theta^8=2\omega_1$, $\omega_1^2=2\omega_2$ e, além disso, $(1-\theta^2)(a_6^2\omega_2^2+a_7^2\omega_3^2)=2(a_6^2\omega_2-a_6^2\omega_3)$. Assim, todos os termos estão multiplicados por 2, de modo que podemos reduzir a congruência, pois $2x\equiv 0\ (mod\ 4)\Rightarrow x\equiv 0\ (mod\ 2)$, donde segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \omega_1(a_0^2+a_1^2\theta^4)+\omega_2a_4^2+a_6^2\omega_2-a_6^2\omega_3\\
&\quad -(a_0^2\theta^4+a_1^2\theta^8+a_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)\\
&\quad -[\omega_1(b_0^2+b_1^2\theta^4)+\omega_2b_4^2-(b_0^2\theta^4+b_1^2\theta^8+b_4^2\omega_1^2\theta^4-a_6a_7\omega_2\omega_3)]\theta^2\\
&\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Usando novamente que $\theta^8\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$, que $\omega_1\theta^4\equiv\omega_1\ (mod\ 2\mathcal{O}_{\mathbb{K}})$, que $\omega_2\theta^2\equiv\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})$, que $\omega_3\theta^2\equiv\omega_3(mod\ 2\mathcal{O}_{\mathbb{K}})$, que $\omega_2\omega_3\theta^2\equiv\omega_2\omega_3(mod\ 2\mathcal{O}_{\mathbb{K}})$ e que $x^2\equiv x\ (mod\ 2)$, segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \omega_1(a_0+a_1)+a_4\omega_2+a_6\omega_2-a_6\omega_3-(a_0\theta^4+a_1+a_4\omega_1)\\
&\quad -[\omega_1(b_0+b_1\theta^4)+\omega_2b_4-(b_0\theta^4+b_1+b_4\omega_1)]\theta^2\\
&\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}),
\end{aligned}$$

ou seja,

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \omega_1(a_0+a_1)+a_4\omega_2+a_6\omega_2-a_6\omega_3-(a_0\theta^4+a_1+a_4\omega_1)\\
&\quad -\omega_1\theta^2(b_0+b_1)-\omega_2b_4+b_0\theta^6+b_1\theta^2+b_4\omega_1\theta^2\\
&\equiv 0\ (mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Como $\{1, \theta^2, \theta^4, \theta^6, \omega_1, \omega_1\theta^2, \omega_2, \omega_3\}$ é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$, os coeficientes dessa combinação linear devem ser congruentes a 0 módulo 2. Logo, segue que

$$\begin{cases} -a_1 \equiv 0 \ (mod\ 2) \\ b_1 \equiv 0 \ (mod\ 2) \\ -a_0 \equiv 0 \ (mod\ 2) \\ b_0 \equiv 0 \ (mod\ 2) \\ a_0 + a_1 - a_4 \equiv 0 \ (mod\ 2) \\ -b_0 - b_1 + b_4 \equiv 0 \ (mod\ 2) \\ a_4 - b_4 + a_6 \equiv 0 \ (mod\ 2) \\ -a_6 \equiv 0 \ (mod\ 2). \end{cases} \tag{3.45}$$

A única solução que satisfaz simultaneamente os Sistemas (3.41) e (3.45) é $a_i, b_i \equiv 0(mod\ 2)$, para $0 \leq i \leq 6$. Desse modo, só falta determinar a paridade de a_7 e b_7, a qual sabemos ser a mesma pelo Sistema (3.41).

(I) a_7 e b_7 são pares. Neste caso, todos os inteiros a_i e b_i são pares, de modo que existem inteiros a'_i e b'_i tais que $a_i = 2a'_i$ e $b_i = 2b'_i$, $0 \leq i \leq 7$. Logo,

$$\begin{aligned} \eta &= \frac{\alpha}{2} + \frac{\beta}{2}\theta = \frac{a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + a_4\omega_1 + a_5\omega_1\theta^2 + a_6\omega_2 + a_7\omega_3}{2} \\ &\quad + \frac{(b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + b_4\omega_1 + b_5\omega_1\theta^2 + b_6\omega_2 + b_7\omega_3)\theta}{2} \\ &= \frac{2a'_0 + 2a'_1\theta^2 + 2a'_2\theta^4 + 2a'_3\theta^6 + 2a'_4\omega_1 + 2a'_5\omega_1\theta^2 + 2a'_6\omega_2 + 2a'_7\omega_3}{2} \\ &\quad + \frac{(2b'_0 + 2b'_1\theta^2 + 2b'_2\theta^4 + 2b'_3\theta^6 + 2b'_4\omega_1 + 2b'_5\omega_1\theta^2 + 2b'_6\omega_2 + 2b'_7\omega_3)\theta}{2} \\ &= a'_0 + a'_1\theta^2 + a'_2\theta^4 + a'_3\theta^6 + a'_4\omega_1 + a'_5\omega_1\theta^2 + a'_6\omega_2 + a'_7\omega_3 \\ &\quad + (b'_0 + b'_1\theta^2 + b'_2\theta^4 + b'_3\theta^6 + b'_4\omega_1 + b'_5\omega_1\theta^2 + b'_6\omega_2 + b'_7\omega_3)\theta. \end{aligned}$$

Dessa forma, $\eta \in \langle 1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_3\theta \rangle$, ou seja, $\eta \in \mathcal{O}_\mathbb{K}[\theta]$, e recaímos no caso anterior expresso no item 4.

(II) a_7 e b_7 são ímpares. Neste caso, existem inteiros a'_i e b'_i tais que $a_i = 2a'_i$ e $b_i = 2b'_i$, para todo $0 \leq i \leq 6$ e $a_7 = 2a'_7 + 1$ e $b_7 = 2b'_7 + 1$. Dessa forma,

$$\begin{aligned}
\eta &= \frac{\alpha}{2}+\frac{\beta}{2}\theta = \frac{a_0+a_1\theta^2+a_2\theta^4+a_3\theta^6+a_4\omega_1+a_5\omega_1\theta^2+a_6\omega_2+a_7\omega_3}{2}\\
&\quad +\frac{(b_0+b_1\theta^2+b_2\theta^4+b_3\theta^6+b_4\omega_1+b_5\omega_1\theta^2+b_6\omega_2+b_7\omega_3)\theta}{2}\\
&= +\frac{2a_0'+2a_1'\theta^2+2a_2'\theta^4+2a_3'\theta^6+2a_4'\omega_1+2a_5'\omega_1\theta^2+2a_6'\omega_2+(2a_7'+1)\omega_3}{2}\\
&\quad +\frac{(2b_0'+2b_1'\theta^2+2b_2'\theta^4+2b_3'\theta^6+2b_4'\omega_1+2b_5'\omega_1\theta^2+2b_6'\omega_2+(2b_7'+1)\omega_3)\theta}{2}\\
&= a_0'+a_1'\theta^2+a_2'\theta^4+a_3'\theta^6+a_4'\omega_1+a_5'\omega_1\theta^2+a_6'\omega_2+(a_7'+\tfrac{1}{2})\omega_3+b_0'+b_1'\theta^2\\
&\quad +b_2'\theta^4+b_3'\theta^6+b_4'\omega_1+b_5'\omega_1\theta^2+b_6'\omega_2+(b_7'+\tfrac{1}{2})\omega_3)\theta\\
&= a_0'+a_1'\theta^2+a_2'\theta^4+a_3'\theta^6+a_4'\omega_1+a_5'\omega_1\theta^2+a_6'\omega_2+a_7'\omega_3+b_0'\theta+b_1'\theta^3\\
&\quad +b_2'\theta^5+b_3'\theta^7+b_4'\omega_1\theta+b_5'\omega_1\theta^3+b_6'\omega_2\theta+b_7'\omega_3\theta+\tfrac{(1+\theta)}{2}\omega_3.
\end{aligned}$$

Como $\omega_4 = \frac{(1+\theta)}{2}\omega_3$, então $\eta \in \langle 1,\theta,\ldots,\theta^7,\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_2,\omega_2\theta,\omega_3,\omega_3\theta,\omega_4\rangle$. Mas $\omega_3\theta = 2\omega_4-\omega_3$, de modo que $\eta \in \langle 1,\theta,\theta^2,\ldots,\theta^7,\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_2,\omega_2\theta,\omega_3,\omega_4\rangle$, donde segue a inclusão $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[1,\theta,\theta^2,\ldots,\theta^7,\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_2,\omega_2\theta,\omega_3,\omega_4]$.

b) $\mathbb{Z}[1,\theta,\theta^2,\ldots,\theta^7,\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_2,\omega_2\theta,\omega_3,\omega_3\theta,\omega_4] \subset \mathcal{O}_{\mathbb{L}}$. Neste caso, os elementos θ, ω_1,ω_2 e ω_3 são inteiros em $\mathbb{L}$, de tal maneira que falta apenas mostrar que ω_4 também o é para concluirmos a inclusão. Como nas seções anteriores, mostraremos que a norma e o traço de ω_4 estão em $\mathcal{O}_{\mathbb{K}}$, de onde a partir da Proposição 1.7, segue que $\omega_4 \in \mathcal{O}_{\mathbb{L}}$. De fato,

$$\begin{aligned}
Tr(\omega_4) &= \omega_4+\sigma_8(\omega_4) = \omega_1\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}\right)\\
&\quad +\omega_1\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1-\theta}{2}\right)\\
&= \omega_1\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}+\tfrac{1-\theta}{2}\right) = \omega_3 \in \mathcal{O}_{\mathbb{K}}.\\
N(\omega_4) &= \omega_4.\sigma_8(\omega_4) = \omega_1\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}\right).\omega_1\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1-\theta}{2}\right)\\
&= \tfrac{1}{8}\omega_3\omega_1\left(\tfrac{1-\theta^8}{2}\right) = \tfrac{1}{8}\omega_3\omega_1(-\omega_1+1) = k\omega_3 \in \mathcal{O}_{\mathbb{K}},
\end{aligned}$$

pois

$$\left(\frac{1+\theta^4}{2}\right)\left(\frac{1+\theta^2}{2}\right)\left(\frac{1+\theta}{2}\right)\left(\frac{1-\theta}{2}\right) = \frac{1-\theta^8}{16} = \frac{1}{8}(1-\omega_1)$$

e

$$\omega_1(-\omega_1+1) = \frac{1+\theta^8}{2}\frac{1-\theta^8}{2} = \frac{1-\theta^{16}}{4} = \frac{1-d}{4} = -8k,$$

já que $d \equiv 1(mod\ 32)$ implica que $\frac{d-1}{4} = 8k$. Desse fato, segue a inclusão

$$\mathbb{Z}[1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_3\theta, \omega_4] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto,

$$\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[1, \theta, \theta^2, \ldots, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_3, \omega_3\theta, \omega_4].$$

Com isso, concluímos a prova do teorema. □

3.3.2 Discriminante

Nesta seção, consideramos $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[16]{d}$, com $d \neq 1$ um inteiro livre de quadrados.

Teorema 3.7. *O discriminante do anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ de $\mathbb{L}$ é dado por*

$$D(\mathbb{L}) = \begin{cases} -16^{16}d^{15}, \text{ se } d \not\equiv 1(mod\ 4) \\ -2^{48}d^{15}, \text{ se } d \equiv 5(mod\ 8) \\ -2^{40}d^{15}, \text{ se } d \equiv 9(mod\ 16) \\ -2^{36}d^{15}, \text{ se } d \equiv 17(mod\ 32) \\ -2^{34}d^{15}, \text{ se } d \equiv 1(mod\ 32). \end{cases}$$

Demonstração. O primeiro caso, $d \not\equiv 1(mod\ 4)$, segue diretamente da Proposição 2.4, pois para $n = 16$ a expressão obtida a partir de $D(\mathbb{L}) = -n^n d^{n-1}$ é $D(\mathbb{L}) = -16^{16}d^{15}$. Para os demais casos, procedemos a partir da Definição 1.32, do mesmo modo que fizemos na prova dos Teoremas 3.2 e 3.4. Se $d \equiv 5(mod\ 8)$, segue pelo Teorema 3.5 que $\mathcal{O}_{\mathbb{L}} = \langle 1, \theta, \ldots, \theta^7, \frac{1+\theta^4}{2}, \frac{\theta+\theta^5}{2}, \ldots, \frac{\theta^7+\theta^{15}}{2} \rangle$, e assim, pela Definição 1.32, considerando $d = \theta^{16}$, e substituindo os valores dos traços que constam no Lema 1.37, segue que

$$D_{\mathbb{L}}\left(1, \theta, \ldots, \theta^7, \frac{1+\theta^8}{2}, \frac{\theta+\theta^9}{2}, \frac{\theta^2+\theta^{10}}{2}, \frac{\theta^3+\theta^{11}}{2}, \ldots, \frac{\theta^7+\theta^{15}}{2}\right) = -2^{42}d^{14}2^6 d = -2^{48}d^{15}.$$

Seguindo o mesmo raciocínio, se $d \equiv 9(mod\ 16)$, segue que

$$D_{\mathbb{L}}\left(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_2, \omega_2\theta, \omega_2\theta^2, \omega_2\theta^3\right) = -2^{34}d^{14}2^6 d = -2^{40}d^{15}.$$

Agora, se $d \equiv 17(mod\ 32)$, segue que

$$D_{\mathbb{L}}\left(1,\theta,\theta^2,\theta^3,\theta^4,\theta^5,\theta^6,\theta^7,\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_2,\omega_2\theta,\omega_3,\omega_3\theta\right) = -2^{30}d^{14}2^6d = -2^{36}d^{15}.$$

Finalmente, se $d \equiv 1(mod\ 32)$, segue que

$$D_{\mathbb{L}}\left(1,\theta,\theta^2,\theta^3,\theta^4,\theta^5,\theta^6,\theta^7,\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_2,\omega_2\theta,\omega_3,\omega_4\right) = -2^{28}d^{14}2^6d = -2^{34}d^{15},$$

o que prova o teorema. □

3.4 Base integral e discriminante do corpo puro de grau 32

Pelos Teoremas 3.1, 3.3 e 3.5 é possível induzir uma base integral para o corpo $\mathbb{Q}(\sqrt[32]{d})$, onde $d \neq 1$ é inteiro livre de quadrados. Nesta seção iremos apenas enunciar o teorema que descreve uma base em todos os seus casos e, consequentemente, o seu discriminante.

Teorema 3.8. *Seja $\mathbb{L} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[32]{d}$, com $d \neq 1$ inteiro e livre de quadrados. Uma base integral de $\mathbb{L}$ é dada por*

1. $\{1,\theta,\theta^2,\ldots,\theta^{31}\}$ *se* $d \equiv 2,3(mod\ 4)$
2. $\{1,\theta,\theta^2,\ldots,\theta^{15},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{15}\}$, *se* $d \equiv 5(mod\ 8)$
3. $\{1,\theta,\theta^2,\ldots,\theta^{15},\omega_1,\omega_1\theta,\omega_1\theta^2,\ldots,\omega_1\theta^7,\omega_2,\omega_2\theta,\omega_2\theta^2,\ldots\omega_2\theta^7\}$, *se* $d \equiv 9(mod\ 16)$
4. $\{1,\theta,\theta^2,\ldots,\theta^{15},\omega_1,\omega_1\theta,\omega_1\theta^2,\ldots,\omega_1\theta^7,\omega_2,\omega_2\theta,\omega_2\theta^2,\omega_2\theta^3,\omega_3,\omega_3\theta,\omega_3\theta^2,\omega_3\theta^3\}$, *se* $d \equiv 17(mod\ 32)$
5. $\{1,\theta,\theta^2,\ldots,\theta^{15},\omega_1,\omega_1\theta,\omega_1\theta^2,\ldots,\omega_1\theta^7,\omega_2,\omega_2\theta,\omega_2\theta^2,\omega_2\theta^3,\omega_3,\omega_3\theta,\omega_4,\omega_4\theta\}$, *se* $d \equiv 33(mod\ 64)$
6. $\{1,\theta,\theta^2,\ldots,\theta^{15},\omega_1,\omega_1\theta,\omega_1\theta^2,\ldots,\omega_1\theta^7,\omega_2,\omega_2\theta,\omega_2\theta^2,\omega_2\theta^3,\omega_3,\omega_3\theta,\omega_4,\omega_5\}$, *se* $d \equiv 1(mod\ 64)$,

onde $\omega_1 = \frac{1+\theta^{16}}{2}, \omega_2 = \frac{1+\theta^8+\theta^{16}+\theta^{24}}{4}, \omega_3 = \frac{1+\theta^4+\theta^8+\theta^{12}+\theta^{16}+\theta^{20}+\theta^{24}+\theta^{28}}{8}$,
$\omega_4 = \frac{1+\theta^2+\theta^4+\theta^6+\theta^8+\theta^{10}+\theta^{12}+\theta^{14}+\theta^{16}+\theta^{18}+\theta^{20}+\theta^{22}+\theta^{24}+\theta^{26}+\theta^{28}+\theta^{30}}{16}$ *e*
$\omega_5 = \frac{1+\theta+\theta^2+\theta^3+\theta^4++\ldots+\theta^{28}+\theta^{29}+\theta^{30}+\theta^{31}}{32}$.

A partir do Teorema 3.8 e da Definição 1.33, podemos determinar o discriminante do anel de inteiros algébricos de $\mathbb{L}$ referente a cada uma dessas bases.

Teorema 3.9. *Seja $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[32]{d}$ com $d \neq 1$ é um inteiro livre de quadrados. O discriminante do anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ de $\mathbb{L}$ é dado por*

$$D(\mathbb{L}) = \begin{cases} -32^{32}d^{32}, \text{ se } d \not\equiv 1(mod\ 4) \\ -2^{128}d^{32}, \text{ se } d \equiv 5(mod\ 8) \\ -2^{112}d^{32}, \text{ se } d \equiv 9(mod\ 16) \\ -2^{104}d^{32}, \text{ se } d \equiv 17(mod\ 32) \\ -2^{100}d^{32}, \text{ se } d \equiv 33(mod\ 64) \\ -2^{98}d^{32}, \text{ se } d \equiv 1(mod\ 64). \end{cases}$$

3.5 Considerações finais

No decorrer deste capítulo, foi possível notar que o anel de inteiros algébricos de cada corpo cujo grau é uma potência de 2 possui um certo padrão em sua formação, tanto na quantidade de casos diferentes de acordo com o grau, mais precisamente o valor da potência de 2 mas, também, nos elementos que o compõem. À vista disso, os próximos capítulos buscam estender esses resultados e apresentar fórmulas que descrevam uma base integral e o discriminante do anel de inteiros algébricos dos corpos puros cujo grau é uma potência de 2 e $d \neq 1$ é um inteiro livre de quadrados. Visando cumprir esse objetivo, faremos uma divisão da prova geral em 3 etapas, expressas nos capítulos a seguir. Primeiro, olhamos apenas para os corpos $\mathbb{Q}(\sqrt[2^k]{d})$ onde d satisfaz $d \equiv 5(mod\ 8)$ e obtemos uma base integral e o discriminante a ela associado. Depois, centralizamos os nosso estudos para o caso em que $d \equiv 9(mod\ 16)$ e, por fim, no último capítulo, generalizamos para as demais congruências de d.

4 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \equiv 5(mod\ 8)$

Neste capítulo, o nosso objetivo é determinar uma base integral do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \equiv 5(mod\ 8)$ ou, equivalentemente, $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$, onde $d \neq 1$ é um inteiro livre de quadrados e $k \geq 2$. Também, a partir desta base, calculamos o discriminante do anel de inteiros algébricos do corpo. Os casos particulares para os corpos de graus 4, 8 e 16 já foram feitos em detalhes no capítulo anterior e, agora, generalizamos este resultado para todo corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é inteiro livre de quadrados e $k \geq 2$.

4.1 Anel de inteiros algébricos

Observando as demonstrações feitas nos Teoremas 3.1, 3.3 e 3.5, podemos notar algumas semelhanças entre elas, sendo a principal, o uso da base integral do corpo cujo grau é a potência de 2 anterior. Considerando cada anel de inteiros algébricos descrito nos teoremas mencionados, restringindo o nosso olhar ao caso $d \equiv 1 \pmod 4$, também é possível notar semelhanças na estrutura dessas bases. Recordamos sua forma para cada grau visto até aqui:

1. uma base integral do corpo de grau 2 é dada por $\{1, \frac{1+\theta}{2}\}$;
2. para o corpo de grau 4, uma base pode ser expressa por $\{1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}\}$;
3. já no caso de grau 8, escrevemos $\{1, \theta, \theta^2, \theta^3, \frac{1+\theta^4}{2}, \frac{\theta+\theta^5}{2}, \frac{\theta^2+\theta^6}{2}, \frac{\theta^3+\theta^7}{2}\}$;
4. finalmente, para o grau 16, obtemos $\{1, \theta, \theta^2, \ldots, \theta^7, \frac{1+\theta^4}{2}, \frac{\theta+\theta^5}{2}, \frac{\theta^2+\theta^6}{2}, \ldots, \frac{\theta^7+\theta^{15}}{2}\}$.

Note que, chamando n ao grau do corpo, se considerarmos $\omega = \frac{1+\theta^{\frac{n}{2}}}{2}$ (note que está de acordo com a expressão que foi definida em cada seção do Capítulo 3 considerando o valor de n como o do grau em questão), é possível escrever essas bases de maneira bem similar umas às outras. Respaldando-nos nesses fatos, enunciamos e provamos o Teroema 4.2. Vale ressaltar também que, no decorrer das provas dos Teoremas 3.1, 3.3 e 3.5 fizemos

o uso de algumas congruências e igualdades, as quais são válidas para todos os graus, conforme a seguinte proposição.

Proposição 4.1. *Seja* $\mathbb{L} = \mathbb{Q}(\theta)$, *com* $\theta = \sqrt[2^k]{d}$, $k \geq 3$, *onde* $d \neq 1$ *é um inteiro livre de quadrados tal que* $d \equiv 5(mod\ 8)$ *e seja* $\mathbb{K} = \mathbb{Q}(\theta^2)$. *Se* $\omega = \frac{1+\theta^{2^{k-1}}}{2}$, *então são válidas as seguintes igualdades e congruências:*

1. $2\omega = 1 + \theta^{2^{k-1}}$
2. $\theta^{2^{k-1}} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$
3. $\omega^2 \equiv \omega + 1(mod\ 2\mathcal{O}_{\mathbb{K}})$
4. $\omega\theta^{2^k} = \omega + 2m \equiv \omega(mod\ 2\mathcal{O}_{\mathbb{K}})$
5. $\omega^3 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$.

Demonstração. Considere os dados da hipótese.

1. A igualdade $2\omega = 1 + \theta^{2^{k-1}}$ é obtida diretamente da definição de ω.
2. Uma vez que $2\omega \in 2\mathcal{O}_{\mathbb{K}}$, a partir do item 1, segue que $\theta^{2^{k-1}} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$.
3. Como $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$, segue que existe $m \in \mathbb{Z}$ ímpar tal que $d - 1 = 4m$, e logo, $\frac{d-1}{4} = m$. Usando a definição de ω, segue que

$$\begin{aligned}\omega^2 &= \left(\frac{1+\theta^{2^{k-1}}}{2}\right)^2 = \frac{1+2\theta^{2^{k-1}}+\theta^{2^k}}{4} = \frac{2-1+2\theta^{2^{k-1}}+d}{4} = \frac{2+2\theta^{2^{k-1}}}{4} + \frac{d-1}{4} = \frac{1+\theta^{2^{k-1}}}{2} + m \\ &= \omega + m \quad \equiv \quad \omega + 1(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

4. Da definição de ω, segue que

$$\omega\theta^{2^{k-1}} = \frac{1+\theta^{2^{k-1}}}{2}\theta^{2^{k-1}} = \frac{\theta^{2^{k-1}}+\theta^{2^k}}{2} = \frac{\theta^{2^{k-1}}+d}{2}.$$

   Por outro lado,

$$\omega + 2m = \frac{1+\theta^{2^{k-1}}}{2} + \frac{d-1}{2} = \frac{\theta^{2^{k-1}}+d}{2}.$$

   Das duas expressões, segue a igualdade. Além disso, como $2m \in 2\mathbb{Z} \subset 2\mathcal{O}_{\mathbb{K}}$, segue que $\omega\theta^{2^{k-1}} \equiv \omega \pmod{2\mathcal{O}_{\mathbb{K}}}$.

5. Utilizando o item 3, segue que

$$\omega^3 = \omega^2\omega = (\omega + m)\omega = \omega^2 + m\omega = \omega + m + m\omega \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}),$$

o que prova a proposição. □

Antes de enunciar o próximo Teorema, vale destacar que no corpo de grau 2, o qual é o corpo de menor grau em que levamos em consideração a congruência $d \equiv 1(mod\ 4)$ para definir uma base, pelo fato de que nesse corpo o 4 é a maior potência de 2 que tal que $d \equiv 1(mod\ 4)$ que interfere na estrutura do anel de inteiros algébricos, a maneira de demonstrar uma base se difere um pouco da prova a seguir. No caso de grau 4, o expoente da potência de 2 do grau e da congruência é o mesmo e veremos nos capítulos seguintes que esse fato também gera uma particularidade na demonstração. O mesmo acontece para o caso de grau 8, cujo expoente da potência de 2 tem uma unidade a mais do que a potência da congruência. (esses fatos ficarão claros no decorrer da demonstração do Teorema 6.9). Desse modo, os passos utilizados na demonstração abaixo são válidos para corpos que possuem grau acima de 16, partindo da base integral do corpo de grau 8, porém a validade do Teorema para qualquer potência de 2 não é comprometida, uma vez que os casos particulares já foram feitos.

Teorema 4.2. *Seja* $\mathbb{L} = \mathbb{Q}(\theta)$*, com* $\theta = \sqrt[2^k]{d}$*,* $d \neq 1$ *um inteiro e livre de quadrados e* $k \geq 1$*. Se* $k = 1$ *e* $d \equiv 1(mod\ 4)$ *e se* $k \geq 2$ *e* $d \equiv 5(mod\ 8)$*, sendo* $\mathcal{O}_{\mathbb{L}}$ *o seu anel de inteiros algébricos, então* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4 + \mathbb{Z}\theta^5 + \ldots + \mathbb{Z}\theta^{2^{k-1}-1} + \mathbb{Z}\omega + \mathbb{Z}\omega\theta + \mathbb{Z}\omega\theta^2 + \mathbb{Z}\omega\theta^3 + \mathbb{Z}\omega\theta^4 + \mathbb{Z}\omega\theta^5 + \ldots + \mathbb{Z}\omega\theta^{2^{k-1}-1}$*, onde* $\omega = \frac{1+\theta^{2^{k-1}}}{2}$*. Em outros termos,*

$$\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \ldots \theta^{2^{k-1}-1}, \omega, \omega\theta, \omega\theta^2, \omega\theta^3, \omega\theta^4, \omega\theta^5, \ldots \omega\theta^{2^{k-1}-1}\}$$

é uma base integral do corpo $\mathbb{L}$*.*

Demonstração. Esta prova será feita pelo Princípio da Indução Finita sobre k, ou seja, sobre o expoente do grau $n = 2^k$. Como as provas para os casos $k = 1$ e $k = 2$ já foram feitas, consideraremos $k \geq 3$.

1) *Passo base:* O resultado vale para o valor inicial $k = 3$, ou seja, para grau $n = 8$, conforme visto no Teorema 3.3.

2) *Hipótese de Indução:* Suponhamos que o resultado é verdadeiro para k, ou seja, para grau $n = 2^k$. Logo, uma base do anel de inteiros algébricos de $\mathbb{Q}(\theta)$, com $\theta = \sqrt[2^k]{d}$ é $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \ldots \theta^{2^{k-1}-1}, \omega, \omega\theta, \omega\theta^2, \omega\theta^3, \omega\theta^4, \omega\theta^5, \ldots \omega\theta^{2^{k-1}-1}\}$, onde $\omega = \frac{1+\theta^{2^{k-1}}}{2}$.

3) Provemos que o resultado é válido para $k + 1$, ou seja, para $n = 2^{k+1}$. Isso implica que uma base do anel de inteiros algébricos de $\mathbb{Q}(\theta)$, com $\theta = \sqrt[2^{k+1}]{d}$ é

$$\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \ldots \theta^{2^k-1}, \omega, \omega\theta, \omega\theta^2, \omega\theta^3, \omega\theta^4, \omega\theta^5, \ldots \omega\theta^{2^k-1}\},$$

onde $\omega = \frac{1+\theta^{2^k}}{2}$.

Chamando $\mathbb{L}$ ao corpo de grau 2^{k+1}, isto é, $\mathbb{L} = \mathbb{Q}(\sqrt[2^{k+1}]{d})$, $\mathbb{K}$ ao corpo de grau 2^k, ou seja, $\mathbb{K} = \mathbb{Q}(\sqrt[2^k]{d})$ e $\theta = \sqrt[2^{k+1}]{d}$, segue que $\mathbb{L} = \mathbb{Q}(\theta)$ e $\mathbb{K} = \mathbb{Q}(\theta^2)$. Atendendo a essa notação, note que, como $\mathbb{Z}[1, \theta, \theta^2, \ldots, \theta^{2^k-1}, \omega, \omega\theta, \omega\theta^2, \ldots, \omega\theta^{2^k-1}] = \mathcal{O}_{\mathbb{K}}[\theta]$, é suficiente mostrar que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$, onde ressaltamos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1, \theta^2, \theta^4, \ldots, \theta^{2^k-2}, \omega, \omega\theta^2, \omega\theta^4, \ldots, \omega\theta^{2^k-2}]$, com $\omega = \frac{1+\theta^{2^k}}{2}$, devido à forma que definimos θ. À vista disso, a prova consiste em verificar essas duas inclusões.

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Como $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tal que $2\eta = \alpha + \beta\theta$ e, logo,

$$\alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{4.1}$$

Como $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ e, pela Hipótese de Indução, o conjunto $\{1, \theta^2, \theta^4, \theta^6, \ldots, \theta^{2^k-2}, \omega, \omega\theta^2, \omega\theta^4, \omega\theta^6, \ldots \omega\theta^{2^k-2}\}$, com $\omega = \frac{1+\theta^{2^k}}{2}$, é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, existem inteiros a_i, b_i, onde $0 \leq i \leq 2^k - 1$, tais que

$$\begin{cases} \alpha &= a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + \cdots + a_{2^{k-1}-1}\theta^{2^k-2} + a_{2^{k-1}}\omega + a_{2^{k-1}+1}\omega\theta^2 \\ &\quad + a_{2^{k-1}+2}\omega\theta^4 + \ldots + a_{2^k-1}\omega\theta^{2^k-2} \\ \beta &= b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + \ldots + b_{2^{k-1}-1}\theta^{2^k-2} + b_{2^{k-1}}\omega + b_{2^{k-1}+1}\omega\theta^2 \\ &\quad + b_{2^{k-1}+2}\omega\theta^4 + \ldots + b_{2^k-1}\omega\theta^{2^k-2}. \end{cases}$$

Substituindo esses valores na Equação (4.1), obtemos

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\theta^{16} + \ldots + (a_{2^{k-1}-1})^2\theta^{2^{k+1}-4} \\ &\quad + (a_{2^{k-1}})^2\omega^2 + (a_{2^{k-1}+1})^2\omega^2\theta^4 + (a_{2^{k-1}+2})^2\omega^2\theta^8 + \ldots \\ &\quad + (a_{2^k-1})^2\omega^2\theta^{2^{k+1}-4} + 2(a_{ij}) - (b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^{12} + b_4^2\theta^{16} + \ldots \\ &\quad + (b_{2^{k-1}-1})^2\theta^{2^{k+1}-4} + (b_{2^{k-1}})^2\omega^2 + (b_{2^{k-1}+1})^2\omega^2\theta^4 + (b_{2^{k-1}+2})^2\omega^2\theta^8 \\ &\quad + \ldots + (b_{2^k1})^2\omega^2\theta^{2^{k+1}-4} + 2(b_{ij}))\theta^2 \\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}), \end{aligned} \tag{4.2}$$

onde a_{ij} representa a soma de todas as multiplicações de a_ix por a_jy, com $0 \leq i \leq 2^k - 2$ e $i < j$, e b_{ij} representa a soma de todas as multiplicações de b_ix por b_jy, com $0 \leq i \leq 2^k - 2$ e $i < j$ (note que $i < j \Rightarrow x \neq y$). Neste caso, podemos representar esses valores através das seguintes expressões

$$\begin{aligned} a_{ij} &= \sum_{i_1=0}^{2^{k-1}-2}\sum_{i_2=i_1+1}^{2^{k-1}-1} a_{i_1}a_{i_2}\theta^{2i_1+2i_2} + \sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=2^{k-1}}^{2^k-1} a_{i_1}a_{i_2}\omega\theta^{2i_1+2(i_2-2^{k-1})} \\ &\quad + \sum_{i_1=2^{k-1}}^{2^k-2}\sum_{i_2=i_1+1}^{2^k-1} a_{i_1}a_{i_2}\omega^2\theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1})}, \end{aligned} \tag{4.3}$$

$$\begin{aligned} b_{ij} &= \sum_{i_1=0}^{2^{k-1}-2}\sum_{i_2=i_1+1}^{2^{k-1}-1} b_{i_1}b_{i_2}\theta^{2i_1+2i_2} + \sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=2^{k-1}}^{2^k-1} b_{i_1}b_{i_2}\omega\theta^{2i_1+2(i_2-2^{k-1})} \\ &\quad + \sum_{i_1=2^{k-1}}^{2^k-2}\sum_{i_2=i_1+1}^{2^k-1} b_{i_1}b_{i_2}\omega^2\theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1})}. \end{aligned} \tag{4.4}$$

Reescrevendo a Equação (4.2) em termos da congruência módulo 2, segue que

$$\begin{aligned} \alpha^2-\beta^2\theta^2 &= a_0^2+a_1^2\theta^4+a_2^2\theta^8+a_3^2\theta^{12}+a_4^2\theta^{16}+\ldots+(a_{2^{k-1}-1})^2\theta^{2^{k+1}-4} \\ &\quad +(a_{2^{k-1}})^2\omega^2+(a_{2^{k-1}+1})^2\omega^2\theta^4+(a_{2^{k-1}+2})^2\omega^2\theta^8+\ldots \\ &\quad +(a_{2^k-1})^2\omega^2\theta^{2^{k+1}-4}-(b_0^2+b_1^2\theta^4+b_2^2\theta^8+b_3^2\theta^{12} \\ &\quad +b_4^2\theta^{16}+\ldots+(b_{2^{k-1}-1})^2\theta^{2^{k+1}-4}+(b_{2^{k-1}})^2\omega^2 \\ &\quad +(b_{2^{k-1}+1})^2\omega^2\theta^4+(b_{2^{k-1}+2})^2\omega^2\theta^8+\ldots \\ &\quad +(b_{2^k-1})^2\omega^2\theta^{2^{k+1}-4})\theta^2 \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{4.5}$$

A fim de facilitar a escrita nos próximos passos, podemos escrever a Equação (4.5) de maneira mais sucinta, através da fórmula abaixo, a qual usaremos daqui em diante.

$$\begin{aligned} \alpha^2-\beta^2\theta^2 &= \sum_{i=0}^{2^{k-1}-1} a_i^2\theta^{4i}+\sum_{i=2^{k-1}}^{2^k-1} a_i^2\omega^2\theta^{4(i-2^{k-1})}-\sum_{i=0}^{2^{k-1}-1} b_i^2\theta^{4i+2} \\ &\quad -\sum_{i=2^{k-1}}^{2^k-1} b_i^2\omega^2\theta^{4(i-2^{k-1})+2} \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{4.6}$$

De acordo com a Proposição 4.1, são válidas as seguintes congruências

$$\begin{cases} \theta^{2^k}\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega^2\equiv\omega+1(mod\ 2\mathcal{O}_{\mathbb{K}}) \end{cases} \qquad \begin{cases} \omega\theta^{2^k}\equiv\omega(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ x^2\equiv x(mod\ 2), \end{cases}$$

para todo $x, y \in \mathbb{Z}$. Uma vez que $\alpha^2-\beta^2\theta^2 \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})$, substituindo essas

congruências na Equação (4.6), segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \sum_{i=0}^{2^{k-2}-1}(a_i+a_{i+2^{k-2}})\theta^{4i}+\sum_{i=2^{k-1}}^{3.2^{k-2}-1}(a_i+a_{i+3.2^{k-2}})(\omega+1)\theta^{4(i-2^{k-1})}\\ &\quad-\sum_{i=0}^{2^{k-2}-1}(b_i+b_{i+2^{k-2}})\theta^{4i+2}-\sum_{i=2^{k-1}}^{3.2^{k-2}-1}(b_i+b_{i+3.2^{k-2}})(\omega+1)\theta^{4(i-2^{k-1})+2}\\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}),\end{aligned} \tag{4.7}$$

pois as substituições ocorrem no termo médio de cada somatório. Assim, obtemos os novos limites superiores dos somatórios expressos na Equação (4.7) calculando o ponto médio entre os limites inferior e superior de cada somatório da Equação (4.6). Agrupando os termos semelhantes na Equação (4.7), obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= (a_0+a_{2^{k-2}}+a_{2^{k-1}}+a_{3.2^{k-2}})+(a_{2^{k-1}}+a_{3.2^{k-2}})\omega\\ &\quad+(a_1+a_{2^{k-2}+1}+a_{2^{k-1}+1}+a_{3.2^{k-2}+1})\theta^4+(a_{2^{k-1}+1}+a_{3.2^{k-2}+1})\omega\theta^4\\ &\quad+(a_2+a_{2^{k-2}+2}+a_{2^{k-1}+2}+a_{3.2^{k-2}+2})\theta^8+(a_{2^{k-1}+2}+a_{3.2^{k-2}+2})\omega\theta^8\\ &\quad+(a_3+a_{2^{k-2}+3}+a_{2^{k-1}+3}+a_{3.2^{k-2}+3})\theta^{12}+(a_{2^{k-1}+3}+a_{3.2^{k-2}+3})\omega\theta^{12}\\ &\quad+\ldots+(a_{2^{k-2}-1}+a_{2^{k-1}-1}+a_{3.2^{k-2}-1}+a_{2^k-1})\theta^{2^k-4}\\ &\quad+(a_{3.2^{k-2}-1}+a_{2^k-1})\omega\theta^{2^k-4}-[(b_0+b_{2^{k-2}}+b_{2^{k-1}}+b_{3.2^{k-2}})\theta^2\\ &\quad+(b_{2^{k-1}}+b_{3.2^{k-2}})\omega\theta^2+(b_1+b_{2^{k-2}+1}+b_{2^{k-1}+1}+b_{3.2^{k-2}+1})\theta^6\\ &\quad+(b_{2^{k-1}+1}+b_{3.2^{k-2}+1})\omega\theta^6+(b_2+a_{2^{k-2}+2}+b_{2^{k-1}+2}+b_{3.2^{k-2}+2})\theta^{10}\\ &\quad+(b_{2^{k-1}+2}+b_{3.2^{k-2}+2})\omega\theta^{10}+(b_3+a_{2^{k-2}+3}+b_{2^{k-1}+3}+b_{3.2^{k-2}+3})\theta^{14}\\ &\quad+(b_{2^{k-1}+3}+b_{3.2^{k-2}+3})\omega\theta^{14}+\ldots+(b_{2^{k-2}-1}+b_{2^{k-1}-1}+b_{3-2^{k-2}-1}\\ &\quad+b_{2^k-1})\theta^{2^k-2}+(b_{3-2^{k-2}-1}+b_{2^k-1})\omega\theta^{2^k-2}]\\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Essa expressão fornece uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$, de modo que os coeficientes devem ser congruentes a 0 módulo 2. Desse fato obtemos as seguintes congruências, válidas para todo $0 \leq j \leq 2^{k-2}-1$.

$$\begin{cases} a_j+a_{2^{k-2}+j}+a_{2^{k-1}+j}+a_{3.2^{k-2}+j}\equiv 0(mod\ 2)\\ a_{2^{k-1}+j}+a_{3.2^{k-2}+j}\equiv 0(mod\ 2)\\ b_j+b_{2^{k-2}+j}+b_{2^{k-1}+j}+b_{3.2^{k-2}+j}\equiv 0(mod\ 2)\\ b_{2^{k-1}+j}+b_{3.2^{k-2}+j}\equiv 0(mod\ 2).\end{cases}$$

Por conseguinte, para todo $j=0,1,2,\ldots,2^{k-2}-1$, segue que

$$\begin{cases} a_j \equiv -a_{2^{k-2}+j}(mod\ 2) \\ a_{2^{k-1}+j} \equiv -a_{3.2^{k-2}+j}\ (mod\ 2) \\ b_j \equiv -b_{2^{k-2}+j}(mod\ 2) \\ b_{2^{k-1}+j} \equiv -b_{3.2^{k-2}+j}(mod\ 2). \end{cases} \tag{4.8}$$

E dessas congruências módulo 2, obtemos as seguintes congruências módulo 4

$$\begin{cases} 1.\ (a_j)^2 \equiv (a_{2^{k-2}+j})^2(mod\ 4) \\ 2.\ (a_{2^{k-1}+j})^2 \equiv (a_{3.2^{k-2}+j})^2\ (mod\ 4) \\ 3.\ a_j a_{2^{k-2}+j} \equiv -(a_j)^2(mod\ 4) \\ 4.\ a_{2^{k-1}+j} a_{3.2^{k-2}+j} \equiv -(a_{2^{k-1}+j})^2(mod\ 4) \\ 5.\ a_{j_1} a_{3.2^{k-2}+j_2} \equiv -a_{j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 6.\ a_{2^{k-2}+j_1} a_{2^{k-2}+j_2} \equiv a_{j_1} a_{j_2}(mod\ 4), j_1 \neq j_2 \\ 7.\ a_{2^{k-2}+j_1} a_{2^{k-1}+j_2} \equiv -a_{j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 8.\ a_{2^{k-2}+j_1} a_{3.2^{k-2}+j_2} \equiv a_{j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 9.\ a_{3.2^{k-2}+j_1} a_{3.2^{k-2}+j_2} \equiv a_{2^{k-1}+j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 10.\ (b_j)^2 \equiv (b_{2^{k-2}+j})^2(mod\ 4) \\ 11.\ (b_{2^{k-1}+j})^2 \equiv (b_{3.2^{k-2}+j})^2(mod\ 4) \\ 12.\ b_j b_{2^{k-2}+j} \equiv -(b_j)^2(mod\ 4) \\ 13.\ b_{2^{k-1}+j} b_{3.2^{k-2}+j} \equiv -(b_{2^{k-1}+j})^2(mod\ 4) \\ 14.\ b_{j_1} b_{3.2^{k-2}+j_2} \equiv -b_{j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 15.\ b_{2^{k-2}+j_1} b_{2^{k-2}+j_2} \equiv b_{j_1} b_{j_2}(mod\ 4), j_1 \neq j_2 \\ 16.\ b_{2^{k-2}+j_1} b_{2^{k-1}+j_2} \equiv -b_{j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 17.\ b_{2^{k-2}+j_1} b_{3.2^{k-2}+j_2} \equiv b_{j_1} a_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2 \\ 18.\ b_{3.2^{k-2}+j_1} b_{3.2^{k-2}+j_2} \equiv b_{2^{k-1}+j_1} b_{2^{k-1}+j_2}(mod\ 4), j_1 \neq j_2. \end{cases} \tag{4.9}$$

Observação 4.3. Observe que os coeficientes a_j e b_j exibidos do lado esquerdo da congruência nas equações *1* e *10* do Sistema (4.9) multiplicam θ^j e θ^{j+2}, respectivamente, na Equação (4.2), enquanto os coeficientes do lado direito das mesmas equações, multiplicam, respectivamente, θ^{j+2^k} e θ^{j+2^k+2}. Além disso, nas equações *2* e *11*, os coeficientes $a_{2^{k-1}+j}$ e $b_{2^{k-1}+j}$ escritos ao lado esquerdo, multiplicam, respectivamente, $\omega^2\theta^j$ e $\omega^2\theta^{j+2}$ na Equação (4.2), enquanto os contidos do lado direito multiplicam $\omega^2\theta^{j+2^k}$ e $\omega^2\theta^{j+2^k+2}$. Também chamamos a atenção na Equação (4.2), para os elementos que multiplicam os termos do lado direito das equações *1, 2, 10 e 11* referidas acima, pois são nesses pontos que iremos substituir os valores do Sistema (4.8) nessa equação (note que a diferença entre o expoente de θ no elemento que multiplica os coeficientes esquerdo e direito da mesma equação dentre as que mencionamos acima é sempre 2^k). Agora, as outras linhas do sistema se referem

aos termos de a_{ij} e b_{ij} descritos, respectivamente, nas Equações (4.3) e (4.4). O primeiro somatório da Equação (4.3) se escreverá em 3 somatórios após as substituiçoes contidas no sistema, pois engloba os casos: $i_1, i_2 < 2^{k-2}$, onde a_{i_1} e a_{i_2} permanecem iguais; $i_1 < 2^{k-2}$ e $i_2 \geq 2^{k-2}$, onde utilizaremos a congruência contida na linha *3*; e $i_1, i_2 \geq 2^{k-2}$, onde utilizaremos a linha *6*. O segundo somatório se dividirá em 4: $i_1 < 2^{k-2}$ e $i_2 < 3.2^{k-2}$, onde a_{i_1} e a_{i_2} permanecem iguais; $i_1 < 2^{k-2}$ e $i_2 \geq 3.2^{k-2}$, que engloba a linha *5*, $i_1 \geq 2^{k-2}$ e $i_2 < 3.2^{k-2}$ que engloba a linha *7*; e $i_1 \geq 2^{k-2}$ e $i_2 \geq 3.2^{k-2}$ que engloba a linha *8*. Por fim, seguindo a mesma ideia, o terceiro somatório também se dividirá em 3: $i_1, i_2 < 3.2^{k-2}$ onde a_{i_1} e a_{i_2} permanecem iguais; $i_1 < 3.2^{k-2}$ e $i_2 \geq 3.2^{k-2}$, onde substituiremos a congruência contida na linha *4*; e $i_1, i_2 \geq 3.2^{k-2}$ que engloba a linha *9*. O mesmo raciocínio ocorre na Equação (4.4) utilizando as congruências contidas nas demais linhas do Sistema (4.8).

Levando em consideração a análise feita na Observação (4.3), substituindo as congruências contidas no Sistema (4.9) na Equação (4.2), podemos rreescrevê-la colocando $(1+\theta^{2^k})$ em evidência, donde obtemos

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= (1+\theta^{2^k}) \sum_{i=0}^{2^{k-2}-1} a_i^2\theta^{4i} + (1+\theta^{2^k})\omega^2 \sum_{i=2^{k-1}}^{3.2^{k-2}-1} a_i\theta^{4(i-2^{k-1})} - 2a_{ij}^* \\
&\quad +(1+\theta^{2^k}) \sum_{i=0}^{2^{k-2}-1} b_i^2\theta^{4i+2} + (1+\theta^{2^k})\omega^2 \sum_{i=2^{k-1}}^{3.2^{k-2}-1} b_i\theta^{4(i-2^{k-1})+2} \\
&\quad +2b_{ij}^*\theta^2 \\
&\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}).
\end{aligned} \tag{4.10}$$

onde a_{ij}^* e b_{ij}^* são as expressões obtidas a partir das Equações (4.3) e (4.4) realizando as substituições dos termos inclusos no Sistema (4.9) seguindo o raciocínio exposto na Observação 4.3 e podem ser expressas pelas equações

$$\begin{aligned}
a_{ij}^* &= \sum_{i_1=0}^{2^{k-2}-2} \sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2i_1+2i_2} + \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=0}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2i_1+2(i_2+2^{k-2})} \\
&\quad + \sum_{i_1=0}^{2^{k-2}-2} \sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+2^{k-2})+2(i_2+2^{k-2})} \\
&\quad + \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2i_1+2(i_2-2^{k-1})} \\
&\quad + \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2(i_1+2^{k-2})+2(i_2-2^{k-1})}
\end{aligned} \tag{4.11}$$

$$
\begin{aligned}
&+ \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1} a_{i_2} \omega \theta^{2i_1+2(i_2-2^{k-1}+2^{k-2})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1} a_{i_2} \omega \theta^{2(i_1+2^{k-2})+2(i_2-2^{k-1}+2^{k-2})} \\
&+ \sum_{i_1=2^{k-1}}^{3.2^{k-2}-2} \sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1} a_{i_2} \omega^2 \theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1})} \\
&+ \sum_{i_1=2^{k-1}}^{3.2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1} a_{i_2} \omega^2 \theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1}+2^{k-2})} \\
&+ \sum_{i_1=2^{k-1}}^{3.2^{k-2}-2} \sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1} a_{i_2} \omega^2 \theta^{2(i_1-2^{k-1}+2^{k-2})+2(i_2-2^{k-1}+2^{k-2}}) \\
\end{aligned}
$$

e

$$
\begin{aligned}
b_{ij}^* \quad = \quad & \sum_{i_1=0}^{2^{k-2}-2} \sum_{i_2=i_1+1}^{2^{k-2}-1} b_{i_1} b_{i_2} \theta^{2i_1+2i_2} + \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=0}^{2^{k-2}-1} b_{i_1} b_{i_2} \theta^{2i_1+2(i_2+2^{k-2})} \\
&+ \sum_{i_1=0}^{2^{k-2}-2} \sum_{i_2=i_1+1}^{2^{k-2}-1} b_{i_1} b_{i_2} \theta^{2(i_1+2^{k-2})+2(i_2+2^{k-2})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} b_{i_1} b_{i_2} \omega \theta^{2i_1+2(i_2-2^{k-1})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} b_{i_1} bi_2 \omega \theta^{2(i_1+2^{k-2})+2(i_2-2^{k-1})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} b_{i_1} b_{i_2} \omega \theta^{2i_1+2(i_2-2^{k-1}+2^{k-2})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} b_{i_1} b_{i_2} \omega \theta^{2(i_1+2^{k-2})+2(i_2-2^{k-1}+2^{k-2})} \\
&+ \sum_{i_1=2^{k-1}}^{3.2^{k-2}-2} \sum_{i_2=i_1+1}^{3.2^{k-2}-1} b_{i_1} b_{i_2} \omega^2 \theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1})} \\
&+ \sum_{i_1=2^{k-1}}^{3.2^{k-2}-1} \sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} b_{i_1} b_{i_2} \omega^2 \theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1}+2^{k-2})} \\
&+ \sum_{i_1=2^{k-1}}^{3.2^{k-2}-2} \sum_{i_2=i_1+1}^{3.2^{k-2}-1} b_{i_1} b_{i_2} \omega^2 \theta^{2(i_1-2^{k-1}+2^{k-2})+2(i_2-2^{k-1}+2^{k-2})}.
\end{aligned}
\tag{4.12}
$$

Observação 4.4. Nos somatórios em que houveram substituição dos coeficientes a_{i_j} e b_{ij} conforme o Sistema (4.9) foi adicionado 2^{k-2} ao expoente devido à mudança de variável nos limites do somatório.

Como $1 + \theta^{2^k} = 2\omega$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= 2\omega\sum_{i=0}^{2^{k-2}-1}a_i^2\theta^{4i}+2\omega^3\sum_{i=2^{k-1}}^{3.2^{k-2}-1}a_i\theta^{4(i-2^{k-1})}-2a_{ij}^*\\ &\quad -2\omega\sum_{i=0}^{2^{k-2}-1}b_i^2\theta^{4i+2}+2\omega^3\sum_{i=2^{k-1}}^{3.2^{k-2}-1}b_i\theta^{4(i-2^{k-1})+2}\\ &\quad +2b_{ij}^*\theta^2\\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned}\tag{4.13}$$

Utilizando o fato que $2x \equiv 0(mod\ 4) \Rightarrow x \equiv 0(mod\ 2)$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega\sum_{i=0}^{2^{k-2}-1}a_i^2\theta^{4i}+\omega^3\sum_{i=2^{k-1}}^{3.2^{k-2}-1}a_i\theta^{4(i-2^{k-1})}-a_{ij}^*\\ &\quad -\omega\sum_{i=0}^{2^{k-2}-1}b_i^2\theta^{4i+2}+\omega^3\sum_{i=2^{k-1}}^{3.2^{k-2}-1}b_i\theta^{4(i-2^{k-1})+2}+b_{ij}^*\theta^2\\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}\tag{4.14}$$

Agora, podemos usar novamente as congruências módulo 2 inclusas na Proposição 4.1

$$\begin{cases}\omega^2 \equiv \omega+1(mod\ 2\mathcal{O}_{\mathbb{K}})\\ \omega^3 \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})\\ \theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})\\ x^2 \equiv x, \text{para todo } x \in \mathbb{Z}.\end{cases}\tag{4.15}$$

Observação 4.5. Note que ao substituir essas congruências na Equação (4.11), as três primeiras somas e as três últimas se resumirão em apenas uma somatória cada, enquanto as outras quatro irão todas se cancelar. De fato,

$$\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1}a_{i_1}a_{i_2}\theta^{2i_1+2i_2}+\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=0}^{2^{k-2}-1}a_{i_1}a_{i_2}\theta^{2i_1+2(i_2+2^{k-2})}+$$

$$\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1}a_{i_1}a_{i_2}\theta^{2(i_1+2^{k-2})+2(i_2+2^{k-2})}=$$

$$\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1}a_{i_1}a_{i_2}(\theta^{2i_1+2i_2}+\theta^{2(i_1+2^{k-2})+2(i_2+2^{k-2})})+\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=0}^{2^{k-2}-1}a_{i_1}a_{i_2}\theta^{2i_1+2(i_2+2^{k-2})}$$

$$=\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1}a_{i_1}a_{i_2}(\theta^{2(i_1+i_2)}+\theta^{2(i_1+i_2)+2^k})+\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=0}^{2^{k-2}-1}a_{i_1}a_{i_2}\theta^{2i_1+2(i_2+2^{k-2})}.$$

No somatório $\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1}a_{i_1}a_{i_2}(\theta^{2(i_1+i_2)}+\theta^{2(i_1+i_2)+2^k})$, como a diferença entre os

expoentes de θ é 2^k e $\theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$, segue que

$$\begin{aligned}\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}(\theta^{2(i_1+i_2)}+\theta^{2(i_1+i_2)+2^k}) &= 2\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)}\\ &\equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}.\end{aligned}$$

Agora, em $\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=0}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2i_1+2(i_2+2^{k-2})}$, sempre que $i_1 = i_2$ obtemos $a_i^2\theta^{4i+2^{k-1}}$, contudo, para $i_1 \neq i_2$ as combinações ocorrem aos pares, donde segue que

$$\begin{aligned}\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=0}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2i_1+2(i_2+2^{k-2})} &= \sum_{i=0}^{2^{k-2}-1} a_i^2\theta^{4i+2^{k-1}} + 2\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2+2^{k-2})}\\ &\equiv \sum_{i=0}^{2^{k-2}-1} a_i^2\theta^{4i+2^{k-1}} \pmod{2\mathcal{O}_{\mathbb{K}}}.\end{aligned}$$

Nos quatro somatórios que representam os termos que multiplicam $\omega\theta^y$, temos

$$\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2i_1+2(i_2-2^{k-1})} + \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2(i_1+2^{k-2})+2(i_2-2^{k-1})}$$

$$+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2i_1+2(i_2-2^{k-1}+2^{k-2})}$$

$$+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2(i_1+2^{k-2})+2(i_2-2^{k-1}+2^{k-2})}$$

$$= \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega(\theta^{2(i_1+i_2-2^{k-1})}+\theta^{2(i_1+i_2-2^{k-1})+2^k})+$$

$$\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega(\theta^{2(i_1+i_2+2^{k-2}-2^{k-1})}+\theta^{2(i_1+i_2+2^{k-2}-2^{k-1})}).$$

Nesse caso, na segunda parcela da igualdade obtemos um somatório onde a diferença no expoente do θ é 2^k, e outro onde os expoentes são iguais. Logo,

$$\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega(\theta^{2(i_1+i_2-2^{k-1})}+\theta^{2(i_1+i_2-2^{k-1})+2^k})+$$

$$\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega(\theta^{2(i_1+i_2+2^{k-2}-2^{k-1})}+\theta^{2(i_1+i_2+2^{k-2}-2^{k-1})}) =$$

$$2\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega\theta^{2(i_1+i_2-2^{k-1})}+$$

$$2\sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega(\theta^{2(i_1+i_2+2^{k-2}-2^{k-1})} \equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}.$$

Finalmente, analisando os somatórios referente aos termos que multiplicam $\omega^2\theta^y$, temos

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2\theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1})}+$$

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2\theta^{2(i_1-2^{k-1})+2(i_2-2^{k-1}+2^{k-2})}+$$

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2\theta^{2(i_1-2^{k-1}+2^{k-2})+2(i_2-2^{k-1}+2^{k-2})} =$$

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-2^{k-1}-2^{k-1})}+\theta^{2(i_1+i_2-2^{k-1}-2^{k-1}+2^{k-2}+2^{k-2})})+$$

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-2^{k-1}-2^{k-1}+2^{k-2})}) =$$

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-2^k)}+\theta^{2(i_1+i_2-2^k)+2^k})+$$

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-3.2^{k-2})}).$$

No somatório $\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-2^k)}+\theta^{2(i_1+i_2-2^k)+2^k})$, como a diferença entre os expoentes de θ é 2^k e $\theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$, segue que

$$\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-2^k)}+\theta^{2(i_1+i_2-2^k)+2^k}) = 2\sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2+2^k)}$$

$$\equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}.$$

Agora, analisando $\sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-3.2^{k-2})})$, sempre que $i_1=i_2$ obtemos $\sum_{i=0}^{3.2^{k-2}-1} a_i^2\theta^{4i-3.2^{k-1}}$ enquanto para $i_1\neq i_2$ as combinações ocorrem aos pares, donde segue que

$$\begin{aligned}\sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega^2(\theta^{2(i_1+i_2-3.2^{k-2})}) &= \sum_{i=2^{k-1}}^{3.2^{k-2}-1}\omega^2a_i^2\theta^{4i-3.2^{k-1}}+\\ &+ 2\sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1}\omega^2a_{i_1}a_{i_2}\theta^{2(i_1+i_2-3.2^{k-2})}\\ &\equiv \sum_{i=2^{k-1}}^{3.2^{k-2}-1}\omega^2a_i^2\theta^{4i-3.2^{k-1}} \pmod{2\mathcal{O}_{\mathbb{K}}}.\end{aligned}$$

Portanto,

$$a_{ij}^* \equiv \sum_{i=0}^{2^{k-1}-1} a_i^2\theta^{4i+2^{k-1}} + \sum_{i=2^{k-1}}^{3.2^{k-2}-1} a_i^2\omega^2\theta^{4i-3.2^{k-1}} (mod\ 2\mathcal{O}_{\mathbb{K}}). \tag{4.16}$$

O mesmo ocorre na Equação (4.12) usando os mesmos argumentos. Logo,

$$b_{ij}^* \equiv \sum_{i=0}^{2^{k-1}-1} b_i^2\theta^{4i+2^{k-1}} + \sum_{i=2^{k-1}}^{3.2^{k-2}-1} b_i^2\omega^2\theta^{4i-3.2^{k-1}} (mod\ 2\mathcal{O}_{\mathbb{K}}). \tag{4.17}$$

Realizando as substituições englobadas no Sistema (4.15) e nas Equações (4.16) e (4.17) na Equação (4.14), segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \left(\sum_{i=0}^{2^{k-2}-1} a_i\theta^{4i}\omega\right)+\left(\sum_{i=2^{k-1}}^{3.2^{k-2}-1} a_i\theta^{4(i-2^{k-1})}\right)-\left(\sum_{i=0}^{2^{k-2}-1} a_i\theta^{4i+2^{k-1}}\right)\\ &-\left(\sum_{i=2^{k-1}}^{3.2^{k-2}-1} a_i\theta^{4i-3.2^{k-1}}(\omega+1)\right)-\left(\sum_{i=0}^{2^{k-2}-1} b_i\theta^{4i+2}\omega\right)\\ &-\left(\sum_{i=2^{k-1}}^{3.2^{k-2}-1} b_i\theta^{4(i-2^{k-1})+2}\right)+\left(\sum_{i=0}^{2^{k-2}-1} b_i\theta^{4i+2^{k-1}+2}\right)\end{aligned}$$

$$+\left(\sum_{i=2^{k-1}}^{3.2^{k-2}-1} b_i\theta^{4i-3.2^{k-1}+2}(\omega+1)\right)$$
$$\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Note que na terceira somatória da equação acima, tomando $i = 2^{k-3}$, o expoente do θ fica $4.2^{k-3}+2^{k-1} = 2^k$ e para o mesmo valor de i, na sétima somatória, o expoente de θ fica θ^{2^k+2}. Agora, na quarta somatória, tomando $i = 5.2^{k-3}$, o expoente de θ fica $4(5.2^{k-3}) - 3.2^{k-1} = 5.2^{k-1} - 3.2^{k-1} = 2^k$ enquanto na oitava somatória, para o mesmo valor de i o expoente de θ é $2^k + 2$. Assim, usando novamente que $\theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e, consequentemente, $\theta^{2^k+y} \equiv \theta^y(mod\ 2\mathcal{O}_{\mathbb{K}})$, segue que

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= \left(\sum_{i=0}^{2^{k-2}-1} a_i\theta^{4i}\omega\right) + \left(\sum_{i=2^{k-1}}^{3.2^{k-2}-1} a_i\theta^{4(i-2^{k-1})}\right) - \left(\sum_{i=0}^{2^{k-3}-1} a_i\theta^{2^{k-1}+4i}\right) \\
&\quad - \left(\sum_{i=2^{k-3}}^{2^{k-2}-1} a_i\theta^{4(i-2^{k-3})}\right) - \left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} a_i\theta^{4i-3.2^{k-1}}(\omega+1)\right) \\
&\quad - \left(\sum_{i=5.2^{k-3}}^{3.2^{k-2}-1} a_i\theta^{4(i-5.2^{k-3})}(\omega+1)\right) - \left(\sum_{i=0}^{2^{k-2}-1} b_i\theta^{4i+2}\omega\right) \\
&\quad - \left(\sum_{i=2^{k-1}}^{3.2^{k-2}-1} b_i\theta^{4(i-2^{k-1})+2)}\right) + \left(\sum_{i=0}^{2^{k-3}-1} b_i\theta^{2^{k-1}+4i+2}\right) \\
&\quad + \left(\sum_{i=2^{k-3}}^{2^{k-2}-1} b_i\theta^{4(i-2^{k-3})+2}\right) + \left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} b_i\theta^{4i-3.2^{k-1}+2}(\omega+1)\right) \\
&\quad + \left(\sum_{i=5.2^{k-3}}^{3.2^{k-2}-1} b_i\theta^{4(i-5.2^{k-3})+2}(\omega+1)\right) \\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}$$

Agrupando os termos semelhantes, obtemos uma combinação linear inteira entre os elementos da base de $\mathcal{O}_{\mathbb{K}}$, $\{1, \theta^2, \theta^4, \theta^6, \ldots, \theta^{2^k-2}, \omega, \omega\theta^2, \omega\theta^4, \omega\theta^6, \ldots \omega\theta^{2^k-2}\}$. Desse modo, obtemos as seguintes congruências módulo 2, válidas para todo $0 \leq j \leq 2^{k-3} - 1$.

$$\begin{cases}
a_{2^{k-1}+j} - a_{2^{k-3}+j} - a_{5.2^{k-3}+j} \equiv 0(mod\ 2) \\
a_{5.2^{k-3}+j} - a_j - a_{2^{k-1}+j} \equiv 0(mod\ 2) \\
a_j - a_{5.2^{k-3}+j} \equiv 0(mod\ 2) \\
a_{2^{k-3}+j} - a_{2^{k-1}+j} \equiv 0(mod\ 2) \\
b_{2^{k-1}+j} - b_{2^{k-3}+j} - b_{5.2^{k-3}+j} \equiv 0(mod\ 2) \\
b_{5.2^{k-3}+j} - b_j - b_{2^{k-1}+j} \equiv 0(mod\ 2) \\
b_j - b_{5.2^{k-3}+j} \equiv 0(mod\ 2) \\
b_{2^{k-3}+j} - b_{2^{k-1}+j} \equiv 0(mod\ 2)
\end{cases}$$

De $a_j - a_{5.2^{k-3}+j} \equiv 0(mod\ 2)$ e $a_{2^{k-3}+j} - a_{2^{k-1}+j} \equiv 0(mod\ 2)$, obtemos $a_j \equiv a_{5.2^{k-3}+j}(mod\ 2)$ e $a_{2^{k-3}+j} \equiv a_{2^{k-1}+j}(mod\ 2)$, respectvamente. Substituindo essas duas congruências em $a_{5.2^{k-3}+j} - a_j - a_{2^{k-1}+j} \equiv 0(mod\ 2)$ e $a_{2^{k-1}+j} - a_{2^{k-3}+j} - a_{5.2^{k-3}+j} \equiv 0(mod\, 2)$, respectivamente, obtemos que $a_{2^{k-1}+j} \equiv 0(mod\, 2)$ e $a_{5.2^{k-3}+j} \equiv 0(mod\ 2)$. Repetindo o mesmo argumento, o sistema acuma nos fornece as congruências $b_{2^{k-1}+j} \equiv 0(mod\ 2)$ e $b_{5.2^{k-3}+j} \equiv 0(mod\ 2)$. Agora, substituindo essas congruências no Sistema (4.8), segue que $a_i \equiv 0(mod\ 2)$ para todo $0 \leq i \leq 2^k - 1$ e que $b_i \equiv 0(mod\ 2)$, para todo $0 \leq i \leq 2^k - 1$. Logo, nas expressões $\alpha = a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + \cdots + a_{2^{k-1}-1}\theta^{2^k-2} + a_{2^{k-1}}\omega + a_{2^{k-1}+1}\omega\theta^2 + a_{2^{k-1}+2}\omega\theta^4 + \ldots + a_{2^k-1}\omega\theta^{2^k-2}$ e $\beta = b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + \ldots + b_{2^{k-1}-1}\theta^{2^k-2} + b_{2^{k-1}}\omega + b_{2^{k-1}+1}\omega\theta^2 + b_{2^{k-1}+2}\omega\theta^4 + \ldots + b_{2^k-1}\omega\theta^{2^k-2}$ devemos ter obrigatoriamente $a_i, b_i \equiv 0(mod\ 2)$, ou seja, todos são pares. Dessa forma, segue que $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$ e, portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ e ω são inteiros em $\mathbb{L}$, uma vez que pertencem a $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$, segue a inclusão

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \theta^4, \ldots, \theta^{2^{k-2}}, \omega, \omega\theta^2, \omega\theta^4, \ldots, \omega\theta^{2^{k-2}}][1, \theta] \subset \mathcal{O}_{\mathbb{L}}.$$

Portanto, $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \theta^4, \ldots, \theta^{2^{k-2}}, \omega, \omega\theta^2, \omega\theta^4, \ldots, \omega\theta^{2^{k-2}}][1, \theta]$. Com isso, concuímos a prova do teorema. □

4.2 Discriminante

A partir do Teorema 4.2 podemos concluir que o anel de inteiros algébricos dos corpos puros $\mathbb{Q}(\sqrt[2^k]{d})$, com $k \geq 1$ e $d \neq 1$ é um inteiro livre de quadrados tal que $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 8)$, (exceto para $k = 1$) possui a mesma estrutura, onde o valor de k vai determinar apenas a quantidade de elementos da base. Assim, é esperado que os discriminantes também possuam uma forma similar, que possa ser escrita por meio de uma expressão dependendo apenas da variável k. Essa fórmula, para $k \geq 2$, é dada no seguinte teorema.

Teorema 4.6. *Seja o corpo de números $\mathbb{L} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[n]{d}$ com d livre de quadrados e $n = 2^k$, com $k > 1$. Se $d \equiv 1(mod\ 4)$ e $d \not\equiv 1(mod\ 2^l)$, para todo $l > 2$, então o discriminante do anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ de $\mathbb{L}$ é dado por $-2^{(k-1)n}d^{n-1}$.*

Demonstração. Para essa prova usaremos a definição 1.32, a qual estabelece o cálculo do discriminante do anel de inteiros algébricos de um corpo $\mathbb{L}$ como sendo o discriminante

de sua base integral. Como

$$\{1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \frac{1+\theta^{\frac{n}{2}}}{2}, \frac{\theta+\theta^{\frac{n}{2}+1}}{2}, \frac{\theta^2+\theta^{\frac{n}{2}+2}}{2}, \ldots, \frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}\}$$

é uma base de $\mathcal{O}_{\mathbb{K}}$ quando $d \equiv 1(mod\ 4)$, segundo o Teorema 4.2, segue que o discriminante de $\mathcal{O}_{\mathbb{K}}$,

$$D(\mathbb{K}) = D_{\mathbb{K}}(1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \frac{1+\theta^{\frac{n}{2}}}{2}, \frac{\theta+\theta^{\frac{n}{2}+1}}{2}, \frac{\theta^2+\theta^{\frac{n}{2}+2}}{2}, \ldots, \frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}),$$

é dado pelo seguinte determinante

$$\det \begin{bmatrix}
\mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \ldots & \mathrm{Tr}(\theta^{\frac{n}{2}-1}) & \mathrm{Tr}(\frac{1+\theta^{\frac{n}{2}}}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) \\
\mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \ldots & \mathrm{Tr}(\theta^{\frac{n}{2}}) & \mathrm{Tr}(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^n}{2}) \\
\mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) & \ldots & \mathrm{Tr}(\theta^{\frac{n}{2}+1}) & \mathrm{Tr}(\frac{\theta^2+\theta^{\frac{n}{2}+2}}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}+1}+\theta^{n+1}}{2}) \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\mathrm{Tr}(\theta^{\frac{n}{2}-1}) & \mathrm{Tr}(\theta^{\frac{n}{2}}) & \ldots & \mathrm{Tr}(\theta^{n-2}) & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-2}+\theta^{\frac{3n}{2}-2}}{2}) \\
\mathrm{Tr}(\frac{1+\theta^{\frac{n}{2}}}{2}) & \mathrm{Tr}(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-2}}{2}) & \mathrm{Tr}(\frac{1+2\theta^{\frac{n}{2}}+\theta^n}{4}) & \ldots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+2\theta^{n-1}+\theta^{\frac{3n}{2}-1}}{4}) \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) & \mathrm{Tr}(\frac{\theta+\theta^n}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^2+\theta^{n+1}}{2}) & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-2}+\theta^{\frac{3n}{2}-2}}{2}) & \ldots & \mathrm{Tr}(\frac{\theta^{n-2}+2\theta^{\frac{3n}{2}-2}+\theta^{2n-2}}{4})
\end{bmatrix}.$$

Sendo assim, o primeiro passo para calcular o determinante dessa matriz $n \times n$ é calcular o traço desses elementos. Pela Proposição 1.37, segue que $Tr(1) = n$, $Tr(\theta^n) = nd$ e $Tr(\theta^q) = 0$ para todo $q \neq an$, onde $a \in \mathbb{N}$. A fim de tornar a demonstração e seus passos mais claros, analisamos os traços dos elementos da matriz linha a linha, explicitando alguns valores. Desse modo,

1. Primeira linha: $Tr(1) = n$, $Tr(\theta) = 0$, $Tr(\theta^2) = 0, \cdots, Tr(\theta^{\frac{n}{2}-1}) = 0$, $\mathrm{Tr}(\frac{1+\theta^{\frac{n}{2}}}{2}) = \frac{n}{2} \rightarrow$ coluna $\frac{n}{2}+1$, $\mathrm{Tr}(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}) = 0, \cdots, \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) = 0$.

2. Segunda linha: $Tr(\theta) = 0$, $Tr(\theta^2) = 0, \cdots, Tr(\theta^{\frac{n}{2}}) = 0$, $\mathrm{Tr}(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^2+\theta^{\frac{n}{2}+2}}{2}) = 0, \cdots, \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^n}{2}) = \frac{nd}{2}$.

3. Terceira linha: $Tr(\theta^2) = 0$, $Tr(\theta^3) = 0, \cdots, Tr(\theta^{\frac{n}{2}+1}) = 0$, $\mathrm{Tr}(\frac{\theta^2+\theta^{\frac{n}{2}+2}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^3+\theta^{\frac{n}{2}+3}}{2}) = 0, \cdots, \mathrm{Tr}(\frac{\theta^{\frac{n}{3}-1}+\theta^{\frac{2n}{3}-1}+\theta^{n-1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^n}{2}) = \frac{nd}{2}$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}+1}+\theta^{n+1}}{2}) = 0$.

4. Quarta linha: $Tr(\theta^3) = 0$, $Tr(\theta^4) = 0, \cdots, Tr(\theta^{\frac{n}{2}+2}) = 0$, $\mathrm{Tr}(\frac{\theta^3+\theta^{\frac{n}{2}+3}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^4+\theta^{\frac{n}{2}+4}}{2}) = 0, \cdots, \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^n}{2}) = \frac{nd}{2}$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}+1}+\theta^{n+1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}+2}+\theta^{n+2}}{2}) = 0$.

5. $\frac{n}{2}$-ésima linha: $Tr(\theta^{\frac{n}{2}-1}) = 0$, $Tr(\theta^{\frac{n}{2}}) = 0$, $Tr(\theta^{\frac{n}{2}+1}) = 0, \cdots, \mathrm{Tr}(\theta^{n-2}) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^n-1}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^n}{2}) = \frac{nd}{2} \rightarrow$ coluna $\frac{n}{2}+2$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}+1}+\theta^{n+1}}{2}) = 0, \cdots, \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}) = 0$.

Note que, da segunda linha até a $\frac{n}{2}$-ésima linha, o padrão se repete: para cada linha i, onde $i = 2, 3, \ldots, \frac{n}{2}$, as entradas de todas as colunas é zero, exceto a da coluna $j = n - i + 2$. De fato, os elementos da primeira até a $\frac{n}{2}$-ésima coluna dessas linhas são da forma $\mathrm{Tr}(\theta^q), 1 < q < n$, (pois origina-se de $\theta^{i_1} \times \theta^{i_2}, 1 \leq i_1 \leq \frac{n}{2} - 1$ e $0 \leq i_2 \leq \frac{n}{2} - 1$) que resultam em zero para todos esses valores de q e, os demais, isto é, os elementos da $\frac{n}{2} + 1$-ésima coluna até a última, são do tipo $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}\pm q} + \theta^{n \pm q}}{2}), 0 < q < n$ (pois decorrem da multiplicação de θ^{i_1} por $\frac{\theta^{i_2} + \theta^{i_2 + \frac{n}{2}}}{2}$ com $1 \leq i_1 \leq \frac{n}{2} - 1$ e $0 \leq i_2 \leq \frac{n}{2} - 1$), os quais resultam em zero para todos os valores de q exceto para $q = 0$, fato que, para cada linha i, ocorre na coluna j de posição $n - i + 2$. Agora, fixando a linha $\frac{n}{2} + 1$, a entrada de cada coluna j é dado pelo valor do traço de $\frac{1 + \theta^{\frac{n}{2}}}{2} a_j$. Assim, para que o traço não seja nulo, o termo a_j deve conter os valores $1, \theta^{\frac{n}{2}}$ ou θ^n, fato que ocore nas colunas 1 e $\frac{n}{2} + 1$, onde a_j é, respectivamente, 1 e $\frac{1 + \theta^{\frac{n}{2}}}{2}$. Dando sequência, a partir da linha $i = \frac{n}{2} + q$, com $2 \leq q \leq \frac{n}{2}$, haverão 2 elementos não nulos em cada linha, pois os elementos correspondem ao valor do traço de $a_i a_j$ onde $a_i = \frac{\theta^{q-1} + \theta^{\frac{n}{2} + q - 1}}{2}$ e a_j percorre todos os elementos da base. Assim, para que o traço não seja nulo, o elemento a_j deve conter um dos termos θ^{n-1} ou $\theta^{\frac{n}{2} - 1}$, e isso acontece nas colunas $n - i + 2 = \frac{n}{2} - q + 2$ e $n - i + 2 + \frac{n}{2} = n - q + 2$. Alguns desses valores foram evidenciados abaixo, a fim de reforçar o processo realizado e destacar alguns valores específicos encontrados em cada linha.

1. $\frac{n}{2} + 1$-ésima linha: $\mathrm{Tr}(\frac{1 + \theta^{\frac{n}{2}}}{2}) = \frac{n}{2}$, $\mathrm{Tr}(\frac{\theta + \theta^{\frac{n}{2}+1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^2 + \theta^{\frac{n}{2}+2}}{2}) = 0, \cdots$,
$Tr\left(\left(\frac{1 + \theta^{\frac{n}{2}}}{2}\right)^2\right) = Tr\left(\frac{1}{4} + \frac{\theta^{\frac{n}{2}}}{2} + \frac{\theta^n}{4}\right) = \frac{n}{4} + \frac{nd}{4} \rightarrow$ coluna $\frac{n}{2} + 1$,
$Tr\left(\left(\frac{1 + \theta^{\frac{n}{2}}}{2}\right)\left(\frac{\theta + \theta^{\frac{n}{2}+1}}{2}\right)\right) = Tr\left(\frac{\theta}{4} + \frac{\theta^{\frac{n}{2}+1}}{2} + \frac{\theta^{n+1}}{4}\right) = 0, \cdots, Tr\left(\left(\frac{1 + \theta^{\frac{n}{2}}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-1} + \theta^{n-1}}{2}\right)\right)$
$= Tr\left(\frac{\theta^{\frac{n}{2}-1}}{4} + \frac{\theta^{n-1}}{2} + \frac{\theta^{\frac{3n}{2}-1}}{4}\right) = 0.$

2. $\frac{n}{2} + 2$-ésima linha: $\mathrm{Tr}(\frac{\theta + \theta^{\frac{n}{2}+1}}{2}) = 0$, $\mathrm{Tr}(\frac{\theta^2 + \theta^{\frac{n}{2}+2}}{2}) = 0, \cdots, Tr\left(\left(\frac{\theta + \theta^{\frac{n}{2}+1}}{2}\right)\theta^{n-1}\right) =$
$Tr(\frac{\theta^{\frac{n}{2}} + \theta^n}{2}) = \frac{nd}{2} \rightarrow$ coluna $n - (\frac{n}{2} + 2 - 2) = \frac{n}{2}$, $Tr\left(\left(\frac{\theta + \theta^{\frac{n}{2}+1}}{2}\right)\left(\frac{1 + \theta^{\frac{n}{2}}}{2}\right)\right) =$
$Tr\left(\frac{\theta}{4} + \frac{\theta^{\frac{n}{2}+1}}{2} + \frac{\theta^{n+1}}{4}\right) = 0, \cdots, Tr\left(\left(\frac{\theta + \theta^{\frac{n}{2}+1}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-1} + \theta^{n-1}}{2}\right)\right) =$
$Tr\left(\frac{\theta^{\frac{3n}{2}}}{4} + \frac{\theta^n}{2} + \frac{\theta^{\frac{n}{2}+1}}{2}\right) = \frac{nd}{2} \rightarrow$ coluna $n - (\frac{n}{2} + 2 - 2) + \frac{n}{2} = n$.

3. $n - 2$-ésima linha: $Tr(\frac{\theta^{\frac{n}{2}-3} + \theta^{n-3}}{2}) = 0$, $Tr(\frac{\theta^{\frac{n}{2}-2} + \theta^{n-2}}{2}) = 0$, $Tr(\frac{\theta^{\frac{n}{2}-1} + \theta^{n-1}}{2}) = 0$,
$Tr\left(\left(\frac{\theta^{\frac{n}{2}-3} + \theta^{n-3}}{2}\right)\theta^3\right) = \mathrm{Tr}(\frac{\theta^{\frac{n}{2}} + \theta^n}{2}) = \frac{nd}{2} \rightarrow$ coluna $n - (n-2) + 2 = 4$, $Tr(\frac{\theta^{\frac{n}{2}+1} + \theta^n}{2} +$
$1) = 0$, $Tr(\frac{\theta^{\frac{n}{2}+2} + \theta^{n+2}}{2}) = 0, \cdots, Tr\left(\left(\frac{\theta^{\frac{n}{2}-3} + \theta^{n-3}}{2}\right)\left(\frac{\theta^3 + \theta^{\frac{n}{2}+3}}{2}\right)\right) = Tr(\frac{\theta^{\frac{n}{2}} + 2\theta^n + \theta^{\frac{3n}{2}}}{4}) =$
$\frac{nd}{2} \rightarrow$ coluna $n - (n - 2 - 2) + \frac{n}{2} = \frac{n}{2} + 4, \cdots, Tr\left(\left(\frac{\theta^{\frac{n}{2}-3} + \theta^{n-3}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-2} + \theta^{n-2}}{2}\right)\right) =$
$Tr\left(\frac{\theta^{n-5}}{4} + 2\frac{\theta^{\frac{3n}{2}-5}}{4} + \frac{\theta^{2n-5}}{4}\right) = 0, Tr\left(\left(\frac{\theta^{\frac{n}{2}-3} + \theta^{n-3}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-1} + \theta^{n-1}}{2}\right)\right) =$
$Tr\left(\frac{\theta^{n-4}}{4} + 2\frac{\theta^{\frac{3n}{2}-4}}{4} + \frac{\theta^{2n-4}}{4}\right) = 0.$

4. $n-1$-ésima linha: $Tr(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}) = 0,\ Tr(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) = 0,\ Tr\left(\left(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}\right)\theta^2\right) = Tr(\frac{\theta^{\frac{n}{2}}+\theta^{n}}{2}) = \frac{nd}{2} \rightarrow$ coluna $n-(n-1)+2 = 3,\ Tr(\frac{\theta^{\frac{n}{2}+1}+\theta^{n+1}}{2}) = 0,\ Tr(\frac{\theta^{\frac{n}{2}+2}+\theta^{n+2}}{2}) = 0, \cdots, Tr\left(\left(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}\right)\left(\frac{\theta^{2}+\theta^{\frac{n}{2}+2}}{2}\right)\right) = \mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+2\theta^{n}+\theta^{\frac{3n}{2}}}{4}) = \frac{nd}{2} \rightarrow$ coluna $n-(n-1-2)+\frac{n}{2} = \frac{n}{2}+3, \cdots, Tr\left(\left(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}\right)\right) = Tr\left(\frac{\theta^{n-4}}{4}+2\frac{\theta^{\frac{3n}{2}-4}}{4}+\frac{\theta^{2n-4}}{4}\right) = 0,\ Tr\left(\left(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}\right)\right) = Tr\left(\frac{\theta^{n-3}}{4}+2\frac{\theta^{\frac{3n}{2}-3}}{4}+\frac{\theta^{2n-3}}{4}\right) = 0.$

5. n-ésima linha: $Tr(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) = 0,\ Tr\left(\left(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}\right)\theta\right) = \mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^{n}}{2}) = \frac{nd}{2} \rightarrow$ coluna $n-n+2 = 2$, $Tr(\frac{\theta^{\frac{n}{2}+1}+\theta^{n}}{2}+1) = 0$, $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}+2}+\theta^{n+2}}{2}) = 0, \cdots,$ $Tr\left(\left(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}\right)\left(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}\right)\right) = Tr(\frac{\theta^{\frac{n}{2}}+2\theta^{n}+\theta^{3n}2}{4}) = \frac{nd}{2} \rightarrow$ coluna $n-(n-2)+\frac{n}{2} = \frac{n}{2}+2, \cdots, Tr\left(\left(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}\right)\left(\frac{\theta^{\frac{n}{2}-2}+\theta^{n-2}}{2}\right)\right) = Tr\left(\frac{\theta^{n-3}}{4}+2\frac{\theta^{\frac{3n}{2}-3}}{4}+\frac{\theta^{2n-3}}{4}\right) = 0,$ $Tr\left(\left(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}\right)^2\right) = Tr(\frac{\theta^{n-2}}{4}+\frac{\theta^{\frac{3n}{2}-2}}{2}+\frac{\theta^{2n-2}}{4}) = 0.$

Uma vez que o valor de cada traço é conhecido e, consequentemente, o valor de todas as entradas da matriz, podemos calcular o seu determinante, o qual fornece o discriminante de $\mathcal{O}_{\mathbb{K}}$. Para resolver o determinante desta matriz $n \times n$, aplicamos o método de Laplace $n-2$ vezes até obter uma matriz de ordem 2×2. Como podemos perceber pelos valores dos traços, a segunda linha (e logo, também a segunda coluna, uma vez que a matriz é simétrica) é composta toda de zero's, exceto pela última coluna. Em função disso, por conveniência, aplicamos Laplace nesta linha. Em seguida, obtemos uma matriz de ordem $n-1 \times n-1$, onde a nova segunda linha (a qual era a terceira linha da matriz original) também terá apenas um elemento não nulo, onde aplicaremos Laplace novamente e, assim, procedemos por $\frac{n}{2}-1$ vezes, sempre fazendo o desenvolvimento pela segunda linha. Após estes passos, obtemos uma matriz de ordem $\frac{n}{2}+1 \times \frac{n}{2}+1$ e, devido à simetria da matriz, podemos repetir esses passos mais $\frac{n}{2}-1$ vezes, mas agora desenvolvendo sempre pela segunda coluna, onde todos os elementos, exceto o da última linha da matriz resultante em cada passo, é nulo. Ao fim desses $\frac{n}{2}-1$ passos, obtemos uma matriz de ordem 2×2. Como $\mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^{n}}{2}) = \frac{nd}{2}$ é o único elemento não nulo de cada linha/coluna em que aplicamos Laplace, segue que este é o elemento que irá multiplicar o cofator nas $n-2$ operações, sendo o seu sinal alternado entre positivo e negativo em cada passo (pois o sinal é dado pela fórmula $(-1)^{i+j}$). A matriz 2×2 resultante após os $n-2$ passos anteriores, é a formada pela primeira linha e primeira coluna, e $n+1$-ésima linha e $n+1$-ésima coluna, ou seja, é a matriz

$$\begin{bmatrix} n & \frac{n}{2} \\ \frac{n}{2} & \frac{(n+nd)}{4} \end{bmatrix}.$$

Escrevendo tudo isso matematicamente, segue que o discriminante do anel de inteiros

algébricos de $\mathbb{L}$ é dado por

$$D(\mathbb{L}) = \det(M_1),$$

onde

$$M_1 = \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \dots & \mathrm{Tr}(\theta^{\frac{n}{2}-1}) & \mathrm{Tr}(\frac{1+\theta^{\frac{n}{2}}}{2}) & \dots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \dots & \mathrm{Tr}(\theta^{\frac{n}{2}}) & \mathrm{Tr}(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}) & \dots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}}+\theta^n}{2}) \\ \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) & \dots & \mathrm{Tr}(\theta^{\frac{n}{2}+1}) & \mathrm{Tr}(\frac{\theta^2+\theta^{\frac{n}{2}+2}}{2}) & \dots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}+1}+\theta^{n+1}}{2}) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\theta^{\frac{n}{2}-1}) & \mathrm{Tr}(\theta^{\frac{n}{2}}) & \dots & \mathrm{Tr}(\theta^{n-2}) & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) & \dots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-2}+\theta^{\frac{3n}{2}-2}}{2}) \\ \mathrm{Tr}(\frac{1+\theta^{\frac{n}{2}}}{2}) & \mathrm{Tr}(\frac{\theta+\theta^{\frac{n}{2}+1}}{2}) & \dots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-2}}{2}) & \mathrm{Tr}(\frac{1+2\theta^{\frac{n}{2}}+\theta^n}{4}) & \dots & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+2\theta^{n-1}+\theta^{\frac{3n}{2}-1}}{4}) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-1}+\theta^{n-1}}{2}) & \mathrm{Tr}(\frac{\theta+\theta^n}{2}) & \dots & \mathrm{Tr}(\frac{\theta^2+\theta^{n+1}}{2}) & \mathrm{Tr}(\frac{\theta^{\frac{n}{2}-2}+\theta^{\frac{3n}{2}-2}}{2}) & \dots & \mathrm{Tr}(\frac{\theta^{n-2}+2\theta^{\frac{3n}{2}-2}+\theta^{2n-2}}{4}) \end{bmatrix},$$

ou seja,

$$M_1 = \begin{bmatrix} n & 0 & 0 & 0 & \dots & \dots & 0 & \frac{n}{2} & 0 & 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 0 & \frac{n}{2}d \\ 0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 \\ 0 & 0 & 0 & \dots & \dots & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 \\ 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 & 0 \\ \frac{n}{2} & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{4}(1+d) & 0 & 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d \\ 0 & 0 & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 \\ 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 \\ 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 \end{bmatrix}$$

coluna $\frac{n}{2}$ ↓

← linha $\frac{n}{2}$

Assim,

$$D(\mathbb{L}) = (-1)^{(2+n)}\frac{n}{2}d\det(M_2),$$

onde

$$M_2 = \begin{bmatrix}
n & 0 & 0 & 0 & \dots & \dots & 0 & \frac{n}{2} & 0 & 0 & \dots & \dots & \dots & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 0 & \frac{n}{2}d \\
0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 \\
0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 & 0 \\
\frac{n}{2} & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{4}(1+d) & 0 & 0 & \dots & \dots & \dots & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d \\
0 & 0 & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 \\
0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 \\
0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0
\end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ l \\ i \\ n \\ \leftarrow \ h \\ a \\ \frac{n}{2}-1 \\ \\ \\ \\ \\ \end{matrix}$$

Logo,

$$D(\mathbb{L}) = (-1)^{(2+n)}\frac{n}{2}d(-1)^{2+(n-1)}\frac{n}{2}d\det(M_3),$$

onde

$$M_3 = \begin{bmatrix}
n & 0 & 0 & 0 & \dots & \dots & 0 & \frac{n}{2} & 0 & 0 & \dots & \dots & \dots & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 0 & \frac{n}{2}d \\
0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 \\
0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 & 0 \\
\frac{n}{2} & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{4}(1+d) & 0 & 0 & \dots & \dots & \dots & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d \\
0 & 0 & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 \\
0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 \\
0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0
\end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ l \\ i \\ n \\ \leftarrow \ h \\ a \\ \frac{n}{2}-2 \\ \\ \\ \\ \\ \end{matrix}$$

Prosseguindo desse modo, obtemos

$$D(\mathbb{L}) = (-1)^{(2+n)}(-1)^{2+(n-1)}(-1)^{2+(n-2)}\cdots(-1)^{2+(n-\frac{n}{2})}(\frac{n}{2}d)^{\frac{n}{2}-1}\det(M_4),$$

onde

$$M_4 = \begin{bmatrix} n & 0 & 0 & 0 & \dots & 0 & 0 & \frac{n}{2} \\ \frac{n}{2} & 0 & 0 & \dots & 0 & 0 & 0 & \frac{n}{4}(1+d) \\ 0 & 0 & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 \\ 0 & 0 & \dots & 0 & 0 & \frac{n}{2}d & 0 & 0 \\ \vdots & \dots & \dots & \ddots & \dots & \dots & \dots & \vdots \\ 0 & 0 & \frac{n}{2}d & 0 & 0 & \dots & 0 & 0 \\ 0 & \frac{n}{2}d & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}$$

é uma matriz de ordem $\frac{n}{2}+1 \times \frac{n}{2}+1$. Assim,

$$D(\mathbb{L}) = (-1)(\frac{n}{2}d)^{\frac{n}{2}-1}\det\begin{bmatrix} n & 0 & 0 & 0 & \dots & 0 & 0 & \frac{n}{2} \\ \frac{n}{2} & 0 & 0 & \dots & 0 & 0 & 0 & \frac{n}{4}(1+d) \\ 0 & 0 & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 \\ 0 & 0 & \dots & 0 & 0 & \frac{n}{2}d & 0 & 0 \\ \vdots & \dots & \dots & \ddots & \dots & \dots & \dots & \vdots \\ 0 & 0 & \frac{n}{2}d & 0 & 0 & \dots & 0 & 0 \\ 0 & \frac{n}{2}d & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

Dando continuidade ao processo, obtemos

$$D(\mathbb{L}) = (-1)(\frac{n}{2}d)^{\frac{n}{2}-1}(-1)^{2+(\frac{n}{2}+1)}(-1)^{2+\frac{n}{2}}(-1)^{2+(\frac{n}{2}-1)}\cdots(-1)^{2+3}(\frac{n}{2}d)^{\frac{n}{2}-1}\det(M_5),$$

onde

$$M_5 = \begin{bmatrix} n & \frac{n}{2} \\ \frac{n}{2} & \frac{n}{4}(1+d) \end{bmatrix}.$$

Portanto,

$$\begin{aligned} D(\mathbb{L}) &= (-1)(\tfrac{n}{2}d)^{n-2}\det\begin{bmatrix} n & \frac{n}{2} \\ \frac{n}{2} & \frac{n}{4}(1+d) \end{bmatrix} \\ &= -(\tfrac{n}{2}d)^{n-2}(\tfrac{n^2}{4}+\tfrac{n^2d}{4}-\tfrac{n^2}{4}) = -(\tfrac{nd}{2})^{n-2}\tfrac{n^2d}{4} = -(\tfrac{2^kd}{2})^{2^k-2}(\tfrac{(2^k)^2}{4}d) \\ &= -(2^{(k-1)(2^k-2)})d^{(2^k-2)}d2^{(2k-2)} = -2^{(k2^k-2^k-2k+2+2k-2)}d^{(2^k-2+1)} \\ &= -2^{(k-1)2^k}d^{2^k-1} = -2^{(k-1)n}d^{n-1}, \end{aligned}$$

o que prova o teorema. □

Uma vez que o discriminante do anel de inteiros algébricos do corpo quadrático é dado por $d \neq 1$ quando $d \equiv 1 \pmod 4$, conforme pode ser visto, por exemplo, em [25], juntamente com o teorema acima, podemos enunciar o seguinte teorema, o qual fornece o discrminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$ onde $d \neq 1$ inteiro livre de quadrados satisfazendo $d \equiv 1(mod\ 4)$, para todo $k \geq 1$.

Teorema 4.7. *Seja o corpo de números* $\mathbb{L} = \mathbb{Q}(\theta)$, *onde* $\theta = \sqrt[n]{d}$ *com* $d \neq 1$ *livre de quadrados e* $n = 2^k$, *com* $k \geq 1$. *Se* $d \equiv 1(mod\ 4)$ *para* $k = 1$ *e* $d \equiv 5(mod\ 8)$ *para* $k \geq 2$, *então o discriminante do anel de inteiros algébricos* $\mathcal{O}_{\mathbb{L}}$ *de* $\mathbb{L}$ *é dado por*

$$\mathcal{D}(\mathbb{L}) = \begin{cases} d, \text{ se } k = 1 \\ \\ -2^{(k-1)n} d^{n-1}, \text{ se } k \geq 2. \end{cases}$$

4.3 Considerações finais

A partir do trabalho desenvolvido nesse capítulo, é possível determinar uma base integral de qualquer corpo puro do tipo $\mathbb{Q}(\sqrt[2^k]{d})$, com $k \in \mathbb{N}$, $d \neq 1$ um inteiro e livre de quadrados, onde 4 divide $d-1$ e 4 é maior potência de 2 em que isso ocorre (exceto para $k = 1$), ou seja, o Teorema 4.2 estabelece uma base integral de $\mathbb{Q}(\sqrt[2^k]{d})$ para uma família de valores de d. Além disso, também determinamos uma fórmula para o discriminante do anel de inteiros algébricos de $\mathbb{Q}(\sqrt[2^k]{d})$ com d satisfazendo as mesmas condições acima, a qual depende apenas do valor de k. No próximo capítulo, exploraremos os corpos $\mathbb{Q}(\sqrt[2^k]{d})$ com $d \neq 1$ um inteiro e livre de quadrados e $k \in \mathbb{N}$, $k \geq 2$, considerando agora o caso em que 8 é a maior potência de 2 que divide $d-1$. Seguindo a mesma sequência adotada nesse capítulo, exibiremos uma base do anel de inteiros algébricos e, em seguida, forneceremos uma fórmula para o discriminante.

5 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \equiv 9(mod\ 16)$

Neste capítulo, determinamos uma base integral para o corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e tal que $d \equiv 9(mod\ 16)$ ou, equivalentemente, $d \equiv 1(mod\ 8)$ e 8 é a maior potência de 2 que divide $d-1$. Como consequência, também calculamos o discriminante associado à base integral. Para esse caso, o raciocínio utilizado nas demonstrações é análogo ao utilizado no caso $d \equiv 5(mod\ 8)$ feito no capítulo 4, sendo a diferença entre os valores das congruências enunciados na Proposição 5.1 em relação às enunciadas na Proposição 4.1 e, a base que tomamos inicialmente, as principais diferenças, e é a partir dessas diferenças que obtemos uma nova base.

5.1 Anel de inteiros algébricos

No Capítulo 3, analisando os anéis de inteiros algébricos determinados em cada seção, é possível notar que, para todos os graus investigados, existe uma base integral específica para os corpos $\mathbb{Q}(\sqrt[2^k]{d})$ onde $d \neq 1$ é um inteiro e livre de quadrados com a restrição de que $d \equiv 1(mod\ 8)$, sendo 8 a maior potência de 2 que divide $d-1$, de modo que essa condição de 8 ser a maior potência de 2 que divide $d-1$ não se aplica apenas para $k=2$ (note que, para o corpo quártico, 8 é a maior potência de 2 dividindo $d-1$ que fornece uma nova base, assim como 4 o é no corpo quadrático e, por essa razão, não se aplica essa condição). Sendo assim, o objetivo deste capítulo é generalizar esse resultado apresentando uma base integral para todos os corpos $\mathbb{Q}(\sqrt[2^k]{d})$, com $d \neq 1$ um inteiro e livre de quadrados, $k \geq 4$ natural e $d \equiv 1(mod\ 8)$ tal que $d \not\equiv 1 \pmod{2^l}$, para todo $l \geq 4$. Este resultado, complementado aos casos particulares citados acima, nos dá uma base integral de qualquer corpo $\mathbb{Q}(\sqrt[2^k]{d})$ com $k \geq 2$ e $d \neq 1$ um inteiro e livre de quadrados nas condições acima. Iniciamos a seção enunciando a proposição que fornece algumas congruências e igualdade que serão fortemente utilizadas para demonstrar o Teorema 5.2.

Proposição 5.1. *Sejam $\mathbb{L} = \mathbb{Q}(\theta)$, com $\theta = \sqrt[2^k]{d}$, $k \geq 4$ e $d \neq 1$ um inteiro livre de*

quadrados tal que $d \equiv 1(mod\ 8)$ *e* 8 *é a maior potência de* 2 *que divide* $d-1$ *e* $\mathbb{K} = \mathbb{Q}(\theta^2)$. *Se* $\omega_1 = \frac{1+\theta^{2^{k-1}}}{2}$, $\omega_2 = \frac{1+\theta^{2^{k-2}}+\theta^{2^{k-1}}+\theta^{3.2^{k-2}}}{4}$ *e* m *é um inteiro ímpar tal que* $d-1 = 8m$, *então são válidas as seguintes igualdades e congruências:*

1. $\theta^{2^{k-1}} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})$
2. $\omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$
3. $\omega_1^2 \equiv \omega_1 + 2m(mod\ 4\mathcal{O}_{\mathbb{K}})$
4. $\omega_1\theta^{2^{k-1}} \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$
5. $\omega_2^2 \equiv \omega_2 + \theta^{2^{k-1}} + 1 + \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$
6. $\omega_2\theta^{2^{k-1}} \equiv \omega_2 + 2m(mod\ 4\mathcal{O}_{\mathbb{K}})$
7. $1 + \theta^{2^{k-1}} = 2\omega_1$.

Demonstração. A demonstração dos itens 1, 2, 3, 4 e 8 são análogas às da Proposição 4.1, usando $d-1 = 8m$, onde $m \in \mathbb{Z}$ ao invés de $d-1 = 4m$. Para os demais itens, a demonstração é análoga às demonstrações feitas na prova dos Teoremas 3.3 e 3.5 no caso $d \equiv 1(mod\ 8)$, tomando $n = 2^k$. □

Assim como foi feito no Teorema 4.2, podemos enunciar um teorema equivalente para $d \equiv 9(mod\ 16)$, cuja prova sucedará utilizando o mesmo método, o Princípio da Indução Finita, levando em conta as particularidades que envolvem essa congruência de d.

Teorema 5.2. *Seja* $\mathbb{L} = \mathbb{Q}(\theta), \theta = \sqrt[2^k]{d}$, *com* $d \neq 1$ *um inteiro e livre de quadrados. Se* $k = 2$ *e* $d \equiv 1(mod\ 8)$ *e se* $k \geq 3$ *e* $d \equiv 9(mod\ 16)$, *então* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \ldots + \mathbb{Z}\theta^{2^{k-1}-1} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_1\theta + \mathbb{Z}\omega_1\theta^2 + \mathbb{Z}\omega_1\theta^3 + \ldots + \mathbb{Z}\omega_1\theta^{2^{k-2}-1} + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_2\theta + \mathbb{Z}\omega_2\theta^2 + \mathbb{Z}\omega_2\theta^3 + \ldots + \mathbb{Z}\omega_2\theta^{2^{k-2}-1}$, *onde* $\omega_1 = \frac{1+\theta^{2^{k-1}}}{2}$ *e* $\omega_2 = \frac{1+\theta^{2^{k-2}}+\theta^{2^{k-1}}+\theta^{3.2^{k-2}}}{4}$. *Em outras palavras,*

$$\{1, \theta, \theta^2, \ldots \theta^{2^{k-1}-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \ldots \omega_1\theta^{2^{k-2}-1}, \omega_2, \omega_2\theta, \omega_2\theta^2, \omega_2\theta^3, \ldots, \omega_2\theta^{2^{k-2}-1}\}$$

é uma base integral do corpo $\mathbb{L}$.

Demonstração. O resultado será demonstrado pelo Princípio de Indução Finita, seguindo os mesmos passos utilizados na demonstração do Teorema 4.2. Deste modo, alguns detalhes serão omitidos. Além disso, uma vez que os Teoremas 3.1 e 3.3 já englobam os casos em que $k = 2$ e $k = 3$, respectivamente, consideraremos $k \geq 4$.

1) *Passo Base:* O resultado vale para o valor inicial $k = 4$, ou seja para grau $n = 16$, conforme visto no Teorema 3.5.

2) *Hipótese de indução:* Suponhamos que o resultado é verdadeiro para k, ou seja, para grau $n = 2^k$. Logo, uma base do anel de inteiros algébricos de $\mathbb{Q}(\theta)$, com $\theta = \sqrt[2^k]{d}$ é

$$\{1, \theta, \theta^2, \dots \theta^{2^{k-1}-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \dots \omega_1\theta^{2^{k-2}-1}, \omega_2, \omega_2\theta, \omega_2\theta^2, \omega_2\theta^3, \dots, \omega_2\theta^{2^{k-2}-1}\},$$

onde $\omega_1 = \frac{1+\theta^{2^{k-1}}}{2}$ e $\omega_2 = \frac{1+\theta^{2^{k-2}}+\theta^{2^{k-1}}+\theta^{3.2^{k-2}}}{4} = \omega_1\left(\frac{1+\theta^{2^{k-2}}}{2}\right)$.

3) Agora, provamos que o resultado é válido para $k+1$, ou seja, para $n = 2^{k+1}$. Isso implica provar que uma base do anel de inteiros algébricos de $\mathbb{Q}(\theta)$, com $\theta = \sqrt[2^{k+1}]{d}$ é dada por

$$\{1, \theta, \theta^2, \dots \theta^{2^k-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \dots \omega_1\theta^{2^{k-1}-1}, \omega_2, \omega_2\theta, \omega_2\theta^2, \omega_2\theta^3, \dots, \omega_2\theta^{2^{k-1}-1}\},$$

onde $\omega_1 = \frac{1+\theta^{2^k}}{2}$ e $\omega_2 = \frac{1+\theta^{2^{k-1}}+\theta^{2^k}+\theta^{3.2^{k-1}}}{4} = \omega_1\left(\frac{1+\theta^{2^{k-1}}}{2}\right)$.

Chamando $\mathbb{L} = \mathbb{Q}(\sqrt[2^{k+1}]{d})$, $\mathbb{K} = \mathbb{Q}(\sqrt[2^k]{d})$ e $\theta = \sqrt[2^{k+1}]{d}$, podemos escrever $\mathbb{L} = \mathbb{Q}(\theta)$ e $\mathbb{K} = \mathbb{Q}(\theta^2)$. Com isso em vista, uma vez que

$$\mathbb{Z}[1, \theta, \theta^2, \dots \theta^{2^k-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \dots \omega_1\theta^{2^{k-1}-1}, \omega_2, \omega_2\theta, \omega_2\theta^2, \dots, \omega_2\theta^{2^{k-1}-1}] = \mathcal{O}_{\mathbb{K}}[\theta],$$

é suficiente mostrar que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$, onde, utilizando a notação acima,

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1, \theta^2, \theta^4, \dots, \theta^{2^k-2}, \omega_1, \omega_1\theta^2, \dots, \omega_1\theta^{2^{k-1}-2}, \omega_2, \omega_2\theta^2, \dots, \omega_2\theta^{2^{k-1}-2}],$$

com $\omega_1 = \frac{1+\theta^{2^k}}{2}$ e $\omega_2 = \frac{1+\theta^{2^{k-1}}+\theta^{2^k}+\theta^{3.2^{k-1}}}{4}$. Mostremos, portanto, as duas inclusões.

a) $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Neste caso, seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Como $\{1, \theta\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tal que $2\eta = \alpha + \beta\theta$ e, consequentemente,

$$\alpha^2 - \beta^2\theta^2 \equiv 0 (mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{5.1}$$

Como α, $\beta \in \mathcal{O}_{\mathbb{K}}$ e, pela hipótese de indução, o conjunto

$$\{1, \theta^2, \theta^4, \dots, \theta^{2^k-2}, \omega_1, \omega_1\theta^2, \dots, \omega_1\theta^{2^{k-1}-2}, \omega_2, \omega_2\theta^2, \dots, \omega_2\theta^{2^{k-1}-2}\},$$

onde $\omega_1 = \frac{1+\theta^{2^{k-1}}}{2}$ e $\omega_2 = \frac{1+\theta^{2^{k-2}}+\theta^{2^{k-1}}+\theta^{3.2^{k-2}}}{4}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem inteiros a_i, b_i com $0 \leq i \leq 2^k - 1$ tais que

$$\begin{cases} \alpha &= a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + \cdots + a_{2^{k-1}-1}\theta^{2^k-2} + a_{2^{k-1}}\omega_1 + a_{2^{k-1}+1}\omega_1\theta^2 \\ & \quad + a_{2^{k-1}+2}\omega_1\theta^4 + \ldots + a_{3.2^{k-2}-1}\omega_1\theta^{2^{k-1}-2} + a_{3.2^{k-2}}\omega_2 + a_{3.2^{k-2}+1}\omega_2\theta^2 \\ & \quad + a_{3.2^{k-2}+2}\omega_2\theta^4 + \ldots + a_{2^k-1}\omega_2\theta^{2^{k-1}-2} \\ \beta &= b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + \ldots + b_{2^{k-1}-1}\theta^{2^k-2} + b_{2^{k-1}}\omega_1 + b_{2^{k-1}+1}\omega_1\theta^2 \\ & \quad + b_{2^{k-1}+2}\omega_1\theta^4 + \ldots + b_{3.2^{k-2}-1}\omega_1\theta^{2^{k-1}-2} + + b_{3.2^{k-2}}\omega_2 + b_{3.2^{k-2}+1}\omega_2\theta^2 \\ & \quad + b_{3.2^{k-2}+2}\omega_2\theta^4 + \ldots + b_{2^k-1}\omega_2\theta^{2^{k-1}-2}. \end{cases}$$

Substituindo esses valores na Equação (5.1), obtemos

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= a_0^2 + a_1^2\theta^4 + a_2^2\theta^8 + a_3^2\theta^{12} + a_4^2\theta^{16} + \ldots + a_{2^{k-1}-1}^2\theta^{2^{k+1}-4} + a_{2^{k-1}}^2\omega_1^2 \\ &\quad + a_{2^{k-1}+1}\omega_1^2\theta^4 + a_{2^{k-1}+2}^2\omega_1^2\theta^8 + \ldots + a_{3.2^{k-2}-1}^2\omega_1^2\theta^{2^k-4} + a_{3.2^{k-2}}^2\omega_2^2 \\ &\quad + a_{3.2^{k-2}+1}^2\omega_2^2\theta^2 + a_{3.2^{k-2}+2}\omega_2^2\theta^8 + \ldots + a_{2^k-1}^2\omega_2^2\theta^{2^k-4} + 2(a_{ij}) \\ &\quad - (b_0^2 + b_1^2\theta^4 + b_2^2\theta^8 + b_3^2\theta^{12} + b_4^2\theta^{16} + \ldots + (b_{2^{k-1}-1})^2\theta^{2^{k+1}-4} \\ &\quad + b_{2^{k-1}}^2\omega_1^2 + b_{2^{k-1}+1}^2\omega_1^2\theta^4 + b_{2^{k-1}+2}^2\omega_1^2\theta^8 + \ldots + b_{2^{k-1}-1}^2\theta^{2^{k+1}-4} \\ &\quad + b_{2^{k-1}}^2\omega_1^2 + b_{2^{k-1}+1}\omega_1^2\theta^4 + b_{2^{k-1}+2}^2\omega_1^2\theta^8 + \ldots (b_{2^k-1})^2\omega_1^2\theta^{2^{k+1}-4} \\ &\quad + b_{3.2^{k-2}-1}^2\omega_1^2\theta^{2^k-4} + b_{3.2^{k-2}}^2\omega_2^2 + b_{3.2^{k-2}+1}^2\omega_2^2\theta^2 + b_{3.2^{k-2}+2}\omega_2^2\theta^8 + \ldots \\ &\quad + b_{2^k-1}^2\omega_2^2\theta^{2^k-4} + 2(b_{ij}))\theta^2 \\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}), \end{aligned} \tag{5.2}$$

onde a_{ij} representa a soma de todas as multiplicações de a_ix por a_jy, com $0 \leq i \leq 2^k - 2$ e $i < j$, e b_{ij} representa a soma de todas as multiplicações de b_ix por b_jy, com $0 \leq i \leq 2^k - 2$ e $i < j$. Neste caso, podemos representar esses valores através das seguintes expressões

$$\begin{aligned} a_{ij} &= \sum_{i_1=0}^{2^{k-1}-2}\sum_{i_2=i_1+1}^{2^{k-1}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)} + \sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} + \\ &\quad + \sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=3.2^{k-2}}^{2^{k-1}-1} a_{i_1}a_{i_2}\omega_2\theta^{2(i_1+i_2-3.2^{k-2})} + \sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega_1^2\theta^{2(i_1+i_2-2^k)} \\ &\quad + \sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=3.2^{k-2}}^{2^k-1} a_{i_1}a_{i_2}\omega_1\omega_2\theta^{2(i_1+i_2-5.2^{k-2})} \end{aligned} \tag{5.3}$$

$$+\sum_{i_1=3.2^{k-2}}^{2^k-2}\sum_{i_2=i_1+1}^{2^k-1} a_{i_1}a_{i_2}\omega_2^2\theta^{2(i_1+i_2-3.2^{k-1})}$$

e

$$\begin{aligned} b_{ij} &= \sum_{i_1=0}^{2^{k-1}-2}\sum_{i_2=i_1+1}^{2^{k-1}-1} b_{i_1}b_{i_2}\theta^{2(i_1+i_2)} + \sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} b_{i_1}b_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})}+ \\ &+\sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=3.2^{k-2}}^{2^{k-1}-1} b_{i_1}b_{i_2}\omega_2\theta^{2(i_1+i_2-3.2^{k-2})} + \sum_{i_1=2^{k-1}}^{3.2^{k-2}-2}\sum_{i_2=i_1+1}^{3.2^{k-2}-1} b_{i_1}b_{i_2}\omega_1^2\theta^{2(i_1+i_2-2^k)} \\ &+\sum_{i_1=2^{k-1}}^{3.2^{k-2}-1}\sum_{i_2=3.2^{k-2}}^{2^k-1} b_{i_1}b_{i_2}\omega_1\omega_2\theta^{2(i_1+i_2-5.2^{k-2})}+ \\ &+\sum_{i_1=3.2^{k-2}}^{2^k-2}\sum_{i_2=i_1+1}^{2^k-1} b_{i_1}b_{i_2}\omega_2^2\theta^{2(i_1+i_2-3.2^{k-1})}. \end{aligned} \tag{5.4}$$

Reescrevendo a Equação (5.2) em termos da congruência módulo 2 e com o auxílio de somatórios, a fim de facilitar a escrita nos próximos passos, segue que

$$\begin{aligned} \alpha^2-\beta^2\theta^2 &= \sum_{i=0}^{2^{k-1}-1} a_i^2\theta^{4i} + \sum_{i=2^{k-1}}^{3.2^{k-2}-1} a_i^2\omega_1^2\theta^{4(i-2^{k-1})} + \sum_{i=3.2^{k-2}}^{2^k-1} a_i^2\omega_2^2\theta^{4(i-3.2^{k-2})} \\ &\quad - \sum_{i=0}^{2^{k-1}-1} b_i^2\theta^{4i+2} - \sum_{i=2^{k-1}}^{3.2^{k-2}-1} b_i^2\omega_1^2\theta^{4(i-2^{k-1})+2} - \sum_{i=3.2^{k-2}}^{2^k-1} b_i^2\omega_2^2\theta^{4(i-3.2^{k-2})+2} \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned} \tag{5.5}$$

Nesse corpo, são válidas as seguintes congruências, de acordo com a Proposição 5.1

$$\begin{cases} \theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_1\theta^{2^{k-1}} \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2\theta^{2^{k-1}} \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2^2 \equiv 1+\theta^{2^{k-1}}+\omega_1+\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ x^2 \equiv x(mod\ 2), \end{cases}$$

para todo $x \in \mathbb{Z}$. Note que, substituindo as congruências $\omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e $\omega_2^2 \equiv 1+\theta^{2^{k-1}}+\omega_1+\omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})$ na Equação (5.5), os coeficientes que estão multiplicando $\theta^{2^k}, \omega_1\theta^{2^{k-1}}$ e $\omega_2\theta^{2^{k-1}}$ em cada uma das somatórias, correspondem

exatamente ao termo médio da parcela, de modo que devemos substituir as congruências $\theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}), \omega_1\theta^{2^{k-1}} \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}})$ e $\omega_2\theta^{2^{k-1}} \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}})$ exatamente na posição que ocupa o ponto médio entre os limites inferior e superior de cada somatório. Desse modo, obtemos a expressão

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= \sum_{i=0}^{2^{k-2}-1}(a_i + a_{i+2^{k-2}})\theta^{4i} + \sum_{i=2^{k-1}}^{5.2^{k-3}-1}(a_i + a_{i+2^{k-3}})\omega_1\theta^{4(i-2^{k-1})} \\
&\quad + \sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}(a_i + a_{i+2^{k-3}})(1 + \theta^{2^{k-1}} + \omega_1 + \omega_2)\theta^{4(i-3.2^{k-2})} \\
&\quad - \sum_{i=0}^{2^{k-1}-1}(b_i + b_{i+2^{k-2}})\theta^{4i+2} - \sum_{i=2^{k-1}}^{5.2^{k-3}-1}(b_i + b_{i+2^{k-3}})\omega_1\theta^{4(i-2^{k-1})+2} \\
&\quad - \sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}(b_i + b_{i+2^{k-2}})(1 + \theta^{2^{k-1}} + \omega_1 + \omega_2)\theta^{4(i-3.2^{k-2})+2} \\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}),
\end{aligned} \tag{5.6}$$

que corresponde a uma combinação linear dos elementos da base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Logo, os coeficientes devem ser congruentes a 0 módulo 2, donde obtemos as seguintes congruências, válidas para todo $i = 0, 1, 2, \ldots, 2^{k-2} - 1$ e $j = 0, 1, 2, \ldots, 2^{k-3} - 1$.

$$\begin{cases}
a_i + a_{2^{k-2}+i} + a_{3.2^{k-2}+i} + a_{7.2^{k-3}+i} \equiv 0(mod\ 2) \\
a_{2^{k-1}+j} + a_{5.2^{k-3}+j} + a_{3.2^{k-2}+j} + a_{7.2^{k-3}+j} \equiv 0(mod\ 2) \\
a_{3.2^{k-2}+j} + a_{7.2^{k-3}+j} \equiv 0(mod\ 2) \\
b_i + b_{2^{k-2}+i} + b_{3.2^{k-2}+i} + b_{7.2^{k-3}+i} \equiv 0(mod\ 2) \\
b_{2^{k-1}+j} + b_{5.2^{k-3}+j} + b_{3.2^{k-2}+j} + b_{7.2^{k-3}+j} \equiv 0(mod\ 2) \\
b_{3.2^{k-2}+j} + b_{7.2^{k-3}+j} \equiv 0(mod\ 2).
\end{cases}$$

Consequentemente, para todo $i = 0, 1, 2, \ldots, 2^{k-2} - 1$, e $j = 0, 1, 2, \ldots, 2^{k-3} - 1$ segue que

$$\begin{cases}
a_i \equiv -a_{2^{k-2}+i}(mod\ 2) \\
a_{2^{k-1}+j} \equiv -a_{5.2^{k-3}+j}\ (mod\ 2) \\
a_{3.2^{k-2}+j} \equiv -a_{7.2^{k-3}+j}\ (mod\ 2) \\
b_i \equiv -b_{2^{k-2}+i}(mod\ 2) \\
b_{2^{k-1}+j} \equiv -b_{5.2^{k-3}+j}(mod\ 2) \\
b_{3.2^{k-2}+j} \equiv -a_{7.2^{k-3}+j}\ (mod\ 2).
\end{cases} \tag{5.7}$$

E dessas congruências, efetuando os produtos, seguem as congruências a seguir

$$\begin{cases}
1.\ (a_i)^2 \equiv (a_{2^{k-2}+i})^2 (mod\ 4) \\
2.\ (a_{2^{k-1}+j})^2 \equiv (a_{5.2^{k-3}+j})^2\ (mod\ 4) \\
3.(a_{3.2^{k-2}+j})^2 \equiv (a_{7.2^{k-3}+j})^2\ (mod\ 4) \\
4.\ a_i a_{2^{k-2}+i} \equiv -(a_i)^2 (mod\ 4) \\
5.\ a_{2^{k-1}+j} a_{5.2^{k-3}+j} \equiv -(a_{2^{k-1}+j})^2 (mod\ 4) \\
6.\ a_{3.2^{k-2}+j} a_{7.2^{k-3}+j} \equiv -(a_{3.2^{k-2}+j})^2 (mod\ 4) \\
7.\ a_{2^{k-2}+j_1} a_{2^{k-2}+j_2} \equiv a_{j_1} a_{j_2} (mod\ 4), j_1 \neq j_2 \\
8.\ a_{2^{k-2}+j_1} a_{2^{k-1}+j_2} \equiv -a_{j_1} a_{2^{k-1}+j_2} (mod\ 4), j_1 \neq j_2 \\
9.\ a_{2^{k-2}+j_1} a_{3.2^{k-2}+j_2} \equiv -a_{j_1} a_{3.2^{k-2}+j_2} (mod\ 4), j_1 \neq j_2 \\
10.\ a_{j_1} a_{5-2^{k-3}+j_2} \equiv -a_{j_1} a_{2^{k-1}+j_2} (mod\ 4), j_1 \neq j_2 \\
11.\ a_{j_1} a_{7.2^{k-3}+j_2} \equiv -a_{j_1} a_{3.2^{k-2}+j_2} (mod\ 4), j_1 \neq j_2 \\
12.\ a_{2^{k-2}+j_1} a_{7.2^{k-3}+j_2} \equiv a_{j_1} a_{3.2^{k-2}+j_2} (mod\ 4), j_1 \neq j_2 \\
13.\ a_{5.2^{k-3}+j_1} a_{5.2^{k-2}+j_2} \equiv a_{2^{k-1}+j_1} a_{2^{k-1}+j_2} (mod\ 4), j_1 \neq j_2 \\
14.\ a_{5.2^{k-3}+j_1} a_{3.2^{k-2}+j_2} \equiv a_{2^{k-1}+j_1} a_{3.2^{k-2}+j_2} (mod\ 4), j_1 \neq j_2 \\
15.\ a_{5.2^{k-3}+j_1} a_{7.2^{k-3}+j_2} \equiv a_{2^{k-1}+j_1} a_{3.2^{k-2}+j_2} (mod\ 4), j_1 \neq j_2 \\
16.\ a_{7.2^{k-3}+j_1} a_{7.2^{k-2}+j_2} \equiv a_{3.2^{k-2}+j_1} a_{3.2^{k-2}+j_2} (mod\ 4), j_1 \neq j_2 \\
17.\ a_{2^{k-2}+j_1} a_{5.2^{k-3}+j_2} \equiv a_{2^{j_1}} a_{2^{k-1}+j_2} (mod\ 4), j_1 \neq j_2.
\end{cases} \tag{5.8}$$

As mesmas congruências são válidas trocando a por b em cada linha do Sistema (5.8). Agora, fazendo uma análise análoga à que fizemos na Observação 4.3 do Teorema 4.2, observe que o coeficiente a_i do lado esquerdo da congruência na equação *1* multiplica θ^j na Equação (5.2), enquanto o coeficiente do lado direito multiplica θ^{j+2^k}. Também, na equação *2*, o coeficiente do lado esquerdo multiplica $\omega_1^2\theta^j$, ao passo que coeficiente do lado direito multiplica $\omega_1^2\theta^{j+2^{k-1}}$. Além disso, na equação *3*, o coeficiente do lado esquerdo multiplica $\omega_2^2\theta^j$ e o do lado direito, $\omega_2^2\theta^{j+2^{k-1}}$ Agora, as outras linhas do sistema se referem aos termos de a_{ij} descritos na Equação (5.3). Realizando todas as substituições contidas nas linhas *4* a *17* na Equação (5.3), analogamente ao que foi retratado na Observação 4.3, o primeiro, terceiro e sexto somatório da Equação (5.3) poderão ser escritos com 3 somatórios cada, pois representam multiplicações de elementos da mesma classe, onde $i_1 < i_2$. Vejamos esse processo na primeira soma, o qual é análogo para as outras duas citadas:

$$\begin{aligned}
\sum_{i_1=0}^{2^{k-1}-2}\sum_{i_2=i_1+1}^{2^{k-1}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)} &= \sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)} \\
&+ \sum_{i_1=2^{k-2}}^{2^{k-1}-2}\sum_{i_2=i_1+1}^{2^{k-1}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)} \\
&+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-2}}^{2^{k-1}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)} \\
&= \sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2)} \\
&+ \sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=i_1+1}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+2^{k-2}+i_2+2^{k-2})} \\
&+ \sum_{i_1=0}^{2^{k-2}-2}\sum_{i_2=0}^{2^{k-2}-1} a_{i_1}a_{i_2}\theta^{2(i_1+i_2+2^{k-2})}.
\end{aligned}$$

Os demais somatórios, por sua vez, irão se escrever em 4 somatórios cada pois, nesse caso, por se tratar de multiplicação entre elementos de classes distintas, é possível ter $i_1 > i_2$. Vejamos o processo no segundo somatório, o qual se verifica também nos outros dois:

$$\begin{aligned}
\sum_{i_1=0}^{2^{k-1}-1}\sum_{i_2=2^{k-1}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} &= \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{5.2^{k-3}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=5.2^{k-3}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} \\
&+ \sum_{i_1=2^{k-2}}^{2^{k-1}-1}\sum_{i_2=2^{k-1}}^{5.2^{k-3}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} \\
&+ \sum_{i_1=2^{k-2}}^{2^{k-1}-1}\sum_{i_2=5.2^{k-3}}^{3.2^{k-2}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} \\
&= \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{5.2^{k-3}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{5.2^{k-3}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1}+2^{k-3})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{5.2^{k-3}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1}+2^{k-3})} \\
&+ \sum_{i_1=0}^{2^{k-2}-1}\sum_{i_2=2^{k-1}}^{5.2^{k-3}-1} a_{i_1}a_{i_2}\omega_1\theta^{2(i_1+i_2-2^{k-1}+2^{k-2})}.
\end{aligned}$$

Todos os argumentos discorridos acima se repetem quando trocamos a por b analisando a Equação (5.4). Isso posto, substituindo todos esses valores na Equação

(5.2), podemos colocar $(1+\theta^{2^k})$, $\omega_1^2(1+\theta^{2^{k-1}})$ e $\omega_2^2(1+\theta^{2^{k-1}})$ em evidência, donde obtemos

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= (1+\theta^{2^k})\sum_{i=0}^{2^{k-2}-1}a_i^2\theta^{4i}+(1+\theta^{2^{k-1}})\omega_1^2\sum_{i=2^{k-1}}^{5.2^{k-3}-1}a_i\theta^{4(i-2^{k-1})}\\ &\quad+(1+\theta^{2^{k-1}})\omega_2^2\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}a_i\theta^{4(i-3.2^{k-2})}-2a_{ij}^*\\ &\quad-(1+\theta^{2^k})\sum_{i=0}^{2^{k-2}-1}b_i^2\theta^{4i+2}-(1+\theta^{2^{k-1}})\omega_1^2\sum_{i=2^{k-1}}^{5.2^{k-3}-1}b_i\theta^{4(i-2^{k-1})+2}\\ &\quad-(1+\theta^{2^{k-1}})\omega_2^2\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}b_i\theta^{4(i-3.2^{k-2})+2}+2b_{ij}^*\theta^2\\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}),\end{aligned} \tag{5.9}$$

onde a_{ij}^* é a soma das 21 parcelas obtidas diretamente da Equação (5.3) fazendo as substituições contidas no Sistema (5.8), conforme a justificativa acima. O mesmo ocorre para b_{ij}^*, o qual é obtido a partir da Equação (5.4). Agora, como $1+\theta^{2^k}=2\omega_1$, $\omega_1^2(1+\theta^{2^{k-1}})=2m(1+\theta^{2^{k-1}})+2\omega_2$, e $\omega_2^2(1+\theta^{2^{k-1}})=2m(1+\theta^{2^{k-1}}+\omega_1+\omega_2)+2\omega_2$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= 2\omega_1\left(\sum_{i=0}^{2^{k-2}-1}a_i^2\theta^{4i}\right)+2(m+m\theta^{2^{k-1}}+\omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1}a_i^2\theta^{4(i-2^{k-1})}\right)\\ &\quad+2(m+m\theta^{2^{k-1}}+m\omega_1+m\omega_2+\omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}a_i^2\theta^{4(i-3.2^{k-2})}\right)-2a_{ij}^*\\ &\quad-2\omega_1\left(\sum_{i=0}^{2^{k-2}-1}b_i^2\theta^{4i+2}\right)-2(m+m\theta^{2^{k-1}}+\omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1}b_i^2\theta^{4(i-2^{k-1})+2}\right)\\ &\quad-2(m+m\theta^{2^{k-1}}+m\omega_1+m\omega_2+\omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}b_i^2\theta^{4(i-3.2^{k-2})+2}\right)+2bij^*\\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}).\end{aligned} \tag{5.10}$$

Uma vez que todas as parcelas da Equação (5.10) estão multiplicando por 2, utilizando o fato $2x\equiv 0(mod\ 4)\Rightarrow x\equiv 0(mod\ 2)$, segue que

$$\begin{aligned}\alpha^2-\beta^2\theta^2 &= \omega_1\left(\sum_{i=0}^{2^{k-2}-1}a_i^2\theta^{4i}\right)+(m+m\theta^{2^{k-1}}+\omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1}a_i^2\theta^{4(i-2^{k-1})}\right)\\ &\quad+(m+m\theta^{2^{k-1}}+m\omega_1+m\omega_2+\omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1}a_i^2\theta^{4(i-3.2^{k-2})}\right)-a_{ij}^*\end{aligned}$$

$$\begin{aligned} & -\omega_1\left(\sum_{i=0}^{2^{k-2}-1} b_i^2\theta^{4i+2}\right) - (m + m\theta^{2^{k-1}} + \omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} b_i^2\theta^{4(i-2^{k-1})+2}\right) \\ & -(m + m\theta^{2^{k-1}} + m\omega_1 + m\omega_2 + \omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} b_i^2\theta^{4(i-3.2^{k-2})+2}\right) + b_{ij}^* \end{aligned} \tag{5.11}$$

$$\equiv\ 0(mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Agora, utilizaremos novamente as congruências módulo 2 abaixo, exibidas na Proposição 5.1.

$$\begin{cases} m \equiv 1(mod\ 2) \\ \omega_1^2 \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2^2 \equiv 1 + \theta^{2^{k-1}} + \omega_1 + \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_1\theta^{2^{k-1}} \equiv \omega_1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_2\theta^{2^{k-1}} \equiv \omega_2(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ x^2 \equiv x, \text{para todo } x \in \mathbb{Z}. \end{cases}$$

Realizando essas substituições em todas as somatórias nos devidos termos da Equação (5.11), inclusive em a_{ij}^* e b_{ij}^*, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 \ =\ & \omega_1\left(\sum_{i=0}^{2^{k-3}-1} a_i\theta^{4i} + \sum_{i=2^{k-3}}^{2^{k-2}-1} a_i\theta^{4(i-2^{k-3})}\right) \\ & +(1 + \theta^{2^{k-1}} + \omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} a_i\theta^{4(i-2^{k-1})}\right) \\ & +(1 + \theta^{2^{k-1}} + \omega_1)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} a_i\theta^{4(i-3.2^{k-2})}\right) \\ & -\left(\sum_{i=0}^{2^{k-2}-1} a_i\theta^{4i+2^{k-1}}\right) - \left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} \omega_1 a_i\theta^{4i-7.2^{k-2}}\right) \\ & -(1 + \theta^{2^{k-1}} + \omega_1 + \omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} a_i\theta^{4i-11.2^{k-2}}\right) \\ & -\omega_1\left(\sum_{i=0}^{2^{k-3}-1} b_i\theta^{4i} + \sum_{i=2^{k-3}}^{2^{k-2}-1} b_i\theta^{4(i-2^{k-3})+2}\right) \\ & -(1 + \theta^{2^{k-1}} + \omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} b_i\theta^{4(i-2^{k-1})+2}\right) \end{aligned} \tag{5.12}$$

$$
\begin{aligned}
&-(1+\theta^{2^{k-1}}+\omega_1)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} b_i\theta^{4(i-3.2^{k-2})+2}\right)\\
&+\left(\sum_{i=0}^{2^{k-2}-1} b_i\theta^{4i+2^{k-1}+2}\right)+\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} \omega_1 b_i\theta^{4i-7.2^{k-2}+2^{k-2}+2}\right)\\
&+(1+\theta^{2^{k-1}}+\omega_1+\omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} b_i\theta^{4i-11.2^{k-2}+2}\right)\\
\equiv\ & 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}
$$

Vale destacar que a expressão correspondente a a^*_{ij} resume-se a

$$
\begin{aligned}
&\left(\sum_{i=0}^{2^{k-2}-1} a_i\theta^{4i+2^{k-1}}\right)-\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} \omega_1 a_i\theta^{4i-7.2^{k-2}}\right)-\\
&(1+\theta^{2^{k-1}}+\omega_1+\omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} a_i\theta^{4i-11.2^{k-2}}\right)
\end{aligned}
\tag{5.13}
$$

após substituirmos as congruências módulo 2 expressas na Proposição 5.1, exatamente pelo mesmo motivo explicado em detalhes na Observação 4.5 contida na demonstração do Teroema 4.2. Dessa forma, das 21 parcelas, restam apenas as somas que representam multiplicações entre elementos da mesma classe e satisfazendo $i_1 = i_2$. O mesmo sucede na expressão b^*_{ij}, que consiste em

$$
\begin{aligned}
&\left(\sum_{i=0}^{2^{k-2}-1} b_i\theta^{4i+2^{k-1}+2}\right)+\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} \omega_1 b_i\theta^{4i-7.2^{k-2}+2}\right)+\\
&+(1+\theta^{2^{k-1}}+\omega_1+\omega_2)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} b_i\theta^{4i-11.2^{k-2}+2}\right).
\end{aligned}
\tag{5.14}
$$

Além disso, note que na primeira somatória da Equação (5.13), tomando $i = 2^{k-3}$, o expoente do θ fica $4.2^{k-3} + 2^{k-1} = 2^k$. O mesmo ocorre na primeira somatória da Equação (5.14), onde se $i = 2^{k-3}$, o expoente de θ fica $2^k + 2$. Agora, analisando a segunda somatória da Equação (5.13), tomando $i = 9.2^{k-4}$, o expoente de θ fica $4(9.2^{k-4}) - 7.2^{k-2} = 9.2^{k-2} - 7.2^{k-2} = 2.2^{k-2} = 2^{k-1}$, e o mesmo se verifica na segunda somatória da Equação (5.14). Também, na terceira somatória de ambas as equações, tomando $i = 13.2^{k-4}$, o expoente de θ fica 2^{k-1} e $2^{k-1}+2$, respectivamente. Assim, usando novamente que $\theta^{2^k} \equiv 1, \theta^{2^k+y} \equiv \theta^y$, $\omega_1\theta^{2^{k-1}} \equiv \omega_1$ e que $\omega_2\theta^{2^{k-1}} \equiv \omega_2$, segue que

$$
\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= \omega_1\left(\sum_{i=0}^{2^{k-3}-1} a_i\theta^{4i} + \sum_{i=2^{k-3}}^{2^{k-2}-1} a_i\theta^{4(i-2^{k-3})}\right) \\
&\quad +(1+\theta^{2^{k-1}}+\omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} a_i\theta^{4(i-2^{k-1})}\right) \\
&\quad +(1+\theta^{2^{k-1}}+\omega_1)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} a_i\theta^{4(i-3.2^{k-2})}\right) \\
&\quad -\left(\sum_{i=0}^{2^{k-3}-1} a_i\theta^{4i+2^{k-1}}\right) - \left(\sum_{i=2^{k-3}}^{2^{k-2}-1} a_i\theta^{4(i-2^{k-3})}\right) \\
&\quad -\left(\sum_{i=2^{k-1}}^{9.2^{k-4}-1} \omega_1 a_i\theta^{4(i-2^{k-1})+2^{k-2}}\right) - \left(\sum_{i=9.2^{k-4}}^{5.2^{k-3}-1} \omega_1 a_i\theta^{4(i-9.2^{k-4})}\right) \\
&\quad -(1+\theta^{2^{k-1}}+\omega_1+\omega_2)\left(\sum_{i=3.2^{k-2}}^{13.2^{k-4}-1} a_i\theta^{4(i-3.2^{k-2})+2^{k-2}}\right. \\
&\quad \left. -\sum_{13.2^{k-4}}^{7.2^{k-3}-1} a_i\theta^{4(i-13.2^{k-4})}\right) \\
&\quad -\omega_1\left(\sum_{i=0}^{2^{k-3}-1} b_i\theta^{4i} + \sum_{i=2^{k-3}}^{2^{k-2}-1} b_i\theta^{4(i-2^{k-3})+2}\right) \\
&\quad -(1+\theta^{2^{k-1}}+\omega_2)\left(\sum_{i=2^{k-1}}^{5.2^{k-3}-1} b_i\theta^{4(i-2^{k-1})+2}\right) \\
&\quad -(1+\theta^{2^{k-1}}+\omega_1)\left(\sum_{i=3.2^{k-2}}^{7.2^{k-3}-1} b_i\theta^{4(i-3.2^{k-2})+2}\right) \\
&\quad +\left(\sum_{i=0}^{2^{k-3}-1} b_i\theta^{4(i)+2^{k-1}+2}\right) + \left(\sum_{i=2^{k-3}}^{2^{k-2}-1} b_i\theta^{4(i-2^{k-3})+2}\right) \\
&\quad +\left(\sum_{i=2^{k-1}}^{9.2^{k-4}-1} \omega b_i\theta^{4(i-2^{k-1})+2^{k-2}+2}\right) + \left(\sum_{i=9.2^{k-4}}^{5.2^{k-3}-1} \omega b_i\theta^{4(i-9.2^{k-4})+2}\right) \\
&\quad +(1+\theta^{2^{k-1}}+\omega_1+\omega_2)\left(\sum_{i=3.2^{k-2}}^{13.2^{k-4}-1} b_i\theta^{4(i-3.2^{k-2})+2^{k-2}+2}\right. \\
&\quad \left. +\sum_{i=13.2^{k-4}}^{7.2^{k-3}-1} b_i\theta^{4(i-13.2^{k-4})+2}\right) \\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}
\tag{5.15}
$$

Dessa forma, obtemos uma combinação linear inteira dos elementos da base

$$\{1, \theta^2, \theta^4, \ldots \theta^{2^k-2}, \omega, \omega\theta^2, \omega\theta^4, \ldots \omega\theta^{2^{k-1}-2}, \omega_2, \omega_2\theta^2, \omega_2\theta^4, \ldots, \omega_2\theta^{2^{k-1}-2}\}$$

de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Logo, os coeficientes devem ser congruentes a 0 módulo 2, donde obtemos as seguintes congruências, válidas para todo $0 \leq h \leq 2^{k-4}-1$.

$$\begin{cases} a_{2^{k-1}+h} + a_{3.2^{k-2}+h} - a_{2^{k-3}+h} - a_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ a_{9.2^{k-4}+h} - a_{13.2^{k-4}+h} - a_{3.2^{k-4}+h} - a_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ a_{2^{k-1}+h} - a_{3.2^{k-2}+h} - a_h - a_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ a_{9.2^{k-4}+h} - a_{13.2^{k-4}+h} - a_{2^{k-4}} - a_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ a_h + a_{2^{k-3}+h} - a_{3.2^{k-2}+h} + a_{9.2^{k-4}+h} - a_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ a_{2^{k-4}+h} + a_{3.2^{k-4}+h} - a_{13.2^{k-4}+h} + a_{2^{k-1}+h} - a_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ a_{2^{k-1}+h} - a_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ a_{9.2^{k-4}+h} - a_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ b_{2^{k-1}+h} + b_{3.2^{k-2}+h} - b_{2^{k-3}+h} - b_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ b_{9.2^{k-4}+h} - b_{13.2^{k-4}+h} - b_{3.2^{k-4}+h} - b_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ b_{2^{k-1}+h} - b_{3.2^{k-2}+h} - b_h - b_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ a_{9.2^{k-4}+h} - a_{13.2^{k-4}+h} - b_{2^{k-4}} - b_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ b_h + b_{2^{k-3}+h} - b_{3.2^{k-2}+h} + b_{9.2^{k-4}+h} - b_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ b_{2^{k-4}+h} + b_{3.2^{k-4}+h} - b_{13.2^{k-4}+h} + b_{2^{k-1}+h} - b_{3.2^{k-2}+h} \equiv 0(mod\ 2) \\ b_{2^{k-1}+h} - b_{13.2^{k-4}+h} \equiv 0(mod\ 2) \\ b_{9.2^{k-4}+h} - b_{3.2^{k-2}+h} \equiv 0(mod\ 2). \end{cases}$$

Da 7ª e da 8ª linha do sistema, segue que $a_{2^{k-1}+h} \equiv a_{13.2^{k-4}+h}(mod\ 2)$ e $a_{9.2^{k-4}+h} \equiv a_{3.2^{k-2}+h}(mod\ 2)$, respectivamente. Substituindo $a_{2^{k-1}+h} \equiv a_{13.2^{k-4}+h}(mod\ 2)$ na 1ª e na 3ª linha e $a_{9.2^{k-4}+h} \equiv a_{3.2^{k-2}+h}(mod\ 2)$ na 2ª e na 4ª linha, obtemos, respectivamente $a_{3.2^{k-2}+h} \equiv a_{2^{k-3}+h} \equiv a_i(mod\ 2)$ e $a_{13.2^{k-4}+h} \equiv a_{3.2^{k-4}+h} \equiv a_{2^{k-4}+h}(mod\ 2)$. Agora, na 5ª linha, substituímos $a_{3.2^{k-2}+h} \equiv a_{2^{k-3}+i} \equiv a_i \equiv a_{9.2^{k-4}+h}(mod\ 2)$, donde obtemos $a_{13.2^{k-4}+h} \equiv 0(mod\ 2)$ e, substituindo $a_{13.2^{k-4}+h} \equiv a_{3.2^{k-4}+h} \equiv a_{2^{k-4}+h} \equiv a_{2^{k-1}+h}(mod\ 2)$ na 6ª linha, obtemos $a_{3.2^{k-2}+h} \equiv 0(mod\ 2)$. Dessas congruências, juntamente com as contidas no Sistema (5.7), vem que $a_i \equiv 0(mod\ 2)$, para todo $0 \leq i \leq 2^k - 1$. Utilizando o mesmo argumento segue também que $b_i \equiv 0(mod\ 2)$, para todo $0 \leq i \leq 2^k - 1$. Como a única solução possível é $a_i, b_i \equiv 0(mod\ 2)$, ou seja, todos pares, segue que $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$, e portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

b) $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Como θ e ω_1 e ω_2 são inteiros em $\mathbb{L}$, segue que

$$\begin{aligned} \mathcal{O}_{\mathbb{K}}[\theta] &= \mathbb{Z}[1, \theta^2, \theta^4, \ldots, \theta^{2^k-2}, \omega_1, \omega_1\theta^2, \omega_1\theta^4, \ldots, \omega_1\theta^{2^{k-1}-2}, \\ &\quad \omega_2, \omega_2\theta^2, \omega_2\theta^4, \ldots, \omega_2\theta^{2^{k-1}-2}][1, \theta] \subset \mathcal{O}_{\mathbb{L}}. \end{aligned}$$

Portanto, $\mathcal{O}_{\mathbb{K}}[\theta] = \mathcal{O}_{\mathbb{L}}$. Com isso, concluímos a prova do teorema. □

5.2 Discriminante

O Teorema 5.2, além de nos fornecer uma base integral para todos os corpos puros do tipo $\mathbb{Q}(\sqrt[2^k]{d})$ com $k > 1$ e $d \neq 1$ um inteiro livre de quadrados tal que $d \equiv 1(mod\ 8)$ e $d \not\equiv 1(mod\ 16)$ (exceto para $k = 2$), também deixa claro que todas essas bases possuem o mesmo padrão, se diferenciando apenas pela quantidade de elementos, a qual coincide com o grau da extensão $\mathbb{Q}(\sqrt[2^k]{d}) \supset \mathbb{Q}$, ou seja, está diretamente relacionada ao valor do expoente k. Com isso, reiterando o que foi feito no Teorema 4.6, iremos estabelecer uma expressão que fornece o valor do discriminante associado à base do anel de inteiros algébricos descrito no Teorema 5.2.

Teorema 5.3. *Seja o corpo de números* $\mathbb{L} = \mathbb{Q}(\theta), \theta = \sqrt[n]{d}$ *com* d *livre de quadrados e* $n = 2^k$*. Se* $k = 2$ *e* $d \equiv 1(mod\ 8)$ *e se* $k \geq 3$ *e* $d \equiv 9(mod\ 16)$*, então o discriminante do anel de inteiros algébricos do corpo* $\mathbb{L}$ *é dado por* $-2^{2^{(k-1)}(2k-3)}d^{n-1}$.

Demonstração. Conforme o Teorema 5.2, segue que

$$\{1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, 1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \ldots, \omega_1\theta^{\frac{n}{4}-1}, \omega_2, \omega_2\theta, \omega_2\theta^2, \ldots, \omega_2\theta^{\frac{n}{4}-1}\}$$

é uma base de $\mathcal{O}_{\mathbb{L}}$, onde $\mathbb{L}$ satisfaz as condições do enunciado. Assim, de acordo com Definição 1.32, segue que o discriminante do anel de inteiros algébricos de $\mathbb{L}$, denotado por

$$D(\mathbb{L}) = D_{\mathbb{L}}(1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \ldots, \omega_1\theta^{\frac{n}{4}-1}, \omega_2, \omega_2\theta, \omega_2\theta^2, \ldots, \omega_2\theta^{\frac{n}{4}-1})$$

é dado por

$$D(\mathbb{L}) = \det(M_1),$$

onde

$$M_1 = \begin{bmatrix}
n & 0 & 0 & 0 & \dots & \dots & & \dots 0 & \frac{n}{2} & 0 & \dots & \dots & 0 & \frac{n}{4} & 0 & \dots & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & \frac{n}{4}d \\
0 & 0 & 0 & \dots & & \dots\dots & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{4}d & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & \dots & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{4}d & 0 & 0 & 0 \\
0 & 0 & 0 & \dots & \dots & 0 & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & 0 & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & \dots & & \dots\dots & \dots & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\
\frac{n}{2} & 0 & 0 & \dots & \dots & \dots & \dots & 0 & \frac{n}{4}(1+d) & 0 & 0 & \dots & \dots & \dots & 0 & 0 & 0 \\
0 & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & 0 & \frac{n}{2}d & 0 & 0 & \dots & \dots & \dots & 0 & \frac{n}{2}d & 0 & \dots & \dots & \dots \\
\frac{n}{4} & 0 & \dots & 0 & \frac{n}{4}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & \dots & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \frac{n}{4}d & 0 & \dots & \dots & 0 & 0 & 0 & \frac{n}{2}d & 0 & \dots & 0 & 0 & \dots & \dots & \dots \\
0 & \frac{n}{4}d & 0 & 0 & \dots & \dots & 0 & 0 & \frac{n}{2}d & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots
\end{bmatrix},$$

de modo que todos os elementos a partir da segunda diagonal abaixo da diagonal secundária são irrelevantes ao cálculo do discriminante. Assim,

$$\begin{aligned}
D(\mathbb{L}) &= -\left(\tfrac{nd}{4}\right)^{\frac{n}{2}} \left(\tfrac{nd}{2}\right)^{\frac{n}{2}-2} \det \begin{bmatrix} n & \frac{n}{2} \\ \frac{n}{2} & \frac{n(1+d)}{4} \end{bmatrix} = -\left(\tfrac{nd}{4}\right)^{\frac{n}{2}} \left(\tfrac{nd}{2}\right)^{\frac{n}{2}-2} \tfrac{n^2}{4}d \\
&= -\left(2^{k-2}\right)^{2^{k-1}} \left(2^{k-1}\right)^{2^{k-1}-2} \left(2^{2k-2}d^{n-1}\right) \\
&= -2^{(k-2)2^{k-1}+(k-1)(2^{k-1}-2)+(2k-2)}d^{n-1} = -2^{k2^{k-1}-2(2^{k-1})+k2^{k-1}-2^{k-1}-2k+2+2k-2}d^{n-1} \\
&= -2^{2k(2^{k-1})-3(2^{k-1})}d^{n-1} = -2^{2^{k-1}(2k-3)}d^{n-1},
\end{aligned}$$

o que prova o resultado. □

5.3 Considerações finais

Tendo em vista os resultados apresentados nesse capítulo e no Capítulo 4, somos levados a um questionamento mais geral: É possível determinar todos as possíveis estruturas dos anéis de inteiros algébricos e os respectivivos discriminantes de um corpo puro qualquer cujo grau é uma potência de 2? O próximo capítulo, que constitui o mais significativo

deste trabalho, visa responder a essa questão, fornecendo, a partir do valor de d, mais precisamente a partir da análise da divisão de $d-1$ por valores que representam potências de 2, mais casos de bases integrais para corpos do tipo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. Uma vez que uma base integral de um corpo é conhecida, torna-se mais fácil calcular o seu discriminante, o qual também será fornecido em termos da potência k referente ao grau do corpo e em termos do valor l, que definiremos como sendo a maior potência de 2 que divide $d-1$ (exceto quando $k = l-1$).

6 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$

Após a análise detalhada dos casos particulares estudados até aqui, neste capítulo, dando continuidade à generalização dos resultados que iniciamos nos Capítulos 4 e 5, determinamos uma base para o anel de inteiros algébricos dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, onde $k \in \mathbb{N}$ e $d \neq 1$ é um inteiro livre de quadrados. Além disso, através dessa base, calculamos o discriminante do anel de inteiros algébricos desses corpos $\mathbb{L}$ por meio da Definição 1.32. Esses resultados são os dois mais significativos deste trabalho e, para enunciá-los, recorremos aos resultados contidos em cada capítulo, de modo que todo o trabalho realizado até aqui foi fundamental para a construção dos resultados finais. Para concluir o capítulo, também incluímos exemplos onde determinamos uma base integral e o discriminante a ela associado para certos corpos utilizando as fórmulas descritas na elaboração do capítulo, na qual a partir dos exemplos expostos fica claro a fácil aplicação dos teoremas apresentados.

6.1 Anel de inteiros algébricos

O objetivo desta seção é determinar o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é inteiro livre de quadrados tal que $d \equiv 2^l + 1 (mod\ 2^{l+1})$, com $2 \leq l \leq k-1$ e $d \equiv 1 (mod\ 2^{k+1})$, para $k \geq 2$, explicitando todos os casos possíveis de acordo o valor de d.

Damos início à seção observando algumas características acerca dos casos particulares, cujo estudo detalhado realizado no Capítulo 3 é essencial para a compreensão e naturalidade dos resultados aqui apresentados e, também, enunciando algumas proposições e definições que nos auxiliarão muito nesse processo. Sendo assim, note que, no Capítulo 3, dado $d \neq 1$ livre de quadrados, analisando o corpo $\mathbb{Q}(\sqrt[2]{d})$, apresentamos os valores de d satisfazendo as condições estabelecidas onde obtemos duas estruturas distintas dos anéis de inteiros algébricos que dependem da congruência de d. Já para o corpo $\mathbb{Q}(\sqrt[4]{d})$ apresentamos 3 casos distintos para a estrutura dos anéis de inteiros algébricos e para o

corpo $\mathbb{Q}(\sqrt[8]{d})$, esse valor aumenta para 4 casos distintos, enquanto para $\mathbb{Q}(\sqrt[16]{d})$, obtemos 5 casos distintos. Agora, para o corpo $\mathbb{Q}(\sqrt[32]{d})$, nós listamos 6 possibilidades diferentes das estruturas dos anéis de inteiros algébricos. Analisando esses fatos, podemos observar que a quantidade de casos distintos da estrutura dos anéis de inteiros algébricos aumenta conforme aumentamos os valores do expoente k. Assim, por esta razão, inciamos a seção enunciando uma proposição, a qual será de extrema importância no processo para determinar as estruturas das bases integrais no caso geral.

Proposição 6.1. *[30, Teorema 15] Se $\mathbb{L} = \mathbb{Q}(\sqrt[n]{d})$, onde $n = p^k$, com p primo, $k \in \mathbb{N}$ e $d \neq 1$ um inteiro livre de quadrados, então uma base integral de $\mathbb{L}$ repete periodicamente módulo p^{k+1}.*

Por intermédio dos casos particulares, constatamos que para o corpo $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, se $d \equiv 2^l + 1 (mod\ 2^{l+1})$, variando o valor de l entre 2 e $k-1$ e se $d \equiv 1 (mod\ 2^{k+1})$, para cada valor de l uma base integral que gera estruturas diferentes do anel de inteiros algébricos. Agora, a partir da Proposição 6.1, fica claro que não há outras possibilidades além das listadas. Tendo isso em vista, fixando o grau da extensão $n = 2^k$ e sendo $d \equiv 2^l + 1 (mod\ 2^{l+1})$, onde $2 \leq l \leq k-1$ e $d \equiv 1 (mod\ 2^{k+1})$, para cada valor de l, obtemos uma base integral para o corpo $\mathbb{L}$ de modo que sua estutura é diferente em cada caso e, consequentemente, os discriminantes também serão distintos. Dessa forma, dada uma extensão de grau $n = 2^k$, obtemos $k+1$ estruturas diferentes para o anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$, uma quando $d \equiv 2, 3 (mod\ 4)$, e k possibilidades quando $d \equiv 1 (mod\ 2^l)$, uma para cada valor de l, onde $2 \leq l \leq k+1$, sendo 2^l a maior potência de 2 que divide $d-1$, exceto quando $l = k+1$, pois este corresponde ao maior valor que l pode assumir alterando uma base. Assim, para listar os elementos da base de $\mathcal{O}_{\mathbb{L}}$, devemos levar em consideração os valores de k e de l, pois as bases e os números de elementos variam conforme esses parâmetros. Baseando-se nos casos apresentados até aqui, podemos fazer a prova fixando o grau e variando as congruências, conforme foi realizado nos Teoremas 3.1, 3.3 e 3.5, ou fixando a congruência e variando os graus que a englobam, conforme feito nos Teoremas 4.2 e 5.2. O caminho escolhido para esse caso foi fixar o grau e analisar todas as congruências, destacando suas particularidades. Com o intuito de facilitar o processo de escrita, definimos o conceito de classe de elementos da base, o qual não deve ser confundido com o conceito de classe de equivalência e que, além disso, baseia-se nos fatos observados até aqui considerando $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, com $d \neq 1$ livre de quadrados.

Definição 6.2. Dizemos que os elementos da base integral do corpo $\mathbb{L}$ estão em uma mesma classe se possuem o mesmo número de termos somando no numerador e o mesmo valor no denominador. Além disso, dizemos que o elemento está na q-ésima classe se

escreve-se como:

$$\frac{\sum_{a=0}^{2^{q-1}-1} \theta^{\frac{an}{2^{q-1}}+x}}{2^{q-1}}, \tag{6.1}$$

onde $q \in \{1, 2, \ldots, l-1, l\}$ e $x = 0, 1, 2, \ldots, \frac{n}{2^{q-1}} - 1$, se $q = l$ e $x = 0, 1, 2, \ldots, \frac{n}{2^q} - 1$, se $q \neq l$.

Assim, se $d \equiv 1 (mod\ 2^l)$, de modo que 2^l é a maior potência de 2 que divide $d-1$, de acordo com a Definição (6.2), uma base de $\mathcal{O}_{\mathbb{L}}$ possui l classes de elementos e o número de elementos de cada classe se dá da seguinte forma:

a) $d \equiv 1 (mod\ 2^2)$: há 2 classes, sendo $\frac{n}{2}$ elementos de cada classe (primeira e segunda).

b) $d \equiv 1 (mod\ 2^3)$: há 3 classes, sendo $\frac{n}{2}$ elementos da primeira classe e $\frac{n}{4}$ elementos da segunda e da terceira classe.

c) $d \equiv 1 (mod\ 2^4)$: há 4 classes, sendo $\frac{n}{2}$ elementos da primeira classe e $\frac{n}{4}$ elementos da segunda e $\frac{n}{8}$ elementos da terceira e da quarta classe.

d) $d \equiv 1 (mod\ 2^5)$: há 5 classes, sendo $\frac{n}{2}$ elementos da primeira classe, $\frac{n}{4}$ elementos da segunda, $\frac{n}{8}$ elementos da terceira e $\frac{n}{16}$ elementos da quarta e da quinta classe.

e) $d \equiv 1 (mod\ 2^l)$: há l classes, sendo $\frac{n}{2}$ elementos da primeira classe e $\frac{n}{4}$ elementos da segunda, $\frac{n}{8}$ elementos da terceira, $\frac{n}{16}$ elementos da quarta, e assim sucessivamente, até $\frac{n}{2^{l-1}}$ elementos na penúltima e na última classe.

Chamamos a atenção ao fato de que as duas últimas classes sempre possuem o mesmo número de elementos (mesmo que as duas últimas coincidam com as duas primeiras, como no caso listado item a, onde haverão apenas 2 classes no total, abordado no Capítulo 4), enquanto nas demais, partindo da primeira, a qual possui sempre $\frac{n}{2}$ elementos, essa quantidade vai reduzindo para a metade a cada classe que avançamos.

Por facilidade de escrita, faremos uso da seguinte notação:

$$\begin{cases} \omega_0 = 1 \\ \omega_1 = \frac{1+\theta^{\frac{n}{2}}}{2}, \\ \omega_2 = \frac{1+\theta^{\frac{n}{4}}+\theta^{\frac{n}{2}}+\theta^{3\frac{n}{4}}}{4}, \\ \omega_3 = \frac{1+\theta^{\frac{n}{8}}+\theta^{\frac{n}{4}}+\theta^{3\frac{n}{8}}+\theta^{\frac{n}{2}}+\theta^{5\frac{n}{8}}+\theta^{6\frac{n}{8}}+\theta^{7\frac{n}{8}}}{8}, \end{cases}$$

e, de maneira geral, para $0 \leq i \leq l-1$ denotamos

$$\omega_i = \frac{\sum_{a=0}^{2^i-1} \theta^{\frac{an}{2^i}}}{2^i} \tag{6.2}$$

Também, para $1 \leq i \leq l-1$, podemos escrever ω_i em função do ω_{i-1}, da seguinte forma

$$\omega_i = \omega_{i-1}\left(\frac{1+\theta^{\frac{n}{2^i}}}{2}\right).$$

Note que o valor de ω_i obtido a partir i na Equação (6.2) coincide com o valor encontrado na Expressão (6.1) tomando o valor $q = i+1$ e $x = 0$. Assim, utilizando a notação expressa pela Equação (6.2), os elementos pertencentes à primeira classe, segundo a Definição 6.2, são os obtidos fazendo $i = 0$ e multiplicando-os por θ^x, onde $0 \leq x \leq \frac{n}{2} - 1$, ou seja, são os elementos $1, \theta, \ldots, \theta^{\frac{n}{2}-1}$; seguindo a mesma ideia, os elementos $\omega_1, \omega_1\theta, \ldots, \omega_1\theta^{\frac{n}{4}-1}$, obtidos fazendo $i = 1$ na Equação (6.2) e multiplicando-os por θ^x, estão na segunda classe, e assim sucessivamente.

Com isso em mente, considerando o corpo $\mathbb{L} = \mathbb{Q}(\theta)$ com $\theta = \sqrt[2^k]{d}$, com $d \neq 1$ um inteiro e livre de quadrados onde $d \equiv 2^l + 1 (mod\ 2^{l+1})$, com $2 \leq l \leq k$ ou $d \equiv 1 (mod\ 2^{k+1})$, uma base integral de $\mathbb{L}$ pode ser descrita, adotando a notação expressa pela Equação (6.2), da forma $\{1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^j, \omega_2, \omega_2\theta, \ldots, \omega_2\theta^j, \ldots, \omega_{l-1}, \omega_{l-1}\theta, \ldots \omega_{l-1}\theta^j\}$ onde $j = \frac{n}{2^i}$ se $i = l-1$ (o último) e $j = \frac{n}{2^{1+i}}$ se $i \neq l-1$. Mas, antes de provar esse fato, o qual consiste no nosso principal resultado, veremos algumas proposições e corolários que generalizam as Proposições 4.1 e 5.1, as quais são válidas para todo corpo de grau $n = 2^k$ e $d \equiv 1 (mod\ 2^l)$, onde $4 \leq l \leq k+1$ e l é a maior potência de 2 para o qual 2^l divide $d-1$, exceto quando $l = k+1$, e válidas também para todo $1 \leq j \leq l-1$. Para isso, consideramos $\mathbb{L} = \mathbb{Q}(\theta)$ e $\mathbb{K} = \mathbb{Q}(\theta^2)$, segundo a notação acima.

Proposição 6.3. *Considerando as notações acima, verifica-se*

$$\begin{aligned}
\omega_j^2 &= \omega_j + 2^{l-j-1}m(1 + \theta^{\frac{n}{2^j}} + \theta^{2\frac{n}{2^j}} + \theta^{3\frac{n}{2^j}} + \ldots + \theta^{(2^{j-1}-1)\frac{n}{2^j}} \\
&\quad + \omega_1 + \omega_1\theta^{\frac{n}{2^j}} + \ldots \omega_1\theta^{(2^{j-2}-1)\frac{n}{2^j}} + \ldots + \omega_{j-1}) \\
&= \omega_j + 2^{l-j-1}m\left(\sum_{f=1}^{j}\left(\sum_{i=0}^{2^{j-f}-1}\omega_{f-1}\theta^{\frac{n}{2^j}.i}\right)\right),
\end{aligned}$$

onde $m \in \mathbb{Z}$ é tal que, uma vez que $d \equiv 1 (mod\ 2^l)$, existe $m \in \mathbb{Z}$ tal que $d - 1 = 2^l m$.

Demonstração. Por um lado,

$$\begin{aligned}
\omega_j^2 &= \left(\frac{1+\theta^{\frac{n}{2^j}}+\theta^{\frac{2n}{2^j}}+\theta^{\frac{3n}{2^j}}+\ldots+\theta^{\frac{(2^j-1)n}{2^j}}}{2^j}\right)^2 \\
&= \frac{1+\theta^{\frac{2n}{2^j}}+\theta^{\frac{4n}{2^j}}+\theta^{\frac{6n}{2^j}}+\ldots+\theta^{\frac{(2^{j+1}-2)n}{2^j}}}{2^{2j}} + 2\left(\frac{\theta^{\frac{n}{2^j}}+\theta^{\frac{2n}{2^j}}+\theta^{\frac{3n}{2^j}}+\ldots+\theta^{\frac{(2^j-1)n}{2^j}}}{2^{2j}}\right) \\
&\quad +2\left(\frac{\theta^{\frac{3n}{2^j}}+\theta^{\frac{4n}{2^j}}+\theta^{\frac{5n}{2^j}}+\ldots+\theta^{\frac{(2^j-1)n}{2^j}}\theta^n}{2^{2j}}\right) \\
&\quad +2\left(\frac{\theta^{\frac{5n}{2^j}}+\theta^{\frac{6n}{2^j}}+\theta^{\frac{7n}{2^j}}+\ldots+\theta^{\frac{(2^j-1)n}{2^j}}\theta^n+\theta^{\frac{(2^j+1)n}{2^j}}}{2^{2j}}\right) \\
&\quad +\ldots+2\left(\frac{\theta^{\frac{(2^{j+1}-5)n}{2^j}}+\theta^{\frac{(2^{j+1}-4)n}{2^j}}}{2^{2j}}\right)+2\left(\frac{\theta^{\frac{(2^{j+1}-3)n}{2^j}}}{2^{2j}}\right).
\end{aligned} \tag{6.3}$$

Na Equação (6.3), a primeira fração representa cada termo elevado ao quadrado e, em seguida, cada somatória representa as multiplicações entre termos distintos, de modo que a primeira corresponde à multiplicação de 1 pelos demais termos, a segunda à multiplicação de $\theta^{\frac{n}{2^j}}$ por $\theta^{\frac{gn}{2^j}}$, com $g > 1$, e assim sucessivamente. Note que, no primeiro somatório, g é sempre par e que nos somatórios seguintes oriundos das multiplicações entre os termos diferentes, os termos $\theta^{\frac{gn}{2^j}}$ é sempre multiplicado por 2, ou seja, aparecem aos pares. Desse modo, sempre que g é impar o coeficiente de $\theta^{\frac{gn}{2^j}}$ é um número par e quando g é par, o coeficiente será ímpar. Vale ressaltar também que, a medida que o valor de g aumenta, o termo $\theta^{\frac{gn}{2^j}}$ aparece mais vezes na Equação (6.3), isso quando $0 \leq g \leq 2^j - 1$, devido ao resultado das multiplicações entre os termos. Por outro lado, a partir de $g = 2^j - 1$, a quantidade de termos vai diminuindo. Com isso em vista, vamos analisar quantas vezes cada $\theta^{\frac{gn}{2^j}}$, com $0 \leq g \leq 2^{j+1} - 2$ aparece na Equação (6.3), a fim de determinar qual será o inteiro multiplicando cada termo ao agrupá-los, ou seja, o seu coeficiente.

- $1 \rightarrow$ apenas 1 termo, na primeira somatória
- $\theta^{\frac{n}{2^j}} \rightarrow$ 2 termos: uma vez na segunda somatória, a qual é multiplicada por 2
- $\theta^{\frac{2n}{2^j}} \rightarrow$ 3 termos: uma vez na primeira somatória e uma vez na segunda somatória, a qual é multiplicada por 2
- $\theta^{\frac{3n}{2^j}} \rightarrow$ 4 termos: uma vez na segunda somatória e uma vez na terceira somatória, as quais são multiplicadas por 2

- $\theta^{\frac{4n}{2^j}} \to 5$ termos: uma vez na segunda somatória e uma vez na terceira somatória, as quais são multiplicadas por 2, e uma vez na primeira somatória
  $\vdots$

- $\theta^{\frac{(2^j-1)n}{2^j}} \to 2^j$ termos: uma vez em cada somatória, da segunda até a somatória que representa a multiplicação de $\theta^{\frac{(2^{j-1}-1)n}{2^j}}$ por $\theta^{\frac{gn}{2^j}}$, com $g > 2^{j-1}-1$, ou seja, $2.2^{j-1} = 2^j$ vezes, já que cada expressão é multiplicada por 2

- $\theta^{\frac{2^j n}{2^j}} \to 2^j - 1$ termos: uma vez na primeira somatória e $2(2^j-1)$ nas demais, pois aparece em todas as somatórias da terceira até a somatória que representa a multiplicação de $\theta^{\frac{(2^{j-1}-1)n}{2^j}}$ por $\theta^{\frac{gn}{2^j}}$, com $g > 2^{j-1}-1$

- $\theta^{\frac{(2^j+1)n}{2^j}} \to 2^j - 2$ termos: uma vez em cada somatória, da terceira até a somatória que representa a multiplicação de $\theta^{\frac{(2^{j-1}-1)n}{2^j}}$ por $\theta^{\frac{gn}{2^j}}$, com $g > 2^{j-1}-1$, ou seja, $2.(2^{j-1}-1) = 2^j - 2$ vezes, já que cada expressão é multiplicada por 2
  $\vdots$

- $\theta^{\frac{(2^{j+1}-4)n}{2^j}} \to 3$ termos: uma vez na primeira somatória e uma vez na penúltima somatória, a qual é multiplicada por 2

- $\theta^{\frac{(2^{j+1}-3)n}{2^j}} \to 2$ termos: uma vez na última somatória, a qual é multiplicada por 2

- $\theta^{\frac{(2^{j+1}-2)n}{2^j}} \to 1$ termo: uma vez na primeira somatória

Assim, obtemos

$$\begin{aligned} w_j^2 = \; & 1 + 2\theta^{\frac{n}{2^j}} + 3\theta^{\frac{2n}{2^j}} + 4\theta^{\frac{3n}{2^j}} + 5\theta^{\frac{4n}{2^j}} + \cdots + 2^j\theta^{\frac{(2^j-1)n}{2^j}} + (2^j-1)\theta^n \\ & + (2^j-2)\theta^{\frac{(2^j+1)n}{2^j}} + \cdots + 3\theta^{\frac{(2.2^j-4)n}{2^j}} + 2\theta^{\frac{(2-2j-3)n}{2^j}} + \theta^{\frac{(2^{j+1}-2)n}{2^j}}. \end{aligned} \tag{6.4}$$

Por outro lado,

$$\begin{aligned}
&\omega_j + 2^{l-j-1} m \left(\sum_{f=1}^{j} \left(\sum_{i=0}^{2^{j-f}-1} \omega_{f-1} \theta^{\frac{n}{2^j}.i} \right) \right) = \sum_{a=0}^{2^j-1} \frac{\theta^{\frac{an}{2^j}}}{2^j} \\
&+2^{l-j-1} \tfrac{\theta^n-1}{2^l} \left(\sum_{f=1}^{j} \left(\sum_{i=0}^{2^{j-f}-1} \sum_{a=0}^{2^{f-1}-1} \frac{\theta^{\frac{an}{2^{f-1}}}}{2^{f-1}} \theta^{\frac{n}{2^j}.i} \right) \right) \\
&= \sum_{a=0}^{2^j-1} \frac{\theta^{\frac{an}{2^j}}}{2^j} + \frac{\theta^n - 1}{2^{j+1}} \left(\sum_{f=1}^{j} \left(\sum_{i=0}^{2^{j-f}-1} \sum_{a=0}^{2^{f-1}-1} \frac{\theta^{\frac{(2^{j-f+1})na+ni}{2^j}}}{2^{f-1}} \right) \right) \\
&= \sum_{a=0}^{2^j-1} \frac{\theta^{\frac{an}{2^j}}}{2^j} + \left(\sum_{f=1}^{j} \left(\sum_{i=0}^{2^{j-f}-1} \sum_{a=0}^{2^{f-1}-1} \frac{\theta^{\frac{(2^{j-f+1})na+ni}{2^j}}}{2^{j+f}} (\theta^n - 1) \right) \right) \\
&= \sum_{a=0}^{2^j-1} \frac{\theta^{\frac{an}{2^j}}}{2^j} + \left(\sum_{f=1}^{j} \left(\sum_{i=0}^{2^{j-f}-1} \sum_{a=0}^{2^{f-1}-1} \frac{\theta^{\frac{n(2^{j-f+1}a+i+2^j)}{2^j}} - \theta^{\frac{n(2^{j-f+1}a+i)}{2^j}}}{2^{j+f}} \right) \right) \\
&= 2^j \sum_{a=0}^{2^j-1} \frac{\theta^{\frac{an}{2^j}}}{2^{2j}} + \left(\sum_{f=1}^{j} \left(\sum_{i=0}^{2^{j-f}-1} \sum_{a=0}^{2^{f-1}-1} 2^{j-f} \frac{\theta^{\frac{n(2^{j-f+1}a+i+2^j)}{2^j}} - \theta^{\frac{n(2^{j-f+1}a+i)}{2^j}}}{2^{2j}} \right) \right).
\end{aligned}$$

Repetimos o raciocínio utilizado anteriormente, onde analisamos o coeficiente de cada parcela $\theta^{\frac{gn}{2^j}}$, com $0 \leq g \leq 2^{j+1}-2$. Primeiramente, observamos que no primeiro somatório, cada $\theta^{\frac{gn}{2^j}}$, com $0 \leq g \leq 2^j - 1$, acompanha o coeficiente 2^j. Agora, no segundo somatório, devido à variação dos índices a, i e f em função do valor de j, a expressão $(2^{j-f+1}a+i+2^j)$ varia entre 2^j e $2^{j+1}-2$, ou seja, nas parcelas $\theta^{\frac{gn}{2^j}}$, com $2^j \leq g \leq 2^{j+1}-2$, para determinar seu coeficiente, basta analisar os valores de a, i e j de modo que se tenha $2^{j-f+1}a+i+2^j = g$, e somar os valores 2^{j-f} para cada f tal que se obtenha a igualdade. Agora, a expressão $2^{j-f+1}a + i$ assume valores de 0 a $2^j - 1$, de modo que para estabelecer os coeficientes de $\theta^{\frac{gn}{2^j}}$, com $0 \leq g \leq 2^j - 1$, devemos subtrair de 2^j, referente à primeira somatória, todos os termos 2^{j-f} tais que $2^{j-f+1}a+i = g$, ja que essa expressão é negativa. Fazendo essa análise para cada termo, obtemos todos os seus respectivos coeficientes. Vale ressaltar também que, a solução encontrada para os valores de a, i e f são os mesmos para $0 \leq g \leq 2^j - 1$ e $g+2^j$, porém para g substraímos todos os valores 2^{j-f} de 2^j e para $g+2^j$ apenas somamos os valores 2^{j-f}. Vejamos alguns exemplos:

- $1 \rightarrow$ apenas 1 termo: coeficiente 2^j da primeira somatória e, no segundo termo da segunda somatória, a expressão resulta em 1 para todo valor de $1 \leq f \leq j$ tal que $i = a = 0$, totalizando $2^j - 2^{j-1} - 2^{j-2} - \cdots - 2^{j-j} = 1$

- $\theta^{\frac{n}{2^j}} \rightarrow 2$ termos: coeficiente 2^j da primeira somatória e, no segundo termo da segunda somatória, para todo f excceto $f = j$ onde $a = 0$ e $i = 2$ ou $i = 0$ e $a = 1$, totalizando $2^j - 2^{j-1} - 2^{j-2} - \cdots - 2^{j-(j-1)} = 2$

$\vdots$

- $\theta^{\frac{n(2^{j+1}-2)}{2^j}} \to 1$ termo: só é possível obter no primeiro termo da segunda somatória quando $f = j$ e $i = 1$, ou seja, o coeficiente é 1

Repetindo o raciocínio para cada coeficiente, obtemos

$$\begin{aligned}\omega_j + 2^{l-j-1}m\left(\sum_{f=1}^{j}\left(\sum_{i=0}^{2^{j-f}-1}\omega_{f-1}\theta^{\frac{n}{2^j}.i}\right)\right) = \; & 1 + 2\theta^{\frac{n}{2^j}} + 3\theta^{\frac{2n}{2^j}} + 4\theta^{\frac{3n}{2^j}} + 5\theta^{\frac{4n}{2^j}} + \cdots + 2^j\theta^{\frac{(2^j-1)n}{2^j}} \\ & +(2^j-1)\theta^n + (2^j-2)\theta^{\frac{(2^j+1)n}{2^j}} + \cdots + 3\theta^{\frac{(2.2^j-4)n}{2^j}} \\ & +2\theta^{\frac{(2.2j-3)n}{2^j}} + \theta^{\frac{(2^{j+1}-2)n}{2^j}}.\end{aligned} \tag{6.5}$$

A partir das Equações (6.4) e (6.5), segue a igualdade.

□

Corolário 6.4. *Com as mesmas hipóteses.*

1. $\omega_j^2 \equiv \omega_j (mod\ 2\mathcal{O}_\mathbb{K})$, *para todo* $1 \leq j \leq l-2$
2. $\omega_{l-1}^2 \equiv \omega_{l-1} + 1 + \theta^{\frac{n}{2^{j-1}}} + \theta^{2\frac{n}{2^{j-1}}} + \theta^{3\frac{n}{2^{j-1}}} + \ldots + \theta^{(2^{j-1}-1)\frac{n}{2^{j-1}}} + \omega_1 + \omega_1\theta^{\frac{n}{2^{j-1}}} + \ldots$
$+\omega_1\theta^{(2^{j-2}-1)\frac{n}{2^{j-1}}} + \ldots + \omega_{l-2} (mod\ 2\mathcal{O}_\mathbb{K})$, *para* $2 \leq l \leq k$.

Demonstração. Da Proposição 6.3, segue que

$$\omega_j^2 = \omega_j + 2^{l-j-1}m\left(\sum_{f=1}^{j}\left(\sum_{i=0}^{2^{j-f}-1}\omega_{f-1}\theta^{\frac{n}{2^j}.i}\right)\right).$$

Assim, para $j < l-1$, substituindo j em 2^{l-j-1}, obtemos um múltiplo de 2 que multiplica um elemento de $\mathcal{O}_\mathbb{K}$, de onde vem a congruência do item 1. Agora, para $j = l-1$, $2^{l-j-1} = 2^0 = 1$, entretanto, para $2 \leq l \leq k$, m deve ser ímpar para que 2^l seja a maior potência de 2 que divide $d-1$, ou seja, $m \equiv 1(mod\ 2)$, de onde segue o item 2. □

Proposição 6.5. *Com as mesmas hipóteses.*

1. $\omega_j\theta^{\frac{n}{2^{j+1}}} = 2\omega_{j+1} - \omega_j$, *para todo* $1 \leq j \leq l-2$
2. $\omega_{l-1}\theta^{\frac{n}{2^{l-1}}} = \omega_{l-1} + 2m$.

Demonstração. Para o item 1, $2\omega_{j+1} - \omega_j = 2\omega_j(\frac{1+\theta^{\frac{n}{2^{j+1}}}}{2}) - \omega_j = \omega_j(1+\theta^{\frac{n}{2^{j+1}}} - 1) = \omega_j\theta^{\frac{n}{2^{j+1}}}$.

Para o item 2, por um lado,

$$\omega_{l-1}\theta^{\frac{n}{2^{l-1}}} = \left(\sum_{a=0}^{2^{l-1}-1} \frac{\theta^{\frac{an}{2^{l-1}}}}{2^{l-1}}\right)\theta^{\frac{n}{2^{l-1}}} = \sum_{a=0}^{2^{l-1}-1} \frac{\theta^{\frac{n(a+1)}{2^{l-1}}}}{2^{l-1}} = \sum_{a=1}^{2^{l-1}} \frac{\theta^{\frac{an}{2^{l-1}}}}{2^{l-1}}.$$

Por outro lado,

$$\omega_{l-1} + 2m = \sum_{a=0}^{2^{l-1}-1} \frac{\theta^{\frac{an}{2^{l-1}}}}{2^{l-1}} + 2\frac{\theta^n - 1}{2^l} = \sum_{a=0}^{2^{l-1}-1} \frac{\theta^{\frac{an}{2^{l-1}}}}{2^{l-1}} + \frac{\theta^n - 1}{2^{l-1}} = \sum_{a=1}^{2^{l-1}} \frac{\theta^{\frac{an}{2^{l-1}}}}{2^{l-1}}.$$

Com isso, segue a igualdade. □

Corolário 6.6. *Com as mesmas hipóteses.*

1. $\omega_j\theta^{\frac{n}{2^{j+1}}} \equiv \omega_j (mod\ 2\mathcal{O}_{\mathbb{K}})$, *para todo* $1 \leq j \leq l-2$

2. $\omega_{l-1}\theta^{\frac{n}{2^{l-1}}} \equiv \omega_{l-1} (mod\ 2\mathcal{O}_{\mathbb{K}})$.

Demonstração. Segue diretamente da Proposição 6.5. □

Proposição 6.7. *São válidas as seguintes congruências e igualdades*

1. $\omega_j^2(1+\theta^{\frac{n}{2^{j+1}}}) \equiv 2\omega_{j+1} (mod\ 4\mathcal{O}_{\mathbb{K}})$, *para todo* $1 \leq j \leq l-3$

2. $\omega_{l-2}^2(1+\theta^{\frac{n}{2^{l-1}}}) = 2m\left(\sum_{f=1}^{l-2}\left(\sum_{i=0}^{2^{l-2-f}-1}\omega_{f-1}\theta^{\frac{n}{2^{l-1}}.i}\right)\right) + 2\omega_{l-1}$

3. $\omega_{l-1}^2(1+\theta^{\frac{n}{2^{l-1}}}) = 2m\left(\sum_{f=1}^{l-1}\left(\sum_{i=0}^{2^{l-1-f}-1}\omega_{f-1}\theta^{\frac{n}{2^{l-1}}.i}\right) + \omega_{l-1}\right) + 2\omega_{l-1}.$

Demonstração. Provamos cada caso separadamente.

1. Neste caso, usando a Proposição 6.3 e o fato que para $1 \leq j \leq l-3$, o valor 2^{l-j-1} é um múltiplo de 4 e, em seguida, a Proposição 6.5, segue que

$$\omega_j^2(1+\theta^{\frac{n}{2^{j+1}}}) \equiv \omega_j(1+\theta^{\frac{n}{2^{j+1}}}) = \omega_j + \omega_j\theta^{\frac{n}{2^{j+1}}} = \omega_j + 2\omega_{j+1} - \omega_j = 2\omega_{j+1}.$$

2. Agora, utilizando a Proposição 6.3 e, em seguida, a Proposição 6.5, segue que

$$\begin{aligned}
\omega_{l-2}^2(1+\theta^{\frac{n}{2^{l-1}}}) &= \left(\omega_{l-2}+2m\left(\sum_{f=1}^{l-2}\left(\sum_{i=0}^{2^{l-2-f}-1}\omega_{f-1}\theta^{\frac{n}{2^{l-2}}.i}\right)\right)\right)(1+\theta^{\frac{n}{2^{l-1}}}) \\
&= \omega_{l-2}+\omega_{l-2}\theta^{\frac{n}{2^{l-1}}}+2m\sum_{f=1}^{l-2}\sum_{i=0}^{2^{l-2-f}-1}\omega_{f-1}\left(\theta^{\frac{n}{2^{l-2}}i}+\theta^{\frac{n(2i+1)}{2^{l-1}}}\right) \\
&= \omega_{l-2}+2\omega_{l-1}-\omega_{l-2}+2m\sum_{f=1}^{l-2}\sum_{i=0}^{2^{l-2-f}-1}\omega_{f-1}\left(\theta^{\frac{n(2i)}{2^{l-1}}}+\theta^{\frac{n(2i+1)}{2^{l-1}}}\right) \\
&= 2\omega_{l-1}+2m\sum_{f=1}^{l-2}\sum_{i=0}^{2^{l-1-f}-1}\omega_{f-1}\theta^{\frac{ni}{2^{l-1}}},
\end{aligned}$$

pois analisando o expoente de $\theta^{\frac{n(2i)}{2^{l-1}}}$, para $2i$, tomando cada valor de i expresso no somatório, obtemos todos os inteiros pares entre 0 e $2^{l-1-f}-2$, os quais multiplicam $\frac{n}{2^{l-1}}$ no expoente de θ, já em $\theta^{\frac{n(2i+1)}{2^{l-1}}}$, a expressão $n(2i+1)$ contém todos os valores ímpares de 1 até $2^{l-1-f}-1$, os quais mutiplicam $\frac{n}{2^{l-1}}$ no expoente de θ. Portanto, essa soma engloba todos os valores de i descritos no último somatório, de modo que a igualdade é válida.

3. Neste caso, primeiramente, utilizamos a Proposição 6.3 e, em seguida, utilizamos a Proposição 6.5, como segue

$$\begin{aligned}
\omega_{l-1}^2(1+\theta^{\frac{n}{2^{l-1}}}) &= \left(\omega_{l-1}+m\left(\sum_{f=1}^{l-1}\left(\sum_{i=0}^{2^{l-1-f}-1}\omega_{f-1}\theta^{\frac{n}{2^{l-1}}.i}\right)\right)\right)(1+\theta^{\frac{n}{2^{l-1}}}) \\
&= \omega_{l-1}+\omega_{l-1}\theta^{\frac{n}{2^{l-1}}}+m\sum_{f=1}^{l-1}\left(\sum_{i=0}^{2^{l-1-f}-1}\omega_{f-1}\left(\theta^{\frac{ni}{2^{l-1}}}+\theta^{\frac{n(i+1)}{2^{l-1}}}\right)\right) \\
&= \omega_{l-1}+\omega_{l-1}+2m+2m\sum_{f=1}^{l-1}\left(\sum_{i=1}^{2^{l-1-f}-1}\omega_{f-1}\theta^{\frac{ni}{2^{l-1}}}\right) \\
&\quad +m\sum_{f=1}^{l-1}\omega_{f-1}(\theta^0+\theta^{\frac{n(2^{l-1-f}-1+1)}{2^{l-1}}}) \\
&= 2\omega_{l-1}+2m+2m\sum_{f=1}^{l-1}\left(\sum_{i=1}^{2^{l-1-f}-1}\omega_{f-1}\theta^{\frac{ni}{2^{l-1}}}\right)
\end{aligned}$$

$$
\begin{aligned}
&+m\sum_{f=1}^{l-1}\omega_{f-1}(1+\theta^{\frac{n(2^{l-1-f})}{2^{l-1}}}) \\
= \;& 2\omega_{l-1}+2m+2m\sum_{f=1}^{l-1}\left(\sum_{i=1}^{2^{l-1-f}-1}\omega_{f-1}\theta^{\frac{ni}{2^{l-1}}}\right) \\
&+m\sum_{f=1}^{l-1}\omega_{f-1}(1+\theta^{\frac{n}{2^f}}).
\end{aligned}
$$

Agora, pela Proposição (6.5), segue que $\omega_{f-1}\theta^{\frac{n}{2^f}} = 2\omega_f - \omega_{f-1}$ para todo $1 \leq f \leq l-1$. Realizando essa substituição no último termo da equação acima, segue que $m\sum_{f=1}^{l-1}\omega_{f-1}(1+\theta^{\frac{n}{2^f}}) = 2m\sum_{f=1}^{l-1}\omega_f = 2m(\omega_1+\omega_2+\cdots+\omega_{l-1})$.

Logo,

$$
\begin{aligned}
\omega_{l-1}^2(1+\theta^{\frac{n}{2^{l-1}}}) &= 2\omega_{l-1}+2m+2m\sum_{f=1}^{l-1}\left(\sum_{i=1}^{2^{l-1-f}-2}\omega_{f-1}\theta^{\frac{ni}{2^{l-1}}}\right)+2m\sum_{f=1}^{l-1}\omega_f \\
&= 2m\left(\sum_{f=1}^{l-1}\left(\sum_{i=0}^{2^{l-1-f}-1}\omega_{f-1}\theta^{2^{k-l+2}.i}\right)+\omega_{l-1}\right)+2\omega_{l-1},
\end{aligned}
$$

o que prova a proposição. □

Proposição 6.8. $\omega_{l-2}\omega_{l-1}\theta^2 \equiv \omega_{l-2}\omega_{l-1} \pmod{2\mathcal{O}_{\mathbb{K}}}$

Demonstração. Seja o grau $n = 2^k$. Se $l = k$, pelo Corolário 6.6, segue que $\omega_{l-1}\theta^2 \equiv \omega_{l-1}$, donde segue o resultado. Agora, se $l = k+1$, pelo mesmo corolário, segue que $\omega_{l-1}\theta \equiv \omega_{l-1}$, donde concluímos a prova. □

Agora, estamos prontos para enunciar e demonstrar o principal resultado deste trabalho.

Teorema 6.9. *Seja* $\mathbb{L} = \mathbb{Q}(\theta)$, *onde* $\theta = \sqrt[2^k]{d}$, *com* $d \neq 1$ *um inteiro e livre de quadrados e* $k \geq 1$. *Uma base integral de* $\mathbb{L}$ *é dada por*

- $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ *se* $d \equiv 2, 3 (mod\ 4)$
- $\{1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^{\frac{n}{2}-1}\}$ *se* $d \equiv 5 (mod\ 8)$
- $\{1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^{\frac{n}{4}-1}, \omega_2, \omega_2\theta, \ldots, \omega_2\theta^{\frac{n}{4}-1}\}$ *se* $d \equiv 9 (mod\ 16)$
  $\vdots$
- $\{1, \theta, \theta^2, \ldots, \theta^{\frac{n}{2}-1}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^{\frac{n}{4}-1}, \omega_2, \omega_2\theta, \ldots, \omega_2\theta^{\frac{n}{8}-1}, \ldots, \omega_{k-2}, \omega_{k-2}\theta, \omega_{k-1}, \omega_k\}$ *se* $d \equiv 1 (mod\ 2^{k+1})$.

Em geral, podemos escrever uma base integral do corpo $\mathbb{L}$ *na forma*

$$\Big\{1,\theta,\theta^2,\ldots,\theta^{\frac{n}{2}-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{\frac{n}{4}-1},\omega_2,w_2\theta,\ldots,\omega_2\theta^{\frac{n}{8}-1},\omega_3,\omega_3\theta,\ldots,\omega_3\theta^{\frac{n}{16}-1},\ldots,$$

$$\omega_{l-2},\omega_{l-2}\theta,\ldots\omega_{l-2}\theta^{\frac{n}{2^{l-1}}-1},\omega_{l-1},\omega_{l-1}\theta,\ldots\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-1}\Big\},$$

se $d\equiv 1(mod\ 2^l)$ *sendo* 2^l *a maior potência de* 2 *que divide* $d-1$, *exceto quando* $k=l-1$ *e, de modo que os elementos da última classe são fixos, sempre descritos por* $\omega_{l-1},\omega_{l-1}\theta,\ldots\omega_{l-1}\theta^{\frac{n}{2^{l-1}-1}}$ *ou seja, se* $d\equiv 2^l+1(mod\ 2^{l+1})$ *para* $2\leq l\leq k$ *e* $d\equiv 1(mod\ 2^{k+1})$ *para* $l=k+1$.

Demonstração. O primeiro caso, $d\equiv 2,3(mod\ 4)$, já está incluído no Teorema 2.3. Para os demais, seguiremos o mesmo raciocínio utilizado nas provas dos casos particulares feitos nos Teoremas 3.1, 3.3 e 3.5, de modo que, como o Teorema já foi mostrado para $k=1,2,3$, essa prova será feita tomando $k\geq 4$. Desse modo, como as bases são obtidas a partir da base integral do corpo cujo grau é a potência de 2 anterior, essa base será obtida por recorrência. Neste caso, a maneira mais adequada e intuitiva de realizar a prova é através do Princípio de Indução Finita sobre o grau n, mais precisamente, sobre a potência de 2, conforme os passos a seguir.

Passo base: O Teorema vale para grau 16, de acordo com o Teorema 3.5.

Hipótese de indução: O resultado vale para k, ou seja, para grau $n=2^k$. Isso significa que uma base é dada segundo o Teorema 6.9, ou seja, é possível determinar $k+1$ bases distintas para o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[2^k]{d})$ a depender do valor da congruência de d.

Caso geral: Agora, provamos que o resultado é válido para $k+1$, ou seja, para grau $n=2^{k+1}$. Para isso, devemos mostrar que existem $k+2$ estruturas diferentes (incluindo a potente) para o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[2^{k+1}]{d})$, de acordo com a congruência de d, e, além disso, as mesmas são dadas conforme o Teorema 6.9, ou seja, devemos provar que uma base do anel de inteiros algébricos de $\mathbb{Q}(\theta)$, com $\theta=\sqrt[2^{k+1}]{d}$ é

$$\Big\{1,\theta,\theta^2,\theta^3,\theta^4,\theta^5,\ldots\theta^{2^k-1},\omega_1,\omega_1\theta,\omega_1\theta^2,\omega_1\theta^3,\omega_1\theta^4,\ldots\omega_1\theta^{2^{k-1}-1},\omega_2,\omega_2\theta,\ldots\omega_2\theta^{2^{k-2}-1},$$

$$\omega_3,\omega_3\theta,\ldots,\omega_3\theta^{2^{k-3}-1},\ldots,\omega_{l-2},\omega_{l-2}\theta,\ \ldots,\omega_{l-2}\theta^{2^{k-l}-1},\omega_{l-1},\omega_{l-1}\theta,\ \ldots,\omega_{l-1}\theta^{2^{k-l+2}-1}\Big\}$$

para cada um dos casos $d\equiv 2^l+1(mod\ 2^{l+1})$, onde $2\leq l\leq k+1$ e $d\equiv 1(mod\ 2^{k+2})$ ou, equivalentemente, $d\equiv 1(mod\ 2^l)$ com $2\leq l\leq k+2$ onde 2^l é a maior potência de 2 que divide $d-1$, exceto para $l=k+2$. Mas, se $l=2$ e $l=3$, o Teorema já está provado (ver Teoremas 4.2 e 5.2). Desse modo, nessa demonstração, consideraremos os casos $4\leq l\leq k+2$, sendo esses os valores de l referidos daqui em diante.

Chamando $\mathbb{L}=\mathbb{Q}(\theta)$, onde $\theta=\sqrt[2^{k+1}]{d}$ e $\mathbb{K}=\mathbb{Q}(\theta^2)=\mathbb{Q}(\sqrt[2^k]{d})$, uma vez que de acordo

com Hipótese de Indução e utilizando a notação $\theta^2 = \sqrt[2^k]{d}$, é válido que

$$\mathbb{Z}[1, \theta, \theta^2, \dots \theta^{2^k-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \dots \omega_1\theta^{2^{k-1}-1}, \dots, \omega_{l-1}, \omega_{l-1}\theta, \dots, \omega_{l-1}\theta^{2^{k-l}-1}] = \mathcal{O}_{\mathbb{K}}[\theta],$$

para todo $d \equiv 2^l + 1 (mod\ 2^{l+1})$, com $4 \leq l \leq k+1$, é suficiente mostrar, nesses casos, que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$. Agora, para o caso $l = k+2$, essa igualdade não se verifica, de modo que devemos mostrar que

$$\begin{aligned} \mathcal{O}_{\mathbb{L}} \;=\; & \mathbb{Z}[1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \dots \theta^{2^k-1}, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_1\theta^4, \dots \omega_1\theta^{2^{k-1}-1}, \omega_2, \\ & \omega_2\theta, \dots \omega_2\theta^{2^{k-2}-1}, \omega_3, \omega_3\theta, \dots, \omega_3\theta^{2^{k-3}-1}, \dots, \omega_{k+1}, \omega_{k+1}\theta, \dots, \omega_{k+1}\theta^{2^{k-l+2}-1}]. \end{aligned} \tag{6.6}$$

Sendo assim, a prova será dividida em duas partes, onde, na primeira, faremos a demonstração da igualdade $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$, para todo l entre 4 e $k+1$, a qual possuirá algumas ramificações no decorrer da prova, pois, como veremos, para alguns valores específicos de l decorrem certas particularidades (esse fato foi mencionado no início da Seção 4.1) e, para finalizar, mostramos a igualdade referida na Equação (6.6), onde a estratégia utilizada é similar às demais. Comecemos pelo primeiro caso, provando que as duas inclusões são válidas.

1. $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$. Para essa inclusão, seja $\eta \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{L}$. Como $\{1, \theta\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que existem $\alpha', \beta' \in \mathbb{K}$ tal que $\eta = \alpha' + \beta'\theta$. Pela Proposição 1.39, segue que $2\alpha', 2\beta' \in \mathcal{O}_{\mathbb{K}}$, de modo que existem $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ tais que $\alpha' = \frac{\alpha}{2}$ e $\beta' = \frac{\beta}{2}$. Logo, $2\eta = \alpha + \beta\theta$. Tomando a norma na extensão $\mathbb{L}/\mathbb{K}$ de ambos os lados e usando as propriedades contidas na Proposição 1.2, segue que

$$\alpha^2 - \beta^2\theta^2 \equiv 0 (mod\ 4\mathcal{O}_{\mathbb{K}}). \tag{6.7}$$

   Como α, $\beta \in \mathcal{O}_{\mathbb{K}}$ e, pela Hipótese de Indução, o conjunto $\{1, \theta^2, \theta^4, \theta^6, \dots, \theta^{2^k-2}, \omega_1, \omega_1\theta, \omega_1\theta^2, \omega_1\theta^3, \omega_1\theta^4, \dots \omega_1\theta^{2^{k-1}-2}, \omega_2, \omega_2\theta, \dots, \omega_2\theta^{2^{k-2}-2}, \omega_3, \omega_3\theta, \dots, \omega_3\theta^{2^{k-3}-2}, \dots, \omega_{l-1}, \omega_{l-1}\theta, \dots, \omega_{l-1}\theta^{2^{k-l+2}-2}\}$, com $\omega_j = \sum_{a=0}^{2^j-1} \frac{\theta^{\frac{an}{2^j}}}{2^j}$, onde $0 \leq j \leq l-1$, é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, segue que existem inteiros $a_i, b_i, 0 \leq i \leq 2^{k-1} - 1$ tais que

$$\begin{aligned} \alpha \;=\; & a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6 + \dots + a_{2^{k-1}-1}\theta^{2^k-2} + a_{2^{k-1}}\omega_1 + a_{2^{k-1}+1}\omega_1\theta^2 + \dots \\ & + a_{3.2^{k-2}-1}\omega_1\theta^{2^{k-1}-2} + a_{3.2^{k-2}}\omega_2 + a_{3.2^{k-2}+1}\omega_2\theta^2 + \dots \\ & + a_{7.2^{k-3}-1}\omega_2\theta^{2^{k-2}-2} + \dots + a_{2^k-2^{k-(l-1)}}\omega_{l-1} + \dots + a_{2^k-1}\omega_{l-1}\theta^{2^{k-(l-2)}-2} \end{aligned}$$

   e

$$\begin{aligned}\beta &= b_0 + b_1\theta^2 + b_2\theta^4 + b_3\theta^6 + \cdots + b_{2^{k-1}-1}\theta^{2^k-2} + b_{2^{k-1}}\omega_1 + b_{2^{k-1}+1}\omega_1\theta^2 + \ldots \\ &\quad + b_{3.2^{k-2}-1}\omega_1\theta^{2^{k-1}-2} + b_{3.2^{k-2}}\omega_2 + b_{3.2^{k-2}+1}\omega_2\theta^2 + \ldots \\ &\quad + b_{7.2^{k-3}-1}\omega_2\theta^{2^{k-2}-2} + \ldots + b_{2^k-2^{k-(l-1)}}\omega_{l-1} + \ldots + b_{2^k-1}\omega_{l-1}\theta^{2^{k-(l-2)}-2},\end{aligned}$$

onde a ultima classe é sempre dada pela expressão que multiplica ω_{l-1}. Pela lei de formação da base de $\mathcal{O}_{\mathbb{K}}$, a classe seguinte sempre possui a metade do número de elementos da classe anterior (exceto as duas últimas, que possuem o mesmo número de elementos). Assim, uma fórmula que descreve todos os elementos da soma que representa α é dada por

$$\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i\omega_{j-1}\theta^{2(i-(2^k-2^{k-j+1}))}$$

onde j varia entre 1 e $l-1$; e, para $j=l$, podemos escrever

$$\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} a_i\omega_{j-1}\theta^{2(i-(2^k-2^{k-l+1}))}$$

O mesmo vale para β, trocando os coeficientes a_i por b_i. Assim, podemos recorrer ao uso dos somatórios para denotar α e β mais concisamente, como segue abaixo

$$\alpha = \sum_{j=1}^{l-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i\omega_{j-1}\theta^{2(i-(2^k-2^{k-j+1}))}\right) + \sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} a_i\omega_{l-1}\theta^{2(i-(2^k-2^{k-l+1}))}$$

$$\beta = \sum_{j=1}^{l-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i\omega_{j-1}\theta^{2(i-(2^k-2^{k-j+1}))}\right) + \sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} b_i\omega_{l-1}\theta^{2(i-(2^k-2^{k-l+1}))}.$$

Substituindo esses valores na Equação (6.7), obtemos

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{l-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i^2\omega_{j-1}^2\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\ &\quad + \sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} a_i^2\omega_{l-1}^2\theta^{4(i-(2^k-2^{k-l+1}))} + 2(a_{ij}) \qquad (6.8) \\ &\quad - \sum_{j=1}^{l-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i^2\omega_{j-1}^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)\end{aligned}$$

$$- \sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} b_i^2 \omega_{l-1}^2 \theta^{4(i-(2^k-2^{k-l+1}))+2} - 2(b_{ij})\theta^2$$

$$\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}),$$

onde a_{ij} representa todas as multiplicações $a_i x$ por $a_j y$ com $i < j$ e b_{ij} representa todas as multiplicações de $b_i x$ por $b_j y$ com $i < j$ (note que $i < j \Rightarrow x \neq y$). Podemos também representar a_{ij} e b_{ij} em somatórios, da forma

$$\begin{aligned}
a_{ij} &= \sum_{j_1=1}^{l-1} \omega_{j_1-1} \sum_{i_1=(2^{j_1-1}-1)(2^{k-j_1+1})}^{(2^{j_1}-1)(2^{k-j_1})-1} \sum_{j_2=j_1+1}^{l-1} \omega_{j_2-1} \sum_{i_2=(2^{j_2-1}-1)(2^{k-j_2+1})}^{(2^{j_2}-1)(2^{k-j_2})-1} A^1 \\
&+ \sum_{j=1}^{l-1} \omega_{j-1}^2 \sum_{i_1=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j}-1)(2^{k-j})-2} \sum_{i_2=i_1+1}^{(2^{j}-1)(2^{k-j})-1} a_{i_1} a_{i_2} \theta^{2(i_1-(2^k-2^{k-j+1})+i_2-(2^k-2^{k-j+1}))} \\
&+ \sum_{j=1}^{l-1} \omega_{j-1} \sum_{i_1=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j}-1)(2^{k-j})-2} \sum_{i_2=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} A^2 \\
&+ \sum_{i_1=(2^{l-1}-1)(2^{k-l+1})}^{2^k-2} \sum_{i_2=i_1+1}^{2^k-1} a_{i_1} a_{i_2} \omega_{l-1}^2 \theta^{2(i_1-(2^k-2^{k-l+1})+2(i_2-(2^k-2^{k-l+1}))}
\end{aligned} \tag{6.9}$$

onde

$$A^1 = a_{i_1} a_{i_2} \theta^{2(i_1-(2^k-2^{k-j_1+1})+i_2-(2^k-2^{k-j_2+1}))}$$

e

$$A^2 = a_{i_1} a_{i_2} \omega_{l-1} \theta^{2(i_1-(2^k-2^{k-j+1})+2(i_2-(2^k-2^{k-l+1}))}$$

e

$$\begin{aligned}
b_{ij} &= \sum_{j_1=1}^{l-1} \omega_{j_1-1} \sum_{i_1=(2^{j_1-1}-1)(2^{k-j_1+1})}^{(2^{j_1}-1)(2^{k-j_1})-1} \sum_{j_2=j_1+1}^{l-1} \omega_{j_2-1} \sum_{i_2=(2^{j_2-1}-1)(2^{k-j_2+1})}^{(2^{j_2}-1)(2^{k-j_2})-1} B^1 \\
&+ \sum_{j=1}^{l-1} \omega_{j-1}^2 \sum_{i_1=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j}-1)(2^{k-j})-2} \sum_{i_2=i_1+1}^{(2^{j}-1)(2^{k-j})-1} b_{i_1} b_{i_2} \theta^{2(i_1-(2^k-2^{k-j+1})+i_2-(2^k-2^{k-j+1}))} \\
&+ \sum_{j=1}^{l-1} \omega_{j-1} \sum_{i_1=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j}-1)(2^{k-j})-2} \sum_{i_2=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} B^2
\end{aligned} \tag{6.10}$$

$$+\sum_{i_1=(2^{l-1}-1)(2^{k-l+1})}^{2^k-2}\ \sum_{i_2=i_1+1}^{2^k-1} b_{i_1}b_{i_2}\omega_{l-1}^2\theta^{2(i_1-(2^k-2^{k-l+1})+2(i_2-(2^k-2^{k-l+1}))} \quad \text{onde}$$

$$B^1 = b_{i_1}b_{i_2}\theta^{2(i_1-(2^k-2^{k-j_1+1})+i_2-(2^k-2^{k-j_2+1}))}$$

e

$$B^2 = b_{i_1}b_{i_2}\omega_{l-1}\theta^{2(i_1-(2^k-2^{k-j+1})+2(i_2-(2^k-2^{k-l+1}))}.$$

Reescrevendo a Equação (6.8) em termos da congruência módulo $2\mathcal{O}_{\mathbb{K}}$, obtemos

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \sum_{j=1}^{l-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i^2\omega_{j-1}^2\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
&\quad+\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} a_i^2\omega_{l-1}^2\theta^{4(i-(2^k-2^{k-l+1}))}\\
&\quad-\sum_{j=1}^{l-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i^2\omega_{j-1}^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)\\
&\quad-\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} b_i^2\omega_{l-1}^2\theta^{4(i-(2^k-2^{k-l+1}))+2}\\
&\quad\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned} \tag{6.11}$$

Nesse corpo, são válidas as seguintes congruências, segundo os Cololários 6.4 e 6.6

$$\begin{cases}
\theta^{2^k}\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}})\\
\omega_j^2\equiv\omega_j(mod\ 2\mathcal{O}_{\mathbb{K}}), \text{para todo } 1\le j\le l-2\\
\omega_{l-1}^2\equiv\sum_{j=1}^{l-1}\left(\sum_{i=0}^{2^{l-(j+1)}-1}\omega_{j-1}\theta^{2^{k-l+2}.i}\right)+\omega_{l-1}(mod\ 2\mathcal{O}_{\mathbb{K}}),\\
\omega_j\theta^{\frac{n}{2^{j+1}}}\equiv\omega_j(mod\ 2\mathcal{O}_{\mathbb{K}}), \text{para todo } 1\le j\le l-2\\
\omega_{l-1}\theta^{\frac{n}{2^{l-1}}}\equiv\omega_{l-1}, (mod\ 2\mathcal{O}_{\mathbb{K}})\\
x^2\equiv x(mod\ 2),\ \text{para todo } x\in\mathbb{Z}.
\end{cases} \tag{6.12}$$

Mas note que, ao substituir essas congruências na Equação (6.11), as substituições são feitas no termo médio de cada classe. Assim, podemos escrever essa expressão tomando o ponto médio entre os limites inferior e superior de cada somatório da

Equação (6.11), onde para o primeiro e para o terceiro somatórios, obtemos

$$\frac{(2^{j-1}-1)(2^{k-j+1})+(2^j-1)(2^{k-j})}{2}=\frac{2^{k-j}}{2}(2^j-1+(2^{j-1}-1)2)=$$
$$2^{k-j-1}(2^j-1+2^j-2)=2^{k-j-1}(2.2^j-3)=2^{k-j-1}(2^{j+1}-3).$$

Note também que, se $l=k+1$, os limites inferior e superior do segundo somatório da Equação (6.11) são ambos 2^k-1, o que significa que esse somatório se resume a um único termo, isto é,

$$\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} a_i^2\omega_{l-1}^2\theta^{4(i-(2^k-2^{k-l+1}))}=a_{2^k-1}\omega_k^2.$$

O mesmo ocorre no último somatório, o qual se resume em $b_{2^k-1}\omega_k^2\theta^2$. Além disso, tomando $j=l-1=k$ no primeiro somatório, o limite inferior é $i=(2^{k-1}-1)(2^1)=2^k-2$ ao passo que o limite superior é $(2^k-1)-1=2^k-2$, ou seja, para esses valores de j e l, esssa parcela do somatório também conterá apenas um termo, tal como no terceiro somatório. Observe ainda que, para $n=2^{k+1}$ e $l=k+1$, temos que $2^{k-l+2}=2^{k-k-1+2}=2$ e, consequentemente, a expressão $\sum_{j=1}^{l-1}\left(\sum_{i=0}^{2^{l-(j+1)}-1}\omega_{j-1}\theta^{2^{k-l+2}.i}\right)$, oriunda da fórmula para ω_{l-1}^2 expressa no Sistema (6.12), terá múltiplos de 2 e de 4. Por todas essas razões, faremos a primeira ramificação dessa etapa da demonstração, seguindo com a prova fixando o valor $l=k+1$ e, depois, retomamos aos demais casos. Sendo assim, uma vez que $\alpha^2-\beta^2\theta^2\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})$, utilizando as congruências contidas no Sistema (6.12) e as observações acima, a Equação (6.11), torna-se

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_{j-1}\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
&\quad+\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} a_i\omega_{j-1}\theta^{4(i-((2^{j+1}-3)(2^{k-j-1}))}\right)\\
&\quad+a_{2^k-2}\omega_{k-1}+a_{2^k-1}\left(\sum_{j=1}^{k}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{2.i}\right)+\omega_k\right)\\
&\quad-\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_{j-1}\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)
\end{aligned}$$

$$
\begin{aligned}
&-\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} b_i\omega_{j-1}\theta^{4(i-((2^{j+1}-3)(2^{k-j-1}))+2}\right)\\
&-b_{2^k-2}\omega_{k-1}\theta^2 - b_{2^k-1}\left(\sum_{j=1}^{k}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{2.i+2}\right)+\omega_k\theta^2\right)\\
&\equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}.
\end{aligned}
$$

Agora, utilizando novamente as congruências $\omega_j\theta^{\frac{n}{2^{j+1}}} \equiv \omega_j (mod\ 2\mathcal{O}_{\mathbb{K}})$, para todo $0 \leq j \leq k-1$ e $\omega_k\theta^2 \equiv \omega_k (mod\ 2\mathcal{O}_{\mathbb{K}})$, as quais estão contidas no Corolário 6.3, segue que

$$
\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_{j-1}\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
&\quad+\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} a_i\omega_{j-1}\theta^{4(i-((2^{j+1}-3)(2^{k-j-1}))}\right)\\
&\quad+a_{2^k-2}\omega_{k-1}+a_{2^k-1}\left(\sum_{j=1}^{k}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{2.i}\right)+\omega_k\right)\\
&\quad-\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_{j-1}\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)\\
&\quad-\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} b_i\omega_{j-1}\theta^{4(i-((2^{j+1}-3)(2^{k-j-1}))+2}\right)\\
&\quad-b_{2^k-2}\omega_{k-1}-b_{2^k-1}\left(\sum_{j=1}^{k}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{2.i}\right)+\omega_k\right)\\
&\equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}.
\end{aligned}
$$

Observe que, tomando o mesmo valor de j no primeiro e no segundo somatório, obtemos 2 coeficientes a_i diferentes, um em cada somatório, que multiplicam o mesmo elemento de $\mathcal{O}_{\mathbb{K}}$, exatamente como quando consideramos o mesmo valor j no quarto e no quinto somatórios. Assim, agrupando os termos iguais, obtemos uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e, portanto, os coeficientes devem ser congruentes a 0 módulo 2, de onde obtemos o sistema abaixo,

para todo $1 \leq j \leq k-1$ e $0 \leq h \leq 2^{k-j-1}-1$.

$$\begin{cases} a_{(2^{j-1}-1)(2^{k-j+1})+h} + a_{(2^{j+1}-3)(2^{k-j-1})+h} + a_{2^k-1} - b_{2^k-1} \equiv 0(mod\ 2) \\ -b_{(2^{j-1}-1)(2^{k-j+1})+h} - b_{(2^{j+1}-3)(2^{k-j-1})+h} + a_{2^k-1} - b_{2^k-1} \equiv 0(mod\ 2) \\ a_{2^k-2} - b_{2^k-2} + a_{2^k-1} - b_{2^k-1} \equiv 0(mod\ 2) \\ a_{2^k-1} - b_{2^k-1} \equiv 0(mod\ 2). \end{cases}$$

Dessas equações, obtemos as congruências

$$\begin{cases} a_{(2^{j-1}-1)(2^{k-j+1})+h} \equiv -a_{(2^{j+1}-3)(2^{k-j-1})+h}(mod\ 2) \\ b_{(2^{j-1}-1)(2^{k-j+1})+h} \equiv -b_{(2^{j+1}-3)(2^{k-j-1})+h}(mod\ 2) \\ a_{2^k-2} \equiv b_{2^k-2}(mod\ 2) \\ a_{2^k-1} \equiv b_{2^k-1}(mod\ 2). \end{cases} \tag{6.13}$$

Elevando ao quadrado e realizando os produtos, obtemos as conguências módulo 4 descritas a seguir

$$\begin{cases} a^2_{(2^{j-1}-1)(2^{k-j+1})+h} \equiv a^2_{(2^{j+1}-3)(2^{k-j-1})+h}(mod\ 4) \\ b^2_{(2^{j-1}-1)(2^{k-j+1})+h} \equiv b^2_{(2^{j+1}-3)(2^{k-j-1})+h}(mod\ 4) \\ a^2_{2^k-2} \equiv b^2_{2^k-2}(mod\ 4). \\ a^2_{2^k-1} \equiv b^2_{2^k-1}(mod\ 4). \\ a_{(2^{j-1}-1)(2^{k-j+1})+h} a_{(2^{j+1}-3)(2^{k-j-1})+h} \equiv -a^2_{(2^{j-1}-1)(2^{k-j+1})}(mod\ 4) \\ b_{(2^{j-1}-1)(2^{k-j+1})+h} b_{(2^{j+1}-3)(2^{k-j-1})+h} \equiv -b^2_{(2^{j-1}-1)(2^{k-j+1})}(mod\ 4). \end{cases} \tag{6.14}$$

Substituindo essas congruências na Equação (6.8), uma vez que $\alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}})$, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1} \left((1+\theta^{2^{k-(j-1)}})\omega^2_{j-1} \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i^2 \theta^{4(i-(2^k-2^{k-j+1}))} \right) \\ &\quad - \sum_{j=1}^{k-1} \left((1+2^{k-(j-1)})\omega^2_{j-1} \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i^2 \theta^{4(i-(2^k-2^{k-j+1}))+2} \right) \\ &\quad + 2b^*_{ij} - 2a^*_{ij} + (1-\theta^2)(a^2_{2^k-2}\omega^2_{k-1} + a^2_{2^k-1}\omega^2_k) \\ &\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}) \end{aligned} \tag{6.15}$$

onde a^*_{ij} e b^*_{ij} são as expressões obtidas das Equações (6.9) e (6.10), respectivamente, após substituir as congruências dos Sistemas (6.13) e (6.14) e são dadas por:

$$
\begin{aligned}
&a_{ij}^{*} = \\
&\sum_{j_1=1}^{l-1} \omega_{j_1-1} \sum_{i_1=(2^{j_1-1}-1)(2^{k-j_1+1})}^{(2^{j_1}-1)(2^{k-j_1})-1} \sum_{j_2=j_1+1}^{l-1} \omega_{j_2-1} \sum_{i_2=(2^{j_2-1}-1)(2^{k-j_2+1})}^{(2^{j_2}-1)(2^{k-j_2})-1} \\
&(a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j_1+1}+2^{k-j_2+1})} + a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j_1+1}+2^{k-j_1-1}+2^{k-j_2+1})} \\
&+a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j_1+1}+2^{k-j_1-1}+2^{k-j_2+1}+2^{k-j_2-1})} \\
&+a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j_1+1}+2^{k-j_2+1}+2^{k-j_2-1})}) \\
&+\sum_{j=1}^{l-1} \omega_{j-1}^2 \sum_{i_1=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-2} \sum_{i_2=i_1+1}^{(2^{j+1}-3)(2^{k-j-1})-1} (a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+2})} \\
&+a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+2}+2^{k-j-1})} + a_{i_1}a_{i_2}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+2}+2^{k-j-1}+2^{k-j-1})}) \\
&+\sum_{j=1}^{l-1} \omega_{j-1} \sum_{i_1=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j}-1)(2^{k-j})-2} \sum_{i_2=(2^{l-1}-1)(2^{k-l+1})}^{2^k-1} (a_{i_1}a_{i_2}\omega_{l-1}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+1}+2^{k-l+1})}) + \\
&a_{i_1}a_{i_2}\omega_{l-1}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+1}+2^{k-l+1}+2^{k-j-1})} + a_{i_1}a_{i_2}\omega_{l-1}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+1}+2^{k-l+1}+2^{k-l})} \\
&+a_{i_1}a_{i_2}\omega_{l-1}\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+1}+2^{k-l+1}+2^{k-j-1}+2^{k-l})} \\
&+ \sum_{i_1=(2^{l-1}-1)(2^{k-l+1})}^{2^k-2} \sum_{i_2=i_1+1}^{2^k-1} (a_{i_1}a_{i_2}\omega_{l-1}^2\theta^{2(i_1+i_2-2^{k+1}+2^{k-j+1}+2^{k-l+1})} \\
&+a_{i_1}a_{i_2}\omega_{l-1}^2(\theta^{2(i_1+i_2-2^{k+1}+2^{k-l+1}+2^{k-l+1}+2^{k-l})} + \theta^{2(i_1+i_2-2^{k+1}+2^{k-l+1}+2^{k-l+1}+2^{k-l}+2^{k-l})}))
\end{aligned}
\tag{6.16}
$$

de modo que a Equação (6.16) foi escrita para o caso geral, ou seja, para $4 \leq l \leq k+1$. Assim, para obter a_{ij}^{*} referente a esse caso, basta trocar l por $k+1$ nas somatórias. Alem disso, note que, se $l = k+1$, uma vez que $(2^{l-1}-1)(2^{k-l+1}) = 2^k-1$, na terceira somatória, o termo i_2 se resume ao elemento a_{2^k-1} e, além disso, não há elementos representados na quarta somatória, pois também, como observamos acima, essa classe é formada por um único elemento de modo que sua multiplicação por si mesmo já está expressa na Equação (6.15). Pelo mesmo motivo também não há elementos que multiplicam ω_{k-1}^2 além de a_{2^k-2}, também já representado na Equação (6.15). Para obter o valor de b_{ij}^{*}, basta trocar a por b na Equação (6.16), de tal maneira

que todas as observações feitas sobre a_{ij}^* se repetem quando olhamos para b_{ij}^*. Vale observar também, que o raciocínio exposto na Observação 4.3 se aplica à obtenção da Equação (6.16), para qualquer valor de l: a primeira e a terceira somatórias da Equação (6.9) se escrevem, cada uma, em 4 somatórias após as substituições contidas no Sistema (6.14), pois podemos substituir só o valor de i_1, só o valor de i_2, ambos, ou nenhum. Além do mais, sempre que trocamos o valor de i_h, é somado 2^{k-j_h-1} ao valor de i_h no expoente de θ, quando $1 \leq j_h \leq l-1$, devido à mudança de varíavel no índice da somatória, e quando $j_h = l$ (elementos da última classe), somamos 2^{k-l}. Agora, a segunda e a quarta somatórias da Equação (6.9) tornam-se 3 após substituirmos as congruências, pois por se tratar de multiplicações entre elementos da mesma classe e, sendo $i_1 < i_2$, não existe a possibilidade de substituir apenas i_1. Isso posto, como a Equação (6.15) está escrita em termos da congruência módulo $4\mathcal{O}_{\mathbb{K}}$, utilizaremos as congruências contidas na Proposição 6.7, além das igualdades compreendidas na Proposição 6.3, as quais seguem abaixo

$$\begin{cases} 1+\theta^{2^k} = 2\omega_1 \\ \omega_j^2(1+\theta^{k-j}) = 2\omega_{j+1}, 1 \leq j \leq l-3 = k-2 \\ \omega_{l-2}^2 = \omega_{k-1}^2 = \omega_{k-1} + 2m\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{4.i}\right)\right) \\ \omega_{l-1}^2 = \omega_k^2 = \omega_k + m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{2.i}\right)\right). \end{cases} \tag{6.17}$$

Primeiramente, analisemos como ficará a expressão $(1-\theta^2)(a_{2^k-2}^2\omega_{k-1}^2 + a_{2^k-1}^2\omega_k^2)$ ao substituir as igualdades correspondentes a ω_{k-1}^2 e ω_k^2 conforme o Sistema (6.17). Afirmamos que

$$\begin{aligned}(1-\theta^2)(a_{2^k-2}^2\omega_{k-1}^2 + a_{2^k-1}^2\omega_k^2) = \; & 2(a_{2^k-2}^2 - a_{2^k-2}^2\theta^2 + a_{2^k-2}^2\theta^4 - \ldots - a_{2^k-2}^2\theta^{2^k-2} \\ & + a_{2^k-2}^2\omega_1 - a_{2^k-2}^2\omega_1\theta^2 - \ldots - a_{2^k-2}^2\omega_1\theta^{2^{k-1}-2} \\ & + \ldots + a_{2^k-2}^2\omega_{l-2} - a_{2^k-2}^2\omega_{l-1} - a_{2^k-1}^2\omega_{l-1}).\end{aligned} \tag{6.18}$$

De fato,

$$\begin{aligned}&(1-\theta^2)(a_{2^k-2}^2\omega_{k-1}^2 + a_{2^k-1}^2\omega_k^2) \\ &= (1-\theta^2)\left(a_{2^k-2}^2\left(\omega_{k-1} + 2m\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{4.i}\right)\right)\right)\right)\end{aligned}$$

$$
\begin{aligned}
&+(1-\theta^2)\left(a_{2^k-1}^2\left(\omega_k+m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j}-1}\omega_{j-1}\theta^{2.i}\right)\right)\right)\right)\\
&=(1-\theta^2)\left(a_{2^k-2}^2\omega_{k-1}+2m\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j}-1}a_{2^k-2}^2\omega_{j-1}\theta^{4.i}\right)\right)\right)\\
&+(1-\theta^2)\left(a_{2^k-1}^2\omega_k+m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j}-1}a_{2^k-1}^2\omega_{j-1}\theta^{2.i}\right)\right)\right)=a_{2^k-2}^2\omega_{k-1}\\
&-a_{2^k-2}^2\omega_{k-1}\theta^2+2m\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j}-1}a_{2^k-2}^2\omega_{j-1}\theta^{4.i}\right)\right)\\
&-2m\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j}-1}a_{2^k-2}^2\omega_{j-1}\theta^{4.i+2}\right)\right)+a_{2^k-1}^2\omega_k-a_{2^k-1}^2\omega_k\theta^2\\
&+m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j}-1}a_{2^k-1}^2\omega_{j-1}\theta^{2.i}\right)\right)-m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j}-1}a_{2^k-1}^2\omega_{j-1}\theta^{2.i+2}\right)\right).
\end{aligned}
$$

Além disso, pela Proposição (6.5), segue que $\omega_j\theta^{\frac{n}{2^{j+1}}}=2\omega_{j+1}-\omega_j$ para todo $1\leq j\leq k-1$ e $\omega_k\theta^2=\omega_k+2m$. Fazendo essas substituições na última igualdade da equação acima, note que as expressões multiplicadas por $2m$ e $-2m$, respectivamente, abordam todos os termos do tipo $\omega_{j-1}\theta^{2i}$, onde o sinal alterna entre positivo quando $2i$ é múltiplo de 4, e negativo quando θ^{2i} não é múltiplo de 4 (nos extremos, ou seja, no primeiro valor de i na primeira somatória e no último valor de i na segunda somatória, para cada valor de j, utilizamos as congruências $\omega_j\theta^{\frac{n}{2^{j+1}}}=2\omega_{j+1}-\omega_j$, para todo $1\leq j\leq k-1$); agora, nas expressões que multiplicam m e $-m$, só restará o termo $a_{2^k-1}^2\omega_{k-1}$, pois os demais coincidem para $i+1$ e i, com $0\leq i\leq 2^{k-j}-2$, respectivamente, nas duas expressões e, quando $i=0$ na expressão que multiplica m e $i=2^{k-j}-1$ na expressão que multiplica m, ambas se anulam ao substituir as congruências $\omega_j\theta^{\frac{n}{2^{j+1}}}=2\omega_{j+1}-\omega_j$ para todo $1\leq j\leq k-1$. Isso posto, obtemos

$$
\begin{aligned}
&(1-\theta^2)(a_{2^k-2}^2\omega_{k-1}^2+a_{2^k-1}^2\omega_k)\\
&=2(a_{2^k-2}^2-a_{2^k-2}^2\theta^2+a_{2^k-2}^2\theta^4-\ldots-a_{2^k-2}^2\theta^{2^k-2}+a_{2^k-2}^2\omega_1-a_{2^k-2}^2\omega_1\theta^2-\ldots\\
&-a_{2^k-2}^2\omega_1\theta^{2^{k-1}-2}+\ldots+a_{2^k-2}^2\omega_{k-1}-a_{2^k-2}^2\omega_{k-2}-a_{2^k-1}^2\omega_{k-1})\\
&=2m\left(\sum_{j=1}^{l-2=k-1}\left(\sum_{i=0}^{(2^j-1)(2^{k-j-1})-1}a_{2^k-2}^2\omega_{j-1}(-1)^i\theta^{2i}\right)-a_{2^k-2}^2\omega_k-a_{2^k-1}^2\omega_{k-1}\right).
\end{aligned}
$$

Assim, realizando as substituições das igualdades contidas no Sistema (6.17) e na Equação (6.18) na Equação (6.15), segue que

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1}\left(2\omega_j \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i^2\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\
&\quad -\sum_{j=1}^{k-1}\left(2\omega_j \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right) \\
&\quad +2b_{ij}^* - 2a_{ij}^* + 2m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{(2^j-1)(2^{k-j-1})-1} a_{2^k-2}^2\omega_{j-1}(-1)^i\theta^{2i}\right)\right. \\
&\quad \left.-a_{2^k-2}^2\omega_k - a_{2^k-1}^2\omega_k\right) \\
&\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}})
\end{aligned} \tag{6.19}$$

Como todos os termos da Equação (6.19) estão multiplicados por 2, podemos utilizar o fato que $2x \equiv 1 \pmod 4 \Rightarrow x \equiv 1 \pmod 2$, donde obtemos

$$\begin{aligned}
\alpha^2 - \beta^2 &= \sum_{j=1}^{k-1}\omega_j\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i^2\theta^{4(i-(2^k-2^{k-j+1}))}\right) - a_{ij}^* \\
&\quad \sum_{j=1}^{k-1}\omega_j\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right) + b_{ij}^* \\
&\quad +m\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{(2^j-1)(2^{k-j-1})-1} a_{2^k-2}^2\omega_{j-1}(-1)^i\theta^{2i}\right) - a_{2^k-2}^2\omega_k - a_{2^k-1}^2\omega_k\right) \\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned} \tag{6.20}$$

Como ainda há elementos que não pertencem à base de $\mathcal{O}_{\mathbb{K}}$ multiplicando os coeficientes a_i e b_i na Equação (6.20), utilizamos novamente as congruências módulo 2 contidas no Corolário 6.6, onde novamente tomamos o termo médio da primeira e da segunda somatória da Equação (6.20), da seguinte forma:

$$\frac{(2^{j-1}-1)(2^{k-j+1}) + (2^{j+1}-3)(2^{k-j-1})}{2} = \frac{2^{k-j-1}}{2}(2^{j+1} - 3 + (2^{j-1}-1)2^2) =$$
$$2^{k-j-2}(2^{j+1} - 3 + 2^{j+1} - 4) = 2^{k-j-2}(2^{j+2} - 7),$$

exceto para $j = k-1$, pois nesse caso há um único elemento que a representa, $2^k - 4$, não sendo necessário utilizar as congruências. Além disso, após substituir as congruências compreendidas nos Corolários 6.4, 6.6 e 6.8, a parte referente a a_{ij}^* e b_{ij}^* resume-se em

$$\left(\sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i \theta^{4i+2^{k-j}(9-2^{2+j})}\right)\right) \tag{6.21}$$

e

$$\left(\sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i \theta^{4i-2^{k-j}(9-2^{2+j})+2}\right)\right), \tag{6.22}$$

respectivamente, ou seja, ambas contêm apenas as somatórias que representam multiplicações de mesma classe e com $i_1 = i_2$ (análogo à Observação 4.5). Realizando todos os processos descritos acima, além dos fatos que $x^2 \equiv x \pmod 2$, para todo $x \in \mathbb{Z}$ e $m \equiv 1 \pmod 2$, da Equação (6.20), obtemos a seguinte expressão

$$\begin{aligned}
\alpha^2 - \beta^2\theta^2 \quad = \quad & \sum_{j=1}^{k-2} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{2^{k-j-2}(2^{j+2}-7)-1} a_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\
& + \sum_{j=1}^{k-2} \left(\sum_{i=2^{k-j-2}(2^{j+2}-7)}^{2^{k-j-1}(2^{j+1}-3)-1} a_i\omega_j\theta^{4(i-(2^{k-j-2}(2^{j+2}-7))}\right) + a_{2^k-4}\omega_{k-1} \\
& - \left(\sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i \theta^{4i+2^{k-j}(9-2^{2+j})}\right)\right) \\
& - \sum_{j=1}^{k-2} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))+2}\right) \\
& - \sum_{j=1}^{k-2} \left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))+2}\right) \\
& + \left(\sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i \theta^{4i-2^{k-j}(9-2^{k+2})+2}\right)\right) \\
& + \sum_{j=1}^{l-2=k} \left(\sum_{i=0}^{(2^j-1)(2^{k-j-1})-1} a_{2^k-2}\omega_{j-1}(-1)^i\theta^{2i}\right) - a_{2^k-2}\omega_k - a_{2^k-1}\omega_k \\
\equiv \quad & 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned} \tag{6.23}$$

Note ainda que, analisando as Equações (6.21) e (6.22), as quais representam a terceira e a sexta somatórias da Equação (6.23), tomando $i = (2^{j+2}-7)(2^{k-j-2})$, as expressões correspondentes ao expoente do θ resultam em $4.(2^{j+2}-7)(2^{k-j-2}) + (9-2^{j+2})2^{k-j} = 4(2^k - 7.2^{k-j-2}) + 9.2^{k-j} - 2^{k+2} = -7.2^{k-j} + 9.2^{k-j}) = 2^{k-j-1}$ e, $2^{k-j-1}+2$, respectivamente. Assim, substituindo na Equação (6.23) as congruências $\omega_j\theta^{2^{k-j}} \equiv \omega_j \pmod{2\mathcal{O}_{\mathbb{K}}}$, com $0 \leq j \leq k-2$, segue que

$$
\begin{aligned}
\alpha^2 - \beta^2\theta^2 \;=\; & \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{2^{k-j-2}(2^{j+2}-7)-1} a_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\
& + \sum_{j=1}^{k-2}\left(\sum_{i=2^{k-j-2}(2^{j+2}-7)}^{2^{k-j-1}(2^{j+1}-3)-1} a_i\omega_j\theta^{4(i-(2^{k-j-2}(2^{j+2}-7))}\right) \\
& + a_{(2^{k-2}-1)(2^{k-k+2})}\omega_{k-1} \\
& - \left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-j-1}}\right)\right) \\
& - \sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\theta^{4(i-(2^{j+2}-7)(2^{k-j-2}))}\right) \\
& - a_{(2^{k-2}-1)(2^{k-k+2})}\omega_{k-2} \\
& - \sum_{j=1}^{k-2}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))+2}\right) \\
& - \sum_{j=1}^{k-2}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))+2}\right) \\
& + \left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-j-1}+2}\right)\right) \\
& + \sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\theta^{4(i-(2^{j+2}-7)(2^{k-j-2})+2}\right)
\end{aligned}
\tag{6.24}
$$

$$+\sum_{j=1}^{l-2=k}\left(\sum_{i=0}^{(2^j-1)(2^{k-j-1})-1} a_{2^k-2}\omega_{j-1}(-1)^i\theta^{2i}\right) - a_{2^k-2}\omega_k - a_{2^k-1}\omega_k$$

$$\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})$$

Finalmente, obtemos uma combinação linear dos elementos da base de $\mathcal{O}_{\mathbb{K}}$ onde todos os coeficientes são inteiros. Agora, para concluir o nosso primeiro objetivo, resta mostrar que esses inteiros são todos pares. Para isso, vamos observar alguns fatos sobre a Equação (6.24) a fim de agrupar os coeficientes que multiplicam o mesmo elemento da base. Note que, o mesmo valor para j nas duas primeiras somatórias geram dois valores distintos de a_i multiplicando o mesmo elemento e, como as referidas somatórias se iniciam em $j = 1$, as mesmas não possuem elementos da primeira classe (ou seja, que multiplicam θ^i). Já a terceira somatória contém todos os elementos da base referentes à segunda metade de cada classe (até ω_{k-3}) e cujo θ possui expoente múltiplo de 4, ou seja, os elementos do tipo $\omega_{j-1}\theta^{4i+2^{k-j-1}}$, onde $1 \leq j \leq k-2$, enquanto na quarta somatória os intervalos fornecem todos os elementos referentes à primeira metade de cada classe (até ω_{k-3}), com a mesma condição no expente de θ. A mesma coisa vale para os elementos cujo expoente de θ é múltiplo de 2, quando analisamos a sétima e a oitava somatórias. Note também que, o termo a_{2^k-2} multilica todos os elementos da base, devido à última somatória, enquanto a_{2^k-1} multiplica apenas ω_k. Vale observar também que, na primeira, segunda, quinta e sexta somatórias o intervalo de j inicia-se em 1 e a variável é ω_j, enquanto nas demais somatórias, o intervalo de j inicia-se no mesmo valor, porém o substituímos em ω_{j-1}. Esse fato será utilizado na resolução do Sistema (6.25). Após essa análise, agrupando os termos, obtemos o sistema abaixo, válido para todo $0 \leq i \leq 2^{k-2}-1, 1 \leq j \leq k-3$ e $\leq h \leq 2^{k-j-3}$.

$$\begin{cases}
a_{2^k-2} - a_i \equiv 0(mod\ 2), -b_{2^k-2} + b_i \equiv 0(mod\ 2) \\
a_{(2^{j-1}-1)(2^{k-j+1})+h} + a_{2^{k-j-2}(2^{j+2}-7)+h} - a_{2^{k-j-3}(2^{j+3}-7)+h} + a_{2^k-2} \equiv 0(mod\ 2) \\
-b_{(2^{j-1}-1)(2^{k-j+1})+h} - b_{2^{k-j-2}(2^{j+2}-7)+h} + b_{2^{k-j-3}(2^{j+3}-7)+h} + a_{2^k-2} \equiv 0(mod\ 2) \\
a_{(2^{j-1}-1)(2^{k-j+1})+2^{k-j-3}+h} + a_{2^{k-j-2}(2^{j+2}-7)+2^{k-j-3}+h} - a_{2^{k-j}(2^j-1)+h} + a_{2^k-2} \\
\equiv 0(mod\ 2) \\
-b_{(2^{j-1}-1)(2^{k-j+1})+2^{k-j-3}+h} - b_{2^{k-j-2}(2^{j+2}-7)+2^{k-j-3}+h} + b_{2^{k-j}(2^j-1)+h} + a_{2^k-2} \\
\equiv 0(mod\ 2) \\
a_{2^k-8} + a_{2^k-7} + a_{2^k-2} + b_{2^k-4} \equiv 0(mod\ 2) \\
-b_{2^k-8} - b_{2^k-7} + a_{2^k-2} + b_{2^k-4} \equiv 0(mod\ 2) \\
a_{2^k-4} + a_{2^k-2} - b_{2^k-4} \equiv 0(mod\ 2), -a_{2^k-2} - a_{2^k-1} \equiv 0(mod\ 2).
\end{cases} \tag{6.25}$$

Das primeiras equações, obtemos $a_{2^k-2} \equiv a_0 \equiv a_1 \equiv a_2 \equiv \ldots \equiv a_{2^{k-2}-1}(mod\ 2)$ e $b_{2^k-2} \equiv b_0 \equiv b_1 \equiv b_2 \equiv \ldots \equiv b_{2^{k-2}-1}(mod\ 2)$. Substituindo $a_{2^k-2} \equiv a_0 \equiv a_1 \equiv a_2 \equiv \ldots \equiv a_{2^{k-2}-1}(mod\ 2)$ na terceira linha, seguindo a ordem crescente dos valores de j, obtemos $a_{2^{k-j-2}(2^{j+2}-7)+h} \equiv a_{2^{k-j-3}(2^{j+3}-7)+h}$, pois, note que, se $j = 1$, sempre que $i = h$, verifica-se $a_{2^{k-j-2}(2^{j+2}-7)+h} = a_i$, donde vem $a_{2^{k-j-2}(2^{j+2}-7)+h} \equiv a_{2^{k-j-3}(2^{j+3}-7)+h}$ para $j = 1$; se $j = 2, a_{2^{k-j-3}(2^{j+3}-7)+h} = a_{2^{k-(j+1)-2}(2^{(j+1)+2}-7)+h}$ de onde obtemos, ao substituir a congruência obtida quando $j = 1$, que $a_{2^{k-j-2}(2^{j+2}-7)+h} \equiv a_{2^{k-j-3}(2^{j+3}-7)+h}$ para $j = 2$. Em resumo, $a_{2^{k-j-3}(2^{j+3}-7)+h}$ e $a_{2^{k-j-2}(2^{j+2}-7)+h}$ coincidem tomando, respectivamente, j e $j+1$, de modo que a congruência obtida para o valor de j pode ser substituída na equação correspondente a $j+1$, pois dois dos quatro termos serão iguais (esse fato decorre dos intervalos das somatórias correspondentes aos valores de i na primeira e terceira, e segunda e quarta somatórias serem iguais, e do fato que uma multiplica ω_j e a outra ω_{j-1}, como mencionamos acima). Assim, substituindo linha a linha, tanto as congruências obtidas para a_i como as congruências obtidas para b_i, segue que todos os coeficientes a_i e b_i contidos no Sistema (6.25) são pares, donde, ao substituir no Sistema (6.13) obtemos $a_i, b_i \equiv 0 \pmod 2$ para todo $0 \leq i \leq 2^k - 1$, ou seja, a_i, b_i são todos pares, donde segue que, para para grau $n = 2^{k+1}$ e $d \equiv 1(mod\ 2^{k+1})$, a inclusão $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$ é válida. Agora voltemos para os demais valores de l. Para $d \equiv 1(mod\ 2^l)$, com $4 \leq l \leq k$, temos que $\frac{n}{2^{l-1}} \geq 4$, então substituindo as congruências dada pelo Sistema (6.12) e tomando os termos médios de cada somatória na Equação (6.11), obtemos

$$
\begin{aligned}
\alpha^2 - \beta^2\theta^2 = & \sum_{j=1}^{l-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i \omega_{j-1} \theta^{4(i-(2^k-2^{k-j+1}))} \right) \\
& + \sum_{j=1}^{l-1} \left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} a_i \omega_{j-1} \theta^{4(i-(2^{j+1}-3)(2^{k-j-1}))} \right) \\
& + \left(\sum_{j=1}^{l-1} \left(\sum_{q=0}^{2^{l-(j+1)}-1} \omega_{j-1} \theta^{2^{k-l+2}.q} \right) + \omega_{l-1} \right) \left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^{k-l}(2^l-1)-1} a_i \theta^{4(i-(2^k-2^{k-l+1}))} \right) \\
& + \left(\sum_{j=1}^{l-1} \left(\sum_{q=0}^{2^{l-(j+1)}-1} \omega_{j-1} \theta^{2^{k-l+2}.q} \right) + \omega_{l-1} \right) \left(\sum_{i=(2^{k-l})(2^l-1)}^{2^k-1} a_i \theta^{4(i-(2^{k-l})(2^l-1))} \right) \\
& - \sum_{j=1}^{l-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i \omega_{j-1} \theta^{4(i-(2^k-2^{k-j+1}))+2} \right) \\
& - \sum_{j=1}^{l-1} \left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j-1})-1} b_i \omega_{j-1} \theta^{4(i-((2^j-1)(2^{k-j-1})))+2} \right)
\end{aligned}
$$

$$
\begin{aligned}
&- \left(\sum_{j=1}^{l-1}\left(\sum_{q=0}^{2^{l-(j+1)}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)+\omega_{l-1}\right)\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^{k-l}(2^l-1)-1} b_i\theta^{4(i-(2^k-2^{k-l+1})+2}\right)\\
&- \left(\sum_{j=1}^{l-1}\left(\sum_{q=0}^{2^{l-(j+1)}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)+\omega_{l-1}\right)\left(\sum_{i=(2^{k-l})(2^l-1)}^{2^{k-1}} b_i\theta^{4(i-(2^{k-l})(2^l-1))+2}\right)\\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).
\end{aligned}
$$

Note que, agrupando os termos semelhantes, obtemos uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e, portanto, os coeficientes devem ser congruentes a 0 módulo 2. Observe também que, novamente, o mesmo valor de j fornece 2 coeficientes diferentes que são mutliplicados pelo mesmo elemento da base nas seguintes somatórias: primeira e segunda, terceira e quarta, quinta e sexta, e sétima e oitava. Vale observar também que, variando os valores de j e de i na primeria e na segunda somatória, obtemos todos os elementos da base de $\mathcal{O}_{\mathbb{K}}$ tal que o expoente de θ é um múltiplo de 4, exceto os da última classe, já que j varia até $l-1$; do mesmo modo, a quarta e a quinta somatória abrangem todos os elementos da base de $\mathcal{O}_{\mathbb{K}}$, exceto os da última classe, cujo o expoente de θ é múltiplo de 2 e não é múltiplo de 4. Além disso, a terceira e a quarta somatória abrangem todos os elementos cujo expoente do θ é um múltiplo de 4, inclusive os da última classe; e as duas últimas somatórias contém todos os elementos em que o expoente de θ é múltiplo de 2 mas não é múltiplo de 4. À vista disso, obtemos as congruências listadas no sistema abaixo, para todo $1 \leq j \leq l-1$ e $0 \leq h \leq 2^{k-j-1}-1$:

$$
\begin{cases}
a_{(2^{j-1}-1)(2^{k-j+1})+h} \equiv -a_{(2^{j+1}-3)(2^{k-j-1})+h}(mod\ 2)\\
b_{(2^{j-1}-1)(2^{k-j+1})+h} \equiv -b_{(2^{j+1}-3)(2^{k-j-1})+h}(mod\ 2)\\
a_{2^k-2^{k-l+1}+h'} \equiv -a_{2^{k-l}(2^l-1)+h'}(mod\ 2), 0 \leq h' \leq 2^{k-l}-1\\
b_{2^k-2^{k-l+1}+h'} \equiv -b_{2^{k-l}(2^l-1)+h'}(mod\ 2), 0 \leq h' \leq 2^{k-l}-1.
\end{cases}
\tag{6.26}
$$

Elevando os termos ao quadrado e efetuando os devidos produtos, obtemos as congruências módulo 4, as quais substituindo em $\alpha^2-\beta^2\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}})$, obtemos

$$
\begin{aligned}
\alpha^2-\beta^2\theta^2 \;=\; &\sum_{j=1}^{l-1}\left((1+\theta^{2^{k-(j-1)}})\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i^2\omega_{j-1}^2\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
&+\omega_{l-1}^2(1+\theta^{2^{k-l+2}})(a_{2^k-2^{k-l+1}}^2+a_{2^k-2^{k-l+2}+1}^2+\ldots+a_{(2^l-1)(2^{k-l})}^2)
\end{aligned}
\tag{6.27}
$$

$$-\sum_{j=1}^{l-1}\left((1+2^{k-(j-1)})\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i^2\omega_{j-1}^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)$$

$$-\omega_{l-1}^2(1+\theta^{2^{k-l+2}})(b^2_{2^k-2^{k-l+1}}+b^2_{2^k-2^{k-l+2}+1}+\ldots+b^2_{(2^l-1)(2^{k-l})})$$

$$-2a_{ij}^*+2b_{ij}^*\theta^2\equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}),$$

onde a_{ij}^* é dado por (6.16) e b_{ij}^* é a mesma expressão trocando a por b.

De acordo com a Proposição 6.7, verificam-se as igualdades abaixo

$$\begin{cases}
\omega_j^2(1+\theta^{2^{k-(j-1)}})=2\omega_{j+1}, \quad \text{para} \quad 0\leq j\leq l-3 \\
\omega_{l-2}^2(1+\theta^{2^{k-l+2}})=\left(\omega_{l-2}+2m\sum_{j=1}^{l-2}\sum_{q=0}^{2^{l-2-j}-1}\omega_{j-1}\theta^{2^{k-l+3}.q}\right)(1+\theta^{2^{k-l+2}})= \\
=2m\left(\sum_{j=1}^{l-2}\left(\sum_{q=0}^{2^{l-1-j}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)+2\omega_{l-1} \\
\omega_{l-1}^2(1+\theta^{2^{k-l+2}})=\left(\omega_{l-1}+m\sum_{j=1}^{l-1}\sum_{q=0}^{2^{l-1-j}-1}\omega_{j-1}\theta^{2^{l-1-l+2}.q}\right)(1+\theta^{2^{k-l+2}})= \\
=2m\left(\sum_{j=1}^{l-1}\left(\sum_{q=0}^{2^{l-1-j}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)+\omega_{l-1}\right)+2\omega_{l-1},
\end{cases}$$

onde $m\in\mathbb{Z}$ é tal que, como $d\equiv 1(mod\ 2^l)$ e $d\not\equiv 1(mod\ 2^{l+1})$, existe $m\in\mathbb{Z}$ ímpar tal que $m-1=2^lm$. Substituindo-as na Equação (6.27), note que todos os termos ficam multiplicados por 2, donde podemos reduzir a congruência para módulo $2\mathcal{O}_{\mathbb{K}}$, donde segue que

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 \;=\; & \sum_{j=1}^{l-2}\left(\omega_j\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1}a_i^2\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\
& +\left(\sum_{j=1}^{l-2}\left(\sum_{q=0}^{2^{l-1-j}-1}m\omega_{j-1}\theta^{2^{k-l+2}.q}\right)+\omega_{l-1}\right)A_1 \\
& +\left(\sum_{j=1}^{l-1}m\left(\sum_{q=0}^{2^{l-1-j}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}+\omega_{l-1}\right)+\omega_{l-1}\right)A_2 \\
& -\sum_{j=1}^{k-1}\left(\omega_j\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1}b_i^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)
\end{aligned} \tag{6.28}$$

$$+\left(\sum_{j=1}^{l-2}\left(\sum_{q=0}^{2^{l-1-j}-1} m\omega_{j-1}\theta^{2^{k-l+2}.q}\right)+\omega_{l-1}\right)A_3$$

$$+\left(\sum_{j=1}^{l-1} m\left(\sum_{q=0}^{2^{l-1-j}-1} \omega_{j-1}\theta^{2^{k-l+2}.q}+\omega_{l-1}\right)+\omega_{l-1}\right)A_4$$

$$-a_{ij}^{*}+b_{ij}^{*}\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).$$

onde

$$A_1=\left(\sum_{i=(2^{l-2}-1)(2^{k-l+2})}^{(2^l-3)(2^{k-l})-1} a_i^2\theta^{4(i-(2^k-2^{k-l+2})}\right), A_2=\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^{k-l}(2^l-1)-1} a_i^2\theta^{4(i-(2^k-2^{k-l+1})}\right)$$

$$A_3=\left(\sum_{i=(2^{l-2}-1)(2^{k-l+2})}^{(2^l-3)(2^{k-l})-1} b_i^2\theta^{4(i-(2^k-2^{k-l+2}))+2}\right) \text{ e}$$

$$A_4=\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^{k-l}(2^l-1)} b_i^2\theta^{4(i-(2^k-2^{k-l+1}))+2}\right).$$

Agora, podemos utilizar novamente as congruências contidas nos Corolários 6.4 e 6.6, além dos fatos que $m\equiv 1 \pmod 2$ e $x^2\equiv x \pmod 2$, as quais seguem abaixo

$$\begin{cases} \omega_j^2\equiv\omega_j(mod\ 2\mathcal{O}_{\mathbb{K}}), \quad \text{para} \quad 1\leq j\leq l-2 \\ \omega_{l-1}^2\equiv\omega_{l-1}+\left(\sum_{j=1}^{l-1}\left(\sum_{i=0}^{2^{l-1-j}-1}\omega_{j-1}\theta^{2^{k-l+2}.i}\right)\right)(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \theta^{2^k}\equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_j^2\theta^{k-j}\equiv\omega_j(mod\ 2\mathcal{O}_{\mathbb{K}}), \quad \text{para} \quad 1\leq j\leq l-2 \\ \omega_{l-1}^2\theta^{k-l+2}\equiv\omega_{l-1}(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{cases} \tag{6.29}$$

Ao substituí-las na Equação (6.28), as substituições são feitas no termo médio de cada somatória mas, note que, para $l=k$, temos $(2^{l-2}-1)(2^{k-l+2})=2^k-4=(2^l-3)(2^{k-l})-1$ e, também, $(2^{l-1}-1)(2^{k-l+1})=2^k-2=2^{k-l}(2^l-1)-1$, isto é, as expressões cujas somatórias possuem esses limites inferiores e superiores se resumem em um único elemento. Portanto, a partir daqui, dividiremos a demonstração em dois casos: $l=k$ ou $4\leq l\leq k-1$. No primeiro caso, $d\equiv 1(mod\ 2^k)$, após substituirmos as congruências acima e, já trocando l por k, a Equação (6.28) torna-se

$$
\begin{aligned}
\alpha^2-\beta^2\theta^2 &= \sum_{j=1}^{k-2}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
&\quad+\sum_{j=1}^{k-2}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))}\right)\\
&\quad+\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}+\omega_{k-1}\right)\right)a_{2^k-4}\\
&\quad+\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}\right)\right)a_{2^k-2}\\
&\quad-\left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\theta^{4i+2^{k-j}(9-2^{j+2})}\right)\right)-\omega_{k-2}\theta^2a_{2^k-4}\\
&\quad-\left(\omega_{k-1}+\left(\sum_{j=1}^{k-1}\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}\right)\right)a_{2^k-2}\theta^2\\
&\quad-\sum_{j=1}^{k-2}\left(\sum_{i=(2^{j-1})(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)\\
&\quad-\sum_{j=1}^{k-2}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))+2}\right)\\
&\quad-\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}+\omega_{k-1}\right)\right)b_{2^k-4}\theta^2\\
&\quad-\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}\right)\right)b_{2^k-2}\theta^2\\
&\quad+\left(\sum_{j=1}^{k-1}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\theta^{4i+2^{k-j}(9-2^{j+2})+2}\right)\right)+\omega_{k-2}\theta^4b_{2^k-4}\\
&\quad+\left(\omega_{k-1}+\left(\sum_{j=1}^{k-1}\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}\right)\right)b_{2^k-2}\theta^4\\
&\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}),
\end{aligned}
\tag{6.30}
$$

onde a parte referente a a_{ij}^*, repetindo o raciocínio exposto na Observação 4.5, é dada por

$$\left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\theta^{4i+2^{k-j}(9-2^{j+2})}\right)\right)+\omega_{k-2}\theta^2 a_{2^k-4}+$$

$$\left(\omega_{k-1}+\left(\sum_{j=1}^{k-1}\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}\right)\right)a_{2^k-2}\theta^2,$$

sendo a primeira somatória referente aos produtos de elementos da mesma classe com $i_1 = i_2 = i$, isto é, a segunda parcela $a_{i_1}a_{i_2}$ da segunda somatória da Equação (6.16) considerando $i_1 = i_2 = i$ e $1 \leq j \leq k-2$ e, os dois elementos seguintes, a_{2^k-4} e a_{2^k-2} e os respectivos termos que os multiplicam, vem, respectivamente, da somatória referida acima para $j = k-1$ e da última somatória da Equação (6.16), as quais possuem apenas um elemento quando $l = k$. Além disso, o termo ω_{k-1}^2 na última somatória acima, foi substituído pelo valor de sua congruência que consta no Sistema (6.29). A expressão é análoga para b_{ij}^*, trocando a por b. Entretanto, note que na Equação (6.30) ainda há elementos que não pertencem à base de $\mathcal{O}_{\mathbb{K}}$, visto que, tomando $i = (2^{j+2}-7)(2^{k-j-2})$ na primeira somatória da expressão acima correspondente a a_{ij}^*, o expoente do θ resulta em $4.(2^{j+2}-7)(2^{k-j-2})+(9-2^{j+2})2^{k-j} = 4(2^k - 7.2^{k-j-2}) + 9.2^{k-j} - 2^{k+2} = -7.2^{k-j} + 9.2^{k-j} = 2^{k-j-1}$, além do termo $\omega_{k-1}\theta^4$ expresso na última somatória da Equação (6.30), que também não pertence a $\mathcal{O}_{\mathbb{K}}$. Assim, utilizando novamente as congruências contidas no Corolário 6.6: $\omega_j\theta^{k-j} \equiv \omega_j (mod\ 2\mathcal{O}_{\mathbb{K}}), 0 \leq j \leq k-2$ e $\omega_{k-1}\theta^4 \equiv \omega_{k-1}(mod\ 2\mathcal{O}_{\mathbb{K}})$ e, substituindo-as na Equação (6.30), obtemos

$$\begin{aligned}
\alpha^2-\beta^2\theta^2 \;=\; & \sum_{j=1}^{k-2}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
& +\sum_{j=1}^{k-2}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_j\theta^{4(i-(2^{j+2}-7)(2^{k-j-2}))}\right)\\
& +\left(\sum_{j=1}^{k-2}\left(\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}+\omega_{k-1}\right)\right)a_{2^k-4}\\
& +\left(\sum_{j=1}^{k-1}\left(\sum_{i=0}^{2^{k-j-1}-1}\omega_{j-1}\theta^{4.i}\right)\right)a_{2^k-2}\\
& -\left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-j-1}}\right)\right)
\end{aligned} \tag{6.31}$$

$$
\begin{aligned}
&- \sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i \theta^{4(i-(2^{j+2}-7)(2^{k-j-2}))} \right) - \omega_{k-2} a_{2^k-4} \theta^2 \\
&- \left(\omega_{k-1} + \left(\sum_{j=1}^{k-1} \sum_{i=0}^{2^{k-j-}-1} \omega_{j-1} \theta^{4.i} \right) \right) a_{2^k-2} \theta^2 \\
&- \sum_{j=1}^{k-2} \left(\sum_{i=(2^{j-1})(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i \omega_j \theta^{4(i-(2^k-2^{k-j+1}))+2} \right) \\
&- \sum_{j=1}^{k-2} \left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i \omega_j \theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))+2} \right) \\
&- \left(\sum_{j=1}^{k-2} \left(\sum_{i=0}^{2^{k-j-1}-1} \omega_{j-1} \theta^{4.i} + \omega_{k-1} \right) \right) b_{2^k-4} \theta^2 \\
&- \left(\sum_{j=1}^{k-1} \left(\sum_{i=0}^{2^{k-j-1}-1} \omega_{j-1} \theta^{4.i} \right) \right) b_{2^k-2} \theta^2 \\
&+ \left(\sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i \theta^{4(i-(2^k-2^{k-j+1}))+2^{k-j+1}+2} \right) \right) \\
&+ \sum_{j=1}^{k-2} \omega_{j-1} \left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i \theta^{4(i-((2^{j+2}-7)(2^{k-j-2})))+2} \right) + \omega_{k-2} b_{2^k-4} \\
&+ \left(\omega_{k-1} + \left(\sum_{j=1}^{k-1} \sum_{i=0}^{2^{k-j-1}-1} \omega_{j-1} \theta^{4.i} \right) \right) b_{2^k-2} \\
\equiv \;& 0 (mod\ 2\mathcal{O}_{\mathbb{K}})
\end{aligned}
$$

Agrupando os termos semelhantes, obtemos novamente uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$, de modo que os coeficientes que o multiplicam devem ser congruentes a 0 módulo 2. Antes de escrever o sistema contendo essas equações, chamamos a atenção para alguns fatos pertinentes sobre elas: note que o elemento b_{2^k-2} multiplica exatamente todos os elementos da base; o elemento a_{2^k-4} multiplica todos os elementos exceto os da penúltima classe (ω_{k-2} e $\omega_{k-2}\theta^2$) e o elemento a_{2^k-2} multiplica todos os elementos exceto os da última classe (ω_{k-1} e $\omega_{k-1}\theta^2$). Além disso, note também que, assim como no caso $l = k+1$, os elementos da base obtidos considerando o valor $j+1$ na sexta e quinta somatória (todos os elementos da sexta somatória e todos os elementos da quinta somatória, nessa ordem) coincidem com os elementos obtidos tomando j na primeira e na segunda somatória (analogamente, tomando $j+1$ na 13ª e na 12ª (reunindo todos os elementos das duas somatórias, nessa ordem) e j na 8ª e na 9ª), pois estes fatos serão utilizados recorrentemente na resolução do sistema. Também é interessante observar que, quando analisamos os elementos da base que pertencem à primeira classe, há

4 coeficientes diferentes que multiplicam cada elemento, de modo que nas equações referentes a esses termos, teremos 4 elementos somando, assim como nas referentes à última classe; agora, nas equações que representam os coeficientes multiplicando os termos da base da penúltima classe, teremos 5 elementos somando, enquanto nas demais, 6 elementos. Assim, as equações que contemplam os coeficientes multiplicando os termos entre a segunda e a antepenúltima classe podem ser todas escritas através de apenas 4 equações (2 que representam os elementos cujo expoente de θ é múltiplo de 4 e mais 2 quando o expoente de θ é múltiplo de 2). Perante o exposto, segue que, após agrupar os termos, obtemos o sistema abaixo, onde cada linha, é válida para todo $0 \leq i \leq 2^{k-3}-1, 1 \leq j \leq k-3$ e $0 \leq h \leq 2^{k-j-3}-1$.

$$\begin{cases} a_{2^k-4} + a_{2^k-2} - a_{2^{k-3}+i} + b_{2^k-2} \equiv 0(mod\ 2), \\ a_{2^k-4} + a_{2^k-2} - a_i + b_{2^k-2} \equiv 0(mod\ 2), \\ -b_{2^k-4} - b_{2^k-2} + b_{2^{k-3}+i} - a_{2^k-2} \equiv 0(mod\ 2), \quad 0 \leq h \leq 2^{k-3}-1 \\ -b_{2^k-4} - b_{2^k-2} + b_i - a_{2^k-3} \equiv 0(mod\ 2), \\ a_{2^k-4} + a_{2^k-2} + b_{2^k-2} + a_{(2^{j-1}-1)(2^{k-j+1})+h} + a_{(2^{j+2}-7)(2^{k-j-2})+h} \\ -a_{(2^{j+3}-7)(2^{k-j-3})+h} \equiv 0(mod\ 2), \\ a_{2^k-4} + a_{2^k-2} + b_{2^k-2} + a_{(2^{j-1}-1)(2^{k-j+1})+h+2^{k-j-3}} + a_{(2^{j+2}-7)(2^{k-j-2})+h+2^{k-j-3}} \\ -a_{(2^j-1)(2^{k-j})+h} \equiv 0(mod\ 2) \\ -b_{2^k-4} - b_{2^k-2} - a_{2^k-2} - b_{(2^{j-1}-1)(2^{k-j+1})+h} - b_{(2^{j+2}-7)(2^{k-j-2})+h} \\ +b_{(2^{j+3}-7)(2^{k-j-3})+h} \equiv 0(mod\ 2) \\ -b_{2^k-4} - b_{2^k-2} - a_{2^k-3} - b_{(2^{j-1}-1)(2^{k-j+1})+h+2^{k-j-3}} - b_{(2^{j+2}-7)(2^{k-j-2})+h+2^{k-j-3}} \\ +b_{(2^j-1)(2^{k-j})+h} \equiv 0(mod\ 2) \\ a_{2^k-2} + b_{2^k-2} + b_{2^k-4} + a_{2^k-8} + a_{2^k-7} \equiv 0(mod\ 2) \\ -b_{2^k-2} + a_{2^k-2} - a_{2^k-4} - b_{2^k-8} - b_{2^k-7} \equiv 0(mod\ 2) \\ a_{2^k-4} + b_{2^k-2} \equiv 0(mod\ 2) \\ -b_{2^k-4} - a_{2^k-2} \equiv 0(mod\ 2). \end{cases} \tag{6.32}$$

Os passos para a resolução do Sistema (6.32) são os mesmos mencionados para resolver o Sistema (6.25). Assim, procedendo da mesma maneira e substituindo os valores obtidos no Sistema (6.26), obtemos que a única solução possível é $a_i, b_i \equiv 0(mod\ 2)$, para todo $0 \leq i \leq 2^k - 1$ e, logo, $\eta \in \mathcal{O}_{\mathbb{L}}$. Desse modo, segue que, para para grau $n = 2^{k+1}$ e $d \equiv 1(mod\ 2^k)$, a inclusão $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$ se verifica. Agora, para encerrar a primeira etapa da prova, voltemos ao caso $4 \leq l \leq k-1$, onde ao substituir as congruências do Sistema (6.29) na Equação (6.28), tomamos o termo médio de todas as somatórias que a compõem, exceto da segunda e da terceira, pois tomando o último valor de i, esses termos obtidos ainda pertencem à base de $\mathcal{O}_{\mathbb{K}}$. Dessa forma, segue que $\alpha^2 - \beta^2\theta^2 \equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}$ na Equação (6.28) implica que

$$
\begin{aligned}
&\sum_{j=1}^{l-2}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))}\right)\\
&+\sum_{j=1}^{l-2}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))}\right)\\
&+\left(\sum_{j=1}^{l-2}\left(\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}+\omega_{l-1}\right)\right)\left(\sum_{i=(2^{l-2}-1)(2^{k-l+2})}^{(2^l-3)(2^{k-l})-1} a_i\theta^{4(i-(2^k-2^{k-l+2}))}\right)\\
&+\left(\sum_{j=1}^{l-1}\left(\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^{k-l}(2^l-1)-1} a_i\theta^{4(i-(2^k-2^{k-l+1}))}\right)\\
&-\left(\sum_{j=1}^{l-1}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\theta^{\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-j+1}}}\right)\right)\\
&-\sum_{j=1}^{l-1}\omega_{j-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\theta^{4(i-(2^{j+2}-7)(2^{k-j-2}))}\right)\\
&-\left(\omega_{l-1}+\left(\sum_{j=1}^{l-1}\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{(2^{k-l-1})(2^{l+1}-3)-1} a_i\theta^{4(i-(2^{l-1}-1)(2^{k-l+1}))+2^{k-l+1}}\right)\\
&-\left(\omega_{l-1}+\left(\sum_{j=1}^{l-1}\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)\left(\sum_{(2^{k-l-1})(2^{l+1}-3)}^{(2^{k-l})(2^l-1)-1} a_i\theta^{4(i-(2^{k-l-1})(2^{l+1}-3)}\right)\\
&-\sum_{j=1}^{l-2}\left(\sum_{i=(2^{j-1})(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))+2}\right)\\
&-\sum_{j=1}^{l-2}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))+2}\right)\\
&-\left(\sum_{j=1}^{l-2}\left(\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}+\omega_{l-1}\right)\right)\left(\sum_{i=(2^{l-2}-1)(2^{k-l+2})}^{(2^l-3)(2^{k-l})-1} b_i\theta^{4(i-(2^k-2^{k-l+2})+2}\right)\\
&-\left(\sum_{j=1}^{l-1}\left(\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{2^{k-l}(2^l-1)-1} b_i\theta^{4(i-(2^k-2^{k-l+1})+2}\right)\\
&+\left(\sum_{j=1}^{l-1}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\theta^{\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-j+1}}+2}\right)\right)\\
&+\sum_{j=1}^{l-1}\omega_{j-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\theta^{4(i-(2^{j+2}-7)(2^{k-j-2}))+2}\right)\\
&+\left(\omega_{l-1}+\left(\sum_{j=1}^{l-1}\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)\left(\sum_{i=(2^{l-1}-1)(2^{k-l+1})}^{(2^{k-l-1})(2^{l+1}-3)-1} b_i\theta^{4(i-(2^{l-1}-1)(2^{k-l+1}))+2^{k-l+1}+2}\right)\\
&+\left(\omega_{l-1}+\left(\sum_{j=1}^{l-1}\sum_{q=0}^{2^{l-j-1}-1}\omega_{j-1}\theta^{2^{k-l+2}.q}\right)\right)\left(\sum_{(2^{k-l-1})(2^{l+1}-3)}^{(2^{k-l})(2^l-1)-1} b_i\theta^{4(i-(2^{k-l-1})(2^{l+1}-3))+2}\right)\\
&\equiv 0 \pmod{2\mathcal{O}_{\mathbb{K}}}
\end{aligned}
\tag{6.33}
$$

Novamente, obtemos uma combinação linear entre os elementos da base de $\mathcal{O}_{\mathbb{K}}$, a qual fornece um sistema de equações formada pelos seus coeficientes. Mas, antes de escrever o sistema com as equações, observemos alguns aspectos relevantes em relaçao à Equação (6.33). A primeira e a segunda somatória, abordam todos os elementos da segunda classe ($\omega_1 x$) até a penúltima classe ($\omega_{l-1}x$) tal que o expoente de θ é múltiplo de 4. Na terceira somatória aparecem os elementos da primeira classe até a última, com excessão apenas dos elementos da penúltima classe, que nao está eglobada na somatória; porém, note que, ao tomar j e q na primeira somatória, podemos percorrer todos os elementos a_i da segunda somatória, já que o expoente de θ de todos esses termos será menor do que o obtido para o próximo valor de q. Desse modo, se colocarmos as equações dos coeficientes que multiplicam $\omega_j, \omega_j\theta^4, \omega_j\theta^8, \ldots, \omega_j\theta^{2^{k-j}-4}$ seguindo essa ordem, os elementos a_i oriundos somatória, que totalizam 2^{k-l}, e dispostos de modo que estejam seguindo a ordem crescente dos valores de i, "se repetem" $\frac{2^{k+1-j}}{2^{k-l}} = 2^{l-j-1}, 1 \leq j \leq l-2$ vezes no conjunto de equações que representam cada classe. Podemos chamar a esse bloco de elementos a_i composto de 2^{k-l} elementos de bloco B. Neste caso, o bloco B é composto pelos elementos $a_{(2^{l-2}-1)(2^{k-l+2})+h'}$, onde $0 \leq h' \leq 2^{k-l}-1$. Desse modo, no conjunto de equações de cada classe (exceto penúltima), sempre há um desses elementos somando, de modo que se as equações do conjunto estão na ordem $\omega_j, \omega_j\theta^4, \omega_j\theta^8, \ldots, \omega_j\theta^{2^{k-j}-4}$, para cada valor de h', seguindo a ordem crescente, somamos o elemento $a_{(2^{l-2}-1)(2^{k-l+2})+h'}$ à equação e, quando chegamos ao último valor de h', voltamos ao valor $h' = 0$, repetindo essa sequência 2^{l-j-1} vezes em cada conjunto de equações referentes a uma classe (no conjunto de equações referentes aos elementos da última classe, o bloco se repete uma única vez). Na quarta somatória, o raciocínio é o mesmo, porém engloba todas as classes exceto a última. Assim, chamando esse bloco de elementos de C, o mesmo será composto por 2^{k-l} elementos: $a_{(2^{l-1}-1)(2^{k-l+1})+h'}$, onde $0 \leq h' \leq 2^{k-l}-1$. Reproduzindo o raciocínio anterior, em cada conjunto de equações referentes aos termos de cada classe, esse bloco de equações se repete 2^{k-j-1} vezes, de modo que na penúltima classe, repetirá apenas uma vez. Agora, analisando a quinta e a sexta somatórias, como a quinta engloba os elementos que compõem a segunda metade da classe e a sexta os que compõem a primeira metade, mas o índice de seus coeficientes seguem a ordem crescente, se escrevermos as equações dos coeficientes que multiplicam os elementos $\omega_j, \omega_j\theta^4, \omega_j\theta^8, \ldots, \omega_j\theta^{2^{k-j}-4}$, seguindo essa ordem, exatamente na linha que representa a metade das equações, para cada classe (da primeira a penúltima), o indice dos coeficientes a_i "saem"da ordem crescente no elemento $a_{(2^{j+1}-3)(2^{k-j-1})-1}$ e recomeçam do valor $a_{(2^{j-1}-1)(2^{k-j+1})}$. Para finalizar, as soma-

tórias que descrevem os coeficientes a_i na sétima e na oitava somatória repetem esse raciocínio, porém, quando analisamos essas somatórias juntamente com as que as multiplicam, as quais descrevem os termos $\omega_j x$, ocorre o mesmo que mencionamos que sucede na terceira e na quarta somatórias, de modo que esse bloco possui 2^{k-l} elementos, mas não estão todos seguindo a ordem crescente, pois exatamente na metade, o índice i diminui (veja expoentes de θ). Desse modo, se chamarmos esse bloco de elementos de A, o mesmo será composto pelos elementos $-a_{(2^{k-l-1})(2^{l+1}-3)+h*}, 0 \leq h* \leq 2^{k-l-1}-1, -a_{(2^{l-1}-1)(2^{k-l+1})+h*}, 0 \leq h* \leq 2^{k-l-1}-1$, onde esses elementos também repetem, nessa ordem, em todas as linhas do sistema, 2^{l-j-1} vezes em cada conjunto de uma classe (esse bloco é composto por 2 elementos e a ordem se dá da seguinte forma: variamos o valor de $h*$ em ordem crescente no primeiro elemento e depois variamos o valor de $h*$ no segundo elemento. Essas duas sequências, que totalizam 2^{k-l} elementos, formam esse bloco). Usaremos essa notação para descrever o sistema, de modo que, na linha que representa um conjunto de equações em que estiver somado um dos blocos mencionados acima, isso significa que em cada equação há um dos elementos do bloco, seguindo a sequência estabelecida. Agora, quando olhamos para os elementos da base de $\mathcal{O}_{\mathbb{K}}$ expressos na Equação (6.33) cujo expoente de θ é múltiplo de 2 e não múltiplo de 4, todos os coeficientes que os multiplicam são os dados pelas somatórias da 9ª em diante e expressas por b_i. A mesma análise feita para as somatórias envolvendo os coeficientes a_i se aplicam a essas, seguindo a mesma ordem. Assim, ao bloco de elementos oriundos da 11ª somatória, chamamos de B', ao bloco de elementos vindos da 12ª, chamamos C' e, aos elementos oriundos da penúltima e última equação, colocados juntos, chamamos de A'. Após toda essa análise, ao agrupar os termos semelhantes da Equação (6.33), seguindo as notações descritas, obtemos o seguinte sistema de equações, válido para todo $1 \leq j \leq l-2$ e $0 \leq h \leq 2^{k-j-2}-1$, onde as 4 primeiras linhas representam conjuntos de equações de coeficientes que multiplicam elementos da primeira classe; da quinta a oitava linha, temos os conjuntos de equações que representam os coeficientes que multiplicam elementos da segunda até a antepenúltima classe, onde a classe varia de acordo com o valor de j: $j = 1$ obtém as equações formada pelos coeficientes que multiplicam os elementos da segunda classe, e assim sucessivamente. A 9ª e a 10ª linhas do sistema representam os coeficientes que multiplicam os termos da penúltima classe e , por fim, as duas últimas, representam os coeficientes que multiplicam os elementos da última classe, a qual é formada apenas por 2 blocos cada, como segue abaixo.

$$\begin{cases} -a_{2^{k-3}+h} + A + B + C \equiv 0(mod\ 2) \\ -b_{2^{k-3}+h} + A' + B' + C' \equiv 0(mod\ 2) \\ -a_h + A + B + C \equiv 0(mod\ 2) \\ -b_h + A' + B' + C' \equiv 0(mod\ 2) \\ a_{(2^{j-1}-1)(2^{k-j+1})+h} + a_{(2^{j+2}-7)(2^{k-j-2})+h} - a_{(2^{j+3}-7)(2^{k-j-3})+h} \\ +A + B + C \equiv 0(mod\ 2) \\ b_{(2^{j-1}-1)(2^{k-j+1})+h} + b_{(2^{j+2}-7)(2^{k-j-2})+h} - b_{(2^{j+3}-7)(2^{k-j-3})+h} \\ +A' + B' + C' \equiv 0(mod\ 2) \\ a_{(2^{j-1}-1)(2^{k-j+1})+2^{k-j-2}+h} + a_{(2^{j+2}-7)(2^{k-j-2})+2^{k-j-2}+h} - a_{(2^j-1)(2^{k-j})+h} \\ +A + B + C \equiv 0(mod\ 2) \\ b_{(2^{j-1}-1)(2^{k-j+1})+2^{k-j-2}+h} + b_{(2^{j+2}-7)(2^{k-j-2})+2^{k-j-2}+h} - b_{(2^j-1)(2^{k-j})+h} \\ +A' + B' + C' \equiv 0(mod\ 2) \\ a_{(2^{l-3}-1)(2^{k-l+3})+h} + a_{(2^l-7)(2^{k-l})+h} - a_{(2^{l+1}-7)(2^{k-l-1})+h} + A + C \equiv 0(mod\ 2) \\ b_{(2^{l-3}-1)(2^{k-l+3})+h} + b_{(2^l-7)(2^{k-l})+h} - b_{(2^{l+1}-7)(2^{k-l-1})+h} + A' + C' \equiv 0(mod\ 2) \\ A + B \equiv 0(mod\ 2) \\ A' + B' \equiv 0(mod\ 2). \end{cases} \tag{6.34}$$

Para resovler o sistema, começamos pelas equações referentes à última classe, descritas pelo bloco $A + B$, onde temos

$$\begin{cases} a_{(2^{l-2}-1)(2^{k-l+2})+h'} \equiv a_{(2^{k-l-1})(2^{l+1}-3)+h'} \pmod 2, 0 \leq h' \leq 2^{k-l-1} - 1 \\ a_{(2^{l-2}-1)(2^{k-l+2})+2^{k-l-1}+h'} \equiv a_{(2^{l-1}-1)(2^{k-l+1})+h'} \pmod 2, 0 \leq h' \leq 2^{k-l-1} - 1 \end{cases}$$

e pelo bloco $A' + B'$, donde segue que

$$\begin{cases} b_{(2^{l-2}-1)(2^{k-l+2})+h'} \equiv b_{(2^{k-l-1})(2^{l+1}-3)+h'} \pmod 2, 0 \leq h' \leq 2^{k-l-1} - 1 \\ b_{(2^{l-2}-1)(2^{k-l+2})+2^{k-l-1}+h'} \equiv b_{(2^{l-1}-1)(2^{k-l+1})+h'} \pmod 2, 0 \leq h' \leq 2^{k-l-1} - 1. \end{cases}$$

Como em todas as linhas do sistema, exceto a referentes aos termos da penúltima classe, há algum elemento do bloco A e um elemento do bloco B para algum valor de h', substituindo as congruências obtidas nas equações das quatro primeiras linhas (primeira classe) obtemos

$$\begin{cases} a_{(2^{l-1}-1)(2^{k-l+1})+h'} \equiv a_{2^{k-3}+h}, \quad a_{(2^{l-1}-1)(2^{k-l+1})+h'} \equiv a_h \\ b_{(2^{l-1}-1)(2^{k-l+1})+h'} \equiv b_{2^{k-3}+h}, \quad b_{(2^{l-1}-1)(2^{k-l+1})+h'} \equiv b_h, \end{cases}$$

para todo $0 \leq h \leq 2^{k-j-2} - 1$. Substituindo no próximo bloco de equações (note

que, como nos casos anteriores, o valor da congruência obtida tomando j em uma equação, coincide com um dos termos obtidos para $j+1$ na equação seguinte), obtemos

$$\begin{cases} a_{(2^{j+2}-7)(2^{k-j-2})+h} \equiv a_{(2^{j+3}-7)(2^{k-j-3})+h} \pmod 2 \\ a_{(2^{j+2}-7)(2^{k-j-2})+2^{k-j-2}+h} \equiv a_{(2^{j+3}-7)(2^{k-j-3})+2^{k-j-2}+h} \pmod 2 \\ b_{(2^{j+2}-7)(2^{k-j-2})+h} \equiv b_{(2^{j+3}-7)(2^{k-j-3})+h} \pmod 2 \\ b_{(2^{j+2}-7)(2^{k-j-2})+2^{k-j-2}+h} \equiv b_{(2^{j+3}-7)(2^{k-j-3})+2^{k-j-2}+h} \pmod 2, \end{cases}$$

para todo $0 \leq h \leq 2^{k-j-2}-1$. Agora, substituindo essas equações no bloco de equações que representa a penúltima classe, obtemos

$$\begin{cases} a_{(2^{l-1}-1)(2^{k-l+1})+h} \equiv 0 \pmod 2, \quad a_{(2^{l-1}-1)(2^{k-l+1})+h+2^{k-3}} \equiv 0 \pmod 2, \\ b_{(2^{l-1}-1)(2^{k-l+1})+h} \equiv 0 \pmod 2, \quad b_{(2^{l-1}-1)(2^{k-l+1})+h+2^{k-3}} \equiv 0 \pmod 2, \end{cases}$$

onde substituindo nas demais congruências e no Sistema (6.26), segue $a_i, bi \equiv 0 \pmod 2$ para todo $0 \leq i \leq 2^k-1$. Como a única solução possível é $a_i, b_i \equiv 0 (mod\ 2)$, ou seja, todos pares, segue que $\alpha', \beta' \in \mathcal{O}_{\mathbb{K}}$, e portanto, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, donde segue que $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{K}}[\theta]$.

2. $\mathcal{O}_{\mathbb{K}}[\theta] \subset \mathcal{O}_{\mathbb{L}}$. Para encerrar a primeira etapa da prova, se $d \equiv 1 (mod\ 2^l)$ tal que $d \not\equiv 1 (mod\ 2^{l+1})$, onde $4 \leq l \leq k+1$, devido ao fato que $\theta, \omega_1, \omega_2, \ldots, \omega_k \in \mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$, segue que $\theta, \omega_1, \omega_2, \ldots, \omega_k$ são inteiros em $\mathbb{L}$, donde segue diretamente que a inclusão

$$\mathcal{O}_{\mathbb{K}}[\theta] = \mathbb{Z}[1, \theta^2, \ldots, \theta^{2^k-2}, \omega_1, \ldots, \omega_1\theta^{2^{k-1}-2}, \ldots, \omega_{l-1}, \ldots, \omega_{l-1}\theta^{2^{k-l+2}-2}][1, \theta] \subset \mathcal{O}_{\mathbb{L}}$$

é verdadeira.

Portanto, dos itens 1 e 2 segue que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$, para todo $4 \leq l \leq k+1$.

Dando continuidade, realizaremos a segunda etapa da prova, onde $d \equiv 1 \pmod{2^{l+2}}$, ou seja, $l = k+2$. Neste caso, diferentemente de todos os outros, a igualdade $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$ não se verifica, de modo que devemos mostrar que

$$\begin{aligned} \mathcal{O}_{\mathbb{L}} = \ & \mathbb{Z}[1, \theta, \theta^2, \theta^3 \ldots, \theta^{2^k-1}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^{2^{k-1}-1}, \omega_2, \omega_2\theta, \ldots, \omega_2\theta^{2^{k-2}-1}, \ldots, \\ & \omega_{k-2}, \omega_{k-2}\theta, \omega_{k-2}\theta^2, \omega_{k-2}\theta^3, \omega_{k-1}, \omega_{k-1}\theta, \omega_k, \omega_{k+1}]. \end{aligned}$$

Para isso, tomando $\eta \in \mathcal{O}_{\mathbb{L}}$, segue que $2\eta = \alpha + \beta\theta$ onde $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$. Em consequência de $d \equiv 1 \pmod{2^{k+2}}$ acarretar $d \equiv 1 \pmod{2^{k+1}}$, uma base de $\mathcal{O}_{\mathbb{K}}$ correspondente a essa congruência, é a descrita para $d \equiv 1 \pmod{2^{k+1}}$, já que não há uma base específica para $d \equiv 1 \pmod{2^{k+2}}$ para o anel de inteiros algébricos do corpo $\mathbb{K}$ de grau 2^k e, também,

pelo fato de 2^{k+1} ser a última potência de 2 que divide $d-1$ a influenciar na forma da base de $\mathcal{O}_{\mathbb{K}}$, a mesma não possui a restrição que 2^{k+2} não divide $d-1$, não havendo, portanto, nenhum problema em utilizá-la. Assim, pela Hipótese de Indução, como usamos uma base de $\mathcal{O}_{\mathbb{K}}$ correspondente caso $d \equiv 1(mod\ 2^{k+1})$, podemos escrever α e β como combinação linear dos elementos $\{1, \theta^2, \theta^4 \ldots, \theta^{2^k-2}, \omega_1, \omega_1\theta^2, \ldots, \omega_1\theta^{2^{k-1}-2}, \omega_2, \omega_2\theta^2, \ldots, \omega_2\theta^{2^{k-2}-2}, \ldots, \omega_{k-2}, \omega_{k-2}\theta^2, \omega_{k-1}, \omega_k\}$, ou seja

$$\alpha = \sum_{j=1}^{l-3=k-1} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i \theta^{2(i-(2^k-2^{k-j+1}))} \right) + a_{2^k-2}\omega_{k-1} + a_{2^k-1}\omega_k$$

e

$$\beta = \sum_{j=1}^{k-1} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i \theta^{2(i-(2^k-2^{k-j+1}))} \right) + b_{2^k-2}\omega_{k-1} + b_{2^k-1}\omega_k.$$

Observação 6.10. Vale observar que uma base que tomamos inicialmente nesse caso é a mesma utilizada no caso $l = k+1$, porém devido aos valores das congruências, os quais terão algumas diferenças, obteremos uma base distinta da obtida anteriormente.

Substituindo esses valores na Equação (6.7), obtemos

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1} \omega_{j-1}^2 \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i^2 \theta^{4(i-(2^k-2^{k-j+1}))} \right) + a_{2^k-2}^2\omega_{k-1}^2 \\ &\quad + a_{2^k-1}^2\omega_k^2 + 2a_{ij} - \sum_{j=1}^{k-1} \omega_{j-1}^2 \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i^2 \theta^{4(i-(2^k-2^{k-j+1}))+2} \right) \\ &\quad - (b_{2^k-2}^2\omega_{k-1}^2 - b_{2^k-1}^2\omega_k^2 - 2b_{ij})\theta^2 \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}), \end{aligned} \tag{6.35}$$

onde a_{ij} representa a soma de todas as multiplicações de $a_i x$ por $a_j y$, com $0 \leq i \leq 2^k - 2$ e $i < j$, e b_{ij} representa a soma de todas as multiplicações de $b_i x$ por $b_j y$, com $0 \leq i \leq 2^k - 2$ e $i < j$, dadas pelas Equações (6.9) e (6.10). Reescrevendo em termos da congruência módulo $2\mathcal{O}_{\mathbb{K}}$, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1} \omega_{j-1}^2 \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i^2 \theta^{4(i-(2^k-2^{k-j+1}))} \right) \\ &\quad + a_{2^k-2}^2\omega_{k-1}^2 + a_{2^k-1}^2\omega_k^2 \\ &\quad - \sum_{j=1}^{k-1} \omega_{j-1}^2 \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i^2 \theta^{4(i-(2^k-2^{k-j+1}))+2} \right) \end{aligned} \tag{6.36}$$

$$-b_{2^k-2}^2\omega_{k-1}^2\theta^2 - b_{2^k-1}^2\omega_k^2\theta^2 \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).$$

De acordo com os Corolários 6.4 e 6.6, verificam-se as congruências

$$\begin{cases} \theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_j^2 \equiv \omega_j(mod\ 2\mathcal{O}_{\mathbb{K}}), \text{para todo } 1 \leq j \leq k \\ \omega_j\theta^{\frac{n}{2^{j+1}}} = 2\omega_{j+1} - \omega_j \equiv \omega_j(mod\ 2), \text{para todo} 1 \leq j \leq k-1 \\ \omega_k\theta^{\frac{n}{2^k}} = \omega_k\theta^{2^{k+1-k}} = \omega_k\theta^2 = \omega_k + 2k \equiv \omega_k, (mod\ 2) \\ x^2 \equiv x(mod\ 2), \text{ para todo } x \in \mathbb{Z}. \end{cases}$$

Substituindo-as na Equação (6.36), uma vez que $\alpha^2 - \beta^2\theta^2 \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}})$, segue que

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_{j-1}\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\ &\quad + \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} a_i\omega_{j-1}\theta^{4(i-((2^{j+1}-3)(2^{k-j-1}))}\right) \\ &\quad + a_{2^k-2}\omega_{k-1} + a_{2^k-1}\omega_k \\ &\quad - \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_{j-1}\theta^{4(i-(2^k-2^{k-j+1})+2)}\right) \\ &\quad - \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+1}-3)(2^{k-j-1})}^{(2^j-1)(2^{k-j})-1} b_i\omega_{j-1}\theta^{4(i-((2^{j+1}-3)(2^{k-j-1}))+2}\right) \\ &\quad - b_{2^k-2}\omega_{k-1} - b_{2^k-1}\omega_k \\ &\equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Dessa forma, obtemos uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$ e, vale observar que, como tomamos o ponto médio entre os limites inferior e superior de cada somatória, o mesmo valor de j representa dois coeficientes a_i distintos que multiplicam pelo mesmo termo base nas duas primeiras somatórias, ocorrendo o mesmo para b_i nas duas últimas somatórias. À vista disso, obtemos as seguintes congruências, válidas para

todo $1 \leq j \leq l-4 = k-2$ e $0 \leq h \leq \frac{n}{2^{k-j-2}} - 1$.

$$\begin{cases} a_{(2^{j-1}-1)(2^{k-j+1})+h} + a_{(2^{j+1}-3)(2^{k-j-1})+h} \equiv 0(mod\ 2) \\ b_{(2^{j-1}-1)(2^{k-j+1})+h} + b_{(2^{j+1}-3)(2^{k-j-1})+h} \equiv 0(mod\ 2) \\ a_{2^k-2} \equiv b_{2^k-2}(mod\ 2) \\ a_{2^k-1} \equiv b_{2^k-1}(mod\ 2). \end{cases}$$

Dessas equações, nós obtemos as congruências módulo 2 que coincidem com as encontradas no Sistema (6.13), para o caso $l = k+1$ e, por conseguinte, efetuando os quadrados e produtos obtemos as congruências módulo 4 contidas no Sistema (6.14). Substituindo-as na Equação (6.35), obtemos

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1} \left((1+2^{k-(j-1)})\omega_{j-1}^2 \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i^2 \theta^{4(i-(2^k-2^{k-j+1}))} \right) - 2a_{ij}^* \\ &\quad - \sum_{j=1}^{k-1} \left((1+2^{k-(j-1)})\omega_{j-1}^2 \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i^2 \theta^{4(i-(2^k-2^{k-j+1}))+2} \right) - 2b_{ij}^* \\ &\quad + (1-\theta^2)(a_{2^k-2}^2\omega_{k-1}^2 + a_{2^k-1}^2\omega_k^2) \equiv 0(mod\ 4\mathcal{O}_{\mathbb{K}}), \end{aligned} \tag{6.37}$$

onde a_{ij}^* e b_{ij}^* são as expressões obtidas de a_{ij} e de b_{ij}, respectivamente, e podem ser expressas pela Equação (6.16) fazendo $l = k+2$.
Agora, a partir das igualdades

$$\begin{cases} 1 + \theta^{2^k} = 2\omega_1 \\ \omega_j^2(1+\theta^{k-j}) = 2\omega_{j+1}, 2 \leq j \leq k-1 \\ \omega_{k-1}^2 = \omega_{k-1} + 4m \left(\sum_{j=1}^{k-2} \left(\sum_{i=0}^{2^{k-j}-1} \omega_{j-1}\theta^{4.i} \right) \right) \equiv \omega_{k-1}(mod\ 4\mathcal{O}_{\mathbb{K}}) \\ \omega_k^2 = \omega_k + 2m \left(\sum_{j=1}^{k-1} \left(\sum_{i=0}^{2^{k-j}-1} \omega_{j-1}\theta^{2.i} \right) \right) \\ (1-\theta^2)(a_{2^k-2}^2\omega_{k-1}^2 + a_{2^k-1}^2\omega_k^2) = 2(a_{2^k-2}^2\omega_{k-1} - a_{2^k-2}^2\omega_k), \end{cases}$$

as quais constam nas Proposições 6.3 e 6.7 e, a última, pode ser obtida diretamente por meio dessas proposições. Substituindo-as na Equação (6.37), note que todos os termos ficam multiplicados por 2, de modo podemos reduzir a congruência através do fato que

$2x \equiv 0 \pmod 4 \Rightarrow x \equiv 0 \pmod 2$, donde segue que

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1}\left(\omega_j \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i^2\theta^{4(i-(2^k-2^{k-j+1}))}\right) - a_{ij}^* \\ &\quad \sum_{j=1}^{k-1}\left(\omega_j \sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i^2\theta^{4(i-(2^k-2^{k-j+1}))+2}\right) + b_{ij}^* \\ &\quad +(a_{2^k-2}^2\omega_{k-1} + a_{2^k-2}^2\omega_k) \equiv 0(mod\ 2\mathcal{O}_{\mathbb{K}}).\end{aligned}$$

Utilizando novamente as congruências abaixo

$$\begin{cases} \theta^{2^k} \equiv 1(mod\ 2\mathcal{O}_{\mathbb{K}}) \\ \omega_j^2 \equiv \omega_j(mod\ 2\mathcal{O}_{\mathbb{K}}), \text{para todo } 1 \leq j \leq k \\ x^2 \equiv x(mod\ 2),\ \text{para todo } x \in \mathbb{Z}, \end{cases}$$

inclusive nas expressões de a_{ij}^* e b_{ij}^*, obtemos

$$\begin{aligned}\alpha^2 - \beta^2\theta^2 &= \sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))}\right) \\ &\quad +\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))}\right) \\ &\quad -\left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} a_i\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-1}}\right)\right) \\ &\quad -\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} a_i\theta^{4(i-(2^{j+2}-7)(2^{k-j-2})}\right) \\ &\quad -\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\omega_j\theta^{4(i-(2^k-2^{k-j+1}))+2}\right) \\ &\quad -\sum_{j=1}^{k-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\omega_j\theta^{4(i-((2^{j+2}-7)(2^{k-j-2}))+2}\right) \\ &\quad +\left(\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^{j+2}-7)(2^{k-j-2})-1} b_i\theta^{4(i-(2^k-2^{k-j+1}))+2^{k-1}+2}\right)\right)\end{aligned} \tag{6.38}$$

$$+\sum_{j=1}^{k-2}\omega_{j-1}\left(\sum_{i=(2^{j+2}-7)(2^{k-j-2})}^{(2^{j+1}-3)(2^{k-j-1})-1} b_i\theta^{4(i-(2^{j+2}-7)(2^{k-j-2})+2}\right)$$

$$+(a_{2^k-2}\omega_{k-1}+a_{2^k-2}\omega_k)\equiv\ 0(mod\ 2\mathcal{O}_{\mathbb{K}}).$$

Como chegamos novamente em uma combinação linear inteira dos elementos da base de $\mathcal{O}_{\mathbb{K}}$, obtemos o sistema abaixo, onde as equações são válidas para todo $0\leq i\leq 2^{k-2}-1, 1\leq j\leq k-1$ e $0\leq h\leq 2^{k-j-3}-1$.

$$\begin{cases} -a_i\equiv 0(mod\ 2)\\ b_i\equiv 0(mod\ 2)\\ a_{(2^{j-1}-1)(2^{k-j+1})+h}+a_{(2^{j+2}-7)(2^{k-j-2})+h}-a_{(2^{j+3}-7)(2^{k-j-3})+h}(mod\ 2)\\ a_{(2^{j-1}-1)(2^{k-j+1})+2^{k-j-3}+h}+a_{(2^{j+2}-7)(2^{k-j-2})+2^{k-j-3}+h}-a_{(2^j-1)(2^{k-j})+h}(mod\ 2)\\ -b_{(2^{j-1}-1)(2^{k-j+1})+h}-b_{(2^{j+2}-7)(2^{k-j-2})+h}+b_{(2^{j+3}-7)(2^{k-j-3})+h}(mod\ 2)\\ -b_{(2^{j-1}-1)(2^{k-j+1})+2^{k-j-3}+h}-b_{(2^{j+2}-7)(2^{k-j-2})+2^{k-j-3}+h}+b_{(2^j-1)(2^{k-j})+h}(mod\ 2)\\ a_{2^k-4}+a_{2^k-2}-b_{2^k-4}\equiv 0(mod\ 2)\\ -b_{2^k-4}-b_{2^k-2}+a_{2^k-4}\equiv 0(mod\ 2)\\ -a_{2^k-2}\equiv 0(mod\ 2)\\ b_{2^k-2}\equiv 0(mod\ 2). \end{cases}$$

Das duas primeiras equações e das duas últimas equações, obtemos diretamente que $a_i, b_i\equiv 0(mod\ 2)$, para todo $0\leq i\leq 2^{k-2}-1$ e $i=2^k-2$. Substituindo-as nas demais equações e, em seguida, no Sistema (6.13), obtemos $a_i\equiv 0(mod\ 2)$ e $b_i\equiv 0(mod\ 2)$, para todo $0\leq i\leq 2^k-2$. Assim, só resta analisar a paridade de a_{2^k-1} e b_{2^k-1}, a qual sabemos que é a mesma de acordo com o Sistema (6.13).

a) a_{2^k-1} e b_{2^k-1} são pares.

Se a_{2^k-1} e b_{2^k-1} são pares, isso significa que todos os inteiros a_i e b_i são pares, de modo que existem inteiros a_i' e b_i' tais que $a_i=2a_i'$ e $b_i=2b_i'$, para todo $0\leq i\leq 2^k-1$. Logo,

$$\eta=\frac{\alpha}{2}+\frac{\beta}{2}\theta=\frac{\sum_{j=1}^{k-1}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i\theta^{2(i-(2^k-2^{k-j+1}))}\right)+a_{2^k-2}\omega_{k-1}+a_{2^k-1}\omega_k}{2}$$
$$+\frac{\left(\sum_{j=1}^{k-1}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i\theta^{2(i-(2^k-2^{k-j+1}))}\right)+b_{2^k-2}\omega_{k-1}+b_{2^k-1}\omega_k\right)\theta}{2}$$

$$= \frac{\sum_{j=1}^{k-1} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} 2(a'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + 2a'_{2^k-2}\omega_{k-1} + 2a'_{2^k-1}\omega_k)}{2}$$

$$+ \frac{\left(\sum_{j=1}^{k-1} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} 2(b'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + 2b'_{2^k-2}\omega_{k-1} + 2b'_{2^k-1}\omega_k \right) \theta}{2}$$

$$= \sum_{j=1}^{k-1} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} (a'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + a'_{2^k-2}\omega_{k-1} + a'_{2^k-1}\omega_k$$

$$\left(\sum_{j=1}^{k-1} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + b'_{2^k-2}\omega_{k-1} + b'_{2^k-1}\omega_k \right) \theta.$$

Assim, $\eta \in \mathbb{Z}\left[1, \theta, \theta^2, \theta^3 \ldots, \theta^{2^k-1}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^{2^{k-1}-1}, w_2, w_2\theta, \ldots, \omega_2\theta^{2^{k-2}-1}, \ldots, \omega_{k-1}, \omega_{k-1}\theta, \omega_k, \omega_k\theta\right]$, ou seja, $\eta \in \mathcal{O}_{\mathbb{K}}[\theta]$, que recai no caso anterior.

b) a_{2^k-1} e b_{2^k-1} são ímpares

Se a_{2^k-1} e b_{2^k-1} são ímpares, isso significa que existem inteiros a'_i e b'_i tais que $a_i = 2a'_i$ e $b_i = 2b'_i$, para todo $0 \leq i \leq 2^k - 2$ e $a_{2^k-1} = 2a'_{2^k-1} + 1$ e $b_{2^k-1} = 2b'_{2^k-1} + 1$. Logo,

$$\eta = \frac{\alpha}{2} + \frac{\beta}{2}\theta = \frac{\sum_{j=1}^{k} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} a_i \theta^{2(i-(2^k-2^{k-j+1}))} \right) + a_{2^k-1}\omega_k}{2}$$

$$+ \frac{\left(\sum_{j=1}^{k} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i \theta^{2(i-(2^k-2^{k-j+1}))} \right) + b_{2^k-1}\omega_k \right) \theta}{2}$$

$$= \frac{\sum_{j=1}^{k} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} 2(a'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + (2a'_{2^k-1} + 1)\omega_k}{2}$$

$$+ \frac{\left(\sum_{j=1}^{k} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} 2(b'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + (2b'_{2^k-1} + 1)\omega_k \right) \theta}{2}$$

$$= \sum_{j=1}^{k} \omega_{j-1} \left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} (a'_i \theta^{2(i-(2^k-2^{k-j+1}))}) \right) + (a'_{2^k-1} + \frac{1}{2})\omega_k$$

$$+\left(\sum_{j=1}^{k}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i'\theta^{2(i-(2^k-2^{k-j+1}))}\right)+(b_{2^k-1}'+\frac{1}{2})\omega_k\right)\theta$$

$$=\sum_{j=1}^{k}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1}(a_i'\theta^{2(i-(2^k-2^{k-j+1}))})\right)+a_{2^k-1}'\omega_k+$$

$$+\left(\sum_{j=1}^{k}\omega_{j-1}\left(\sum_{i=(2^{j-1}-1)(2^{k-j+1})}^{(2^j-1)(2^{k-j})-1} b_i'\theta^{2(i-(2^k-2^{k-j+1}))}\right)+b_{2^k-1}'\omega_k\theta+(\frac{1}{2}\theta+\frac{1}{2})\omega_k\right).$$

Como $\omega_{k+1}=\frac{(1+\theta)}{2}\omega_k$, segue que

$$\eta\in\mathbb{Z}[1,\theta,\theta^2,\ldots,\theta^{2^k-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{2^{k-1}-1},\ldots,\omega_{k-1},\omega_{k-1}\theta,\omega_k,\omega_k\theta,\omega_{k+1}].$$

Mas $\omega_k\theta=2\omega_{k+1}-\omega_k$, de modo que

$$\eta\in\mathbb{Z}[1,\theta,\theta^2,\ldots,\theta^{2^k-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{2^{k-1}-1},\ldots,\omega_{k-1},\omega_{k-1}\theta,\omega_k,\omega_{k+1}],$$

donde segue a inclusão

$$\mathcal{O}_{\mathbb{L}}\subset\mathbb{Z}[1,\theta,\theta^2,\ldots,\theta^{2^k-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{2^{k-1}-1},\ldots,\omega_{k-1},\omega_{k-1}\theta,\omega_k,\omega_{k+1}].$$

- $\mathbb{Z}[1,\theta,\theta^2,\ldots,\theta^{2^k-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{2^{k-1}-1},\ldots,\omega_{k-1},\omega_{k-1}\theta,\omega_k,\omega_{k+1}]\subset\mathcal{O}_{\mathbb{L}}$.

  Já sabemos que os elementos θ e $\omega_j, 1\leq j\leq k$, são inteiros em $\mathbb{L}$. Deste modo, só resta mostrar que ω_{k+1} também é um inteiro para concluirmos a inclusão. Como nas provas anteriores, mostraremos que a norma e o traço de ω_{k+1}, estão ambos em $\mathcal{O}_{\mathbb{K}}$.

$$\begin{aligned}
Tr(\omega_{k+1}) &= \omega_{k+1}+\sigma_{k+1}(\omega_{k+1})=\omega_1\left(\tfrac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}\right)\\
&\quad+\omega_1\left(\tfrac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1-\theta}{2}\right)\\
&= \omega_1\left(\tfrac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}+\tfrac{1-\theta}{2}\right)\\
&= \omega_k\in\mathcal{O}_{\mathbb{K}}.
\end{aligned}$$

$$\begin{aligned}
N(\omega_{k+1}) &= \omega_{k+1}.\sigma_{k+1}(\omega_{k+1})=\omega_1\left(\tfrac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1+\theta}{2}\right).\omega_1\\
&\quad\left(\tfrac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\tfrac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\tfrac{1+\theta^4}{2}\right)\left(\tfrac{1+\theta^2}{2}\right)\left(\tfrac{1-\theta}{2}\right)\\
&= \tfrac{1}{2^k}\omega_k\omega_1\left(\tfrac{1-\theta^{2^k}}{2}\right)=\tfrac{1}{2^k}\omega_k\omega_1(-\omega_1+1)=m\omega_k\in\mathcal{O}_{\mathbb{K}}.
\end{aligned}$$

De fato, pois

$$\left(\frac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\frac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\frac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\frac{1+\theta^{4}}{2}\right)\left(\frac{1+\theta^{2}}{2}\right)\left(\frac{1+\theta}{2}\right)\left(\frac{1-\theta}{2}\right)=\frac{1-\theta^{2^k}}{2^{k+1}}=\frac{1}{2^k}(1-\omega_1)$$

e

$$\omega_1(-\omega_1+1)=\frac{1+\theta^{2^k}}{2}\frac{1-\theta^{2^k}}{2}=\frac{1-\theta^{2^{k+1}}}{4}=\frac{1-d}{4}=-2^k m,$$

já que $d\equiv 1(mod\ 2^{k+2})$ implica que $\frac{d-1}{4}=2^k m$ e

$$\omega_k=\omega_1\left(\frac{1+\theta^{\frac{n}{4}}}{2}\right)\left(\frac{1+\theta^{\frac{n}{8}}}{2}\right)\left(\frac{1+\theta^{\frac{n}{16}}}{2}\right)\ldots\left(\frac{1+\theta^{4}}{2}\right)\left(\frac{1+\theta^{2}}{2}\right).$$

Desses fatos, a partir da Proposição 1.7, segue que $\omega_{k+1}\in\mathcal{O}_{\mathbb{L}}$ e, por conseguinte, segue a inclusão

$$\mathbb{Z}[1,\theta,\ldots,\theta^{2^k-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{2^{k-1}-1},\omega_2,\omega_2\theta,\ldots,\omega_2\theta^{2^{k-2}-1},\ldots,$$
$$\omega_{k-1},\omega_{k-1}\theta,\omega_k,\omega_{k+1}]\subset\mathcal{O}_{\mathbb{L}},$$

Portanto,

$$\mathcal{O}_{\mathbb{L}}=\mathbb{Z}[1,\theta,\ldots,\theta^{2^k-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{2^{k-1}-1},\omega_2,\omega_2\theta,\ldots,\omega_2\theta^{2^{k-2}-1},\ldots,$$
$$\omega_{k-1},\omega_{k-1}\theta,\omega_k,\omega_{k+1}],$$

o que prova o resultado. □

6.2 Discriminante

Uma vez que conhecemos uma base integral de um corpo de números, é propício calcular também o seu discriminante, já que o mesmo depende do conhecimento de uma base integral (qualquer uma) e possui diversas aplicações na Teoria dos Números. Como um exemplo, podemos citar sua utlidade para determinar quando um número primo se ramifica no anel de inteiros algébricos de um corpo, já que isso se verifica quando o mesmo divide o discriminante do anel de inteiros algébricos do corpo (para mais detalhes, veja [22]); além disso, conhecer o discriminante do anel de inteiros algébricos do corpo também é necessário para calcular a densidade de centro de um reticulado algébrico. Assim sendo, nesta seção, generalizamos as expressões dadas para os discriminantes encontrados nos capítulos anteriores e damos continuidade à Seção 6.1 apresentando uma fórmula para o discriminante do anel de inteiros algébricos do corpo de números $\mathbb{L}=\mathbb{Q}(\sqrt[n]{d})$, onde $n=2^k$, com $k\geq 1$ e $d\neq 1$ um inteiro livre de quadrados, conforme o próximo Teorema.

Teorema 6.11. *Seja* $\mathbb{L}=\mathbb{Q}(\theta)$, *onde* $\theta=\sqrt[n]{d}$, $d\neq 1$ *livre de quadrados e* $n=2^k$, *com* $k\geq 1$. *O discriminante do anel de inteiros algébricos do corpo* $\mathbb{L}$ *é dado por*

$$\mathcal{D}(\mathbb{L})=\begin{cases} 4d, \text{ se } k=1 \text{ e } d\equiv 2,3(mod\ 4)\\ d, \text{ se } k=1 \text{ e } d\equiv 1(mod\ 4)\\ -n^n d^n, \text{ se } k\geq 2 \text{ e } d\equiv 2,3(mod\ 4)\\ -2^{2^{(k-(l-2))}(2^{l-2}k-(2^{l-1}-1))}d^{n-1}, \text{ se } k\geq 2 \text{ e } d\equiv 2^l+1(mod\ 2^{l+1}) \text{ para } 2\leq l\leq k-1 \text{ e}\\ d\equiv 1(mod\ 2^{l+1}) \text{ para } l=k. \end{cases}$$

Demonstração. Os valores do discriminante para $d\equiv 2,3(mod\ 4)$ já foram provados no Teorema 2.4 e o caso em que $k=1$ e $d\equiv 1(mod\ 4)$ está contido no Teorema 4.7. Além disso, considerando o caso restante descrito para $k\geq 2$, o mesmo já foi demonstrado para $l=2$ e $l=3$ nos Teoremas 4.6, e 5.3. Assim, resta provar o resultado apenas para $l\geq 4$, conforme os passos a seguir. De acordo com o Teorema 6.9, uma base de $\mathcal{O}_{\mathbb{L}}$ é dada por

$$\Big\{1,\theta,\theta^2,\ldots,\theta^{\frac{n}{2}-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{\frac{n}{4}-1},\omega_2,\omega_2\theta,\ldots,\omega_2\theta^{\frac{n}{8}-1},\omega_3,\omega_3\theta,\ldots,\omega_3\theta^{\frac{n}{16}-1},\ldots,\omega_{l-1},$$

$$\omega_{l-2},\omega_{l-2}\theta,\ldots\omega_{l-2}\theta^{\frac{n}{2^{l-1}}-1},\omega_{l-1}\theta,\ldots\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-1}\Big\}$$

onde d possui as características descritas no enunciado e de modo que os elementos da última classe são fixos, sempre descritos por $\omega_{l-1},\omega_{l-1}\theta,\ldots\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-1}$. Assim, conforme o Teorema 1.32, segue que o discriminante do anel de inteiros algébricos de $\mathbb{L}$ é dado pelo determinante da matriz cujas entradas são os traços dos produtos dos elementos da base do anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$ de $\mathbb{L}$. Assim, analogamente ao que fizemos nos Capítulos 4 e 5, aplicando Laplace sucessivamente na segunda linha $\frac{n}{2}-1$ vezes e, em seguida, aplicando Laplace mais $\frac{n}{2}-1$ vezes na segunda coluna, obtemos

$$\begin{aligned} &D_{\mathbb{L}}(1,\theta,\theta^2,\ldots,\theta^{\frac{n}{2}-1},\omega_1,\omega_1\theta,\ldots,\omega_1\theta^{\frac{n}{4}-1},\ldots,\omega_{l-1}\theta,\ldots,\omega_{l-1},\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-1}) =\\ &-(2^{k-(l-1)})^{2^{k-(l-2)}}(2^{k-(l-2)})^{2^{k-(l-2)}}(2^{k-(l-3)})^{2^{k-(l-3)}}(2^{k-(l-4)})^{2^{k-(l-4)}}\cdots\\ &\cdots(2^{k-3})^{2^{k-3}}(2^{k-2})^{2^{k-2}}(2^{k-1})^{2^{k-1}-2}2^{2k-2}d^{n-1} =\\ &-2^{(k-(l-1))2^{k-(l-2)}+(k-(l-2))2^{k-(l-2)}+(k-(l-3))2^{k-(l-3)}+\cdots+(k-2)2^{k-2}+(k-1)(2^{k-1}-2)+2k-2}d^{n-1}. \end{aligned} \tag{6.39}$$

O termo $2^{k-(l-1)2^{k-(l-2)}}$ origina-se dos $\frac{n}{2^{l-1}}$ elementos pertencentes à última classe da base (conforme Definição 6.2), os quais são denotados por $\omega_{l-1}\theta^x, 0\leq x\leq \frac{n}{2^{l-1}}-1$. Como nessa classe as somas são dividas por 2^{l-1}, devido à própria definição de ω_{l-1}, e $\mathrm{Tr}(\theta^n)$=nd,

quando multiplicamos $\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-1}$ por θ, $\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-2}$ por θ^2 e, de modo geral, $\omega_{l-1}\theta^{\frac{n}{2^{l-1}}-q}$ por θ^q, o traço do valor que resulta dessa multiplicação é $\frac{Tr(\theta^n)}{2^{l-1}} = 2^{k-(l-1)}d$ e, além disso, essa será a única entrada não nula da matriz na segunda linha e na segunda coluna, as quais escolhemos para aplicar o Teorema de Laplace, ou seja, esse elemento, $2^{k-(l-1)}$, multiplicará seus respectivos cofatores $\frac{n}{2^{l-1}}$ vezes referentes às linhas e $\frac{n}{2^{l-1}}$ vezes referentes às colunas, ou seja $2.\frac{n}{2^{l-1}}$ vezes no total, donde surge o termo $2^{k-(l-1)2^{k-(l-2)}}$, pois $2.\frac{n}{2^{l-1}} = \frac{2^{k+1}}{2^{l-1}} = 2^{k+1-(l-1)} = 2^{k-(l-2)}$, valor de seu expoente. Utilizando o mesmo raciocício, isto é, considerando a multiplicação de cada $\omega_i\theta^{\frac{n}{2^i}-q}$ por θ^q (pode-se observar nas demonstrações dos Teoremas 3.2, 3.4, 3.7, e até mesmo dos Teoremas 4.6 e 5.3, que esses valores são únicos que interferem no resultado, já que ao aplicar Laplace os outros termos vão sendo eliminados), analisando a divisão pela potência 2^i que consta em cada classe de ω_i, onde $0 \leq i \leq l-2$ e o número de elementos que a mesma possui (sempre $\frac{n}{2^{i+1}}$, de acordo com a Definição 6.2), o qual será mutiplicado por 2, pois consideramos as linhas e as colunas simétricas, totalizando $2\frac{n}{2^{i+1}} = 2^{k-i}$ onde $1 \leq i \leq l-2$, ao agrupar os valores resultantes de todos os traços que possuem elementos da mesma classe, do tipo $\omega_i\theta^{\frac{n}{2^i}-q}\theta^q$, $1 \leq i \leq l-2$, os quais constam nas linhas/colunas em que aplicaremos o método de Laplace, obtemos $2^{k-i^{2^{k-i}}}d$ para $\leq i \leq l-2$ e para $i = 1$, referente às multiplicações $\omega_1\theta^{\frac{n}{2^i}-q}\theta^q$, subtraímos 2 ao expoente, resultando em $2^{k-1^{2^{k-1}-2}}$, pois não aplicamos Laplace na $\frac{n}{2}+1$-ésima linha nem na $\frac{n}{2}+1$-ésima coluna da matriz, as quais pernamecem para o determinante 2×2 final. Juntando estes fatos com o fato de que a matriz resultante após os $n-2$ passos, tem determinante

$$\begin{vmatrix} n & \frac{n}{2} \\ \frac{n}{2} & \frac{n}{4}(1+d) \end{vmatrix} = \frac{n^2}{4}(1+d) - \frac{n^2}{4} = \frac{n^2}{4}d = 2^{2k-2}d,$$

obtemos todos os valores que constam na Equação (6.39).

Colocando $2^{k-(l-2)}$ em evidência no expoente, segue que

$$-2^{(2^{k-(l-2)})(k-(l-1)+k-(l-2)+(k-(l-3))2^+(k-(l-4))2^2+\cdots+(k-2)2^{l-2}}2^{(k-1)(2^{k-1}-2)+2k-2}d^{n-1} =$$

$$-2^{(2^{k-(l-2)})(k-(l-1)+k-(l-2)+(k-(l-3))2^+(k-(l-4))2^2+\cdots+(k-2)2^{l-2}}2^{(k(2^{k-1}-2^{k-1}-2k+2)+2k-2}d^{n-1} =$$

$$-2^{(2^{k-(l-2)})(k-(l-1)+k-(l-2)+(k-(l-3))2+(k-(l-4))2^2+\cdots+(k-2)2^{l-2}+k2^{l-3}-2^{l-3})}d^{n-1}.$$

Portanto,

$$D(\mathbb{K}) = -2^{(2^{k-(l-2)})((k+k+2k+4k+8k+16k+\cdots+2^{l-3}k)-((l-1)+(l-2)+(l-3)2+(l-4)2^2+\cdots+2.2^{l-2}+2^{l-3})}d^{n-1}. \tag{6.40}$$

1. Afirmação 1: $k+k+2k+4k+8k+16k+\cdots+2^{l-3}k = 2^{l-2}k$. De fato, observe

que $\{k, 2k, 4k, 8k, \ldots, 2^{l-3}k\}$ são termos de uma progressão geométrica de $l-2$ termos e razão 2. Assim, podemos usar a fórmula geral que determina a soma dos termos de uma progressão geométrica para determinar o valor da soma $k + 2k + 4k + 8k + 16k + \cdots + 2^{l-3}k$ e, em seguida, é suficiente somar k para obter o valor de $k + k + 2k + 4k + 8k + 16k + \cdots + 2^{l-3}k$. Uma vez que $S_n = \frac{a_1(q^n-1)}{q-1}$, substituindo $a_1 = k, q = 2$ e $n = l-2$, segue que $S_{l-2} = k(2^{l-2}-1)$. Portanto, $k + k + 2k + 4k + 8k + 16k + \cdots + 2^{l-3}k = 2^{l-2}k$.

2. Afirmação 2: $(l-1) + (l-2) + (l-3)2 + (l-4)2^2 + \cdots + 2.2^{l-2} + 2^{l-3} = 2^{l-1} - 1$, para todo $l \geq 3$. Primeiramente, observamos que

$$\begin{aligned}&(l-1) + (l-2) + (l-3)2 + (l-4)2^2 + \cdots + 2.2^{l-2} + 2^{l-3} = \\ &= (l + l + 2l + 2^2l + 2^3l + \cdots + 2^{l-4}l + 2^{l-3}l) - \\ &(1 + 2 + 2.3 + 2^2.4 + 2^3.5 + \cdots + 2^{l-4}(l-2) + 2^{l-3}(l-1)).\end{aligned}$$

Vamos calcular o valor das duas somas destacadas pelos parênteses. Os elementos $\{l, 2l, 2^2l, 2^3l, \cdots, 2^{l-4}l, 2^{l-3}l\}$ são termos de uma progressão geométrica de razão 2. Assim, utilizando novamente que $S_n = \frac{a_1(q^n-1)}{q-1}$ e substituindo $a_1 = l$, $q = 2$ e $n = l-2$, segue que $S_{l-2} = \frac{l(2^{l-2}-1)}{2-1} = l2^{l-2} - l$. Logo,

$$l + l + 2l + 2^2l + 2^3l + \cdots + 2^{l-4}l + 2^{l-3}l = l2^{l-2}.$$

Agora, provaremos que $1 + 2 + 2.3 + 2^2.4 + 2^3.5 + \cdots + 2^{l-4}(l-2) + 2^{l-3}(l-1) = 2^{l-2}(l-2) + 1$, para todo $l \geq 3$. Para isso, utilizaremos o Princípio da Indução Finita, mostrando que a afirmação é verdadeira para $k = 3$ e, supondo que vale para $l = n$, provaremos que vale para $l = n+1$, onde para o valor l são consideradas as $l-1$ primeiras somas.

1. Passo base: A afirmação é verdadeira para $l = 3$. De fato, $1+2 = 3$ e $2^{l-2}(l-2)-1 = 2^{3-2}(3-2) + 1 = 2 + 1 = 3$.

2. Passo indutivo: Suponhamos que a afirmação é verdadeira para $l = n$, isto é,

$$1 + 2 + 2.3 + 2^2.4 + 2^3.5 + \cdots + 2^{n-4}(n-2) + 2^{n-3}(n-1) = 2^{n-2}(n-2) + 1,$$

que é equivalente a

$$2 + 2.3 + 2^2.4 + 2^3.5 + \cdots + 2^{n-4}(n-2) + 2^{n-3}(n-1) = 2^{n-2}(n-2)$$

e, a partir disso, mostraremos que o mesmo vale para $l = n + 1$, isto é, que

$$2+2.3+2^2.4+2^3.5+\cdots+2^{(n+1)-5}((n+1)-3)+2^{(n+1)-4}((n+1)-2)+2^{(n+1)-3}((n+1)-1) =$$

$$2^{(n+1)-2}((n+1)-2) = 2^{n-1}(n-1).$$

De fato, pela hipótese de indução, a igualdade

$$2 + 2.3 + 2^2.4 + 2^3.5 + \cdots + 2^{n-4}(n-2) + 2^{n-3}(n-1) = 2^{n-2}(n-2)$$

é válida. Somando $2^{n-2}n$ de ambos os lados, obtemos

$$2+2.3+2^2.4+2^3.5+\cdots+2^{n-4}(n-2)+2^{n-3}(n-1)+2^{n-2}n = 2^{n-2}(n-2)+2^{n-2}n.$$

Logo,

$$2+2.3+2^2.4+2^3.5+\cdots+2^{(n+1)-5}((n+1)-3)+2^{(n+1)-4}((n+1)-2)+2^{(n+1)-3}((n+1)-1) =$$

$$2^{n-2}(n-2) + 2^{n-2}n.$$

Além disso,

$$2^{n-2}(n-2) + 2^{n-2}n = 2^{n-2}(2n-2) = 2^{n-1}(n-1),$$

donde segue a igualdade

$$\begin{aligned}&2 + 2.3 + 2^2.4 + 2^3.5 + \cdots + 2^{(n+1)-5}((n+1)-3) + 2^{(n+1)-4}((n+1)-2)+\\ &+2^{(n+1)-3}((n+1)-1) = 2^{(n+1)-2}((n+1)-2) = 2^{n-1}(n-1).\end{aligned}$$

Assim,

$$(l+l+2l+2^2l+2^3l+\cdots+2^{k-4}l+2^{l-3}l)-(1+2+2.3+\cdots+2^{l-4}(l-2)+2^{l-3}(l-1))$$

$$= l2^{l-2} - 2^{l-2}(l-2) + 1 = 2^{l-1} - 1.$$

Substituindo a Afirmação 1 e a Afirmação 2 na Equação (6.40), segue que

$$D(\mathbb{L}) = -2^{2^{(k-(l-2))}(2^{l-2}k-(2^{l-1}-1))}d^{n-1},$$

como queríamos provar. O sinal negativo da Equação (6.40) e, consequentemente, do resultado final, vem do fato que, ao calcular o determinante da matriz pelo método

de Laplace, obtemos

$$(-1)^{n+2}(-1)^{n-1+2}(-1)^{n-2+2}...(-1)^{\frac{n}{2}+2+2}$$

referente à parte superior, e

$$(-1)^{\frac{n}{2}+1+2}(-1)^{\frac{n}{2}+2}(-1)^{\frac{n}{2}-1+2}...(-1)^{3+2}$$

referente à parte inferior. Dessa forma, são $\frac{n}{2}-1$ termos em cada uma dessas duas parcelas, totalizando $n-2$ termos, onde, metade dos expoentes são ímpares e metade são pares. Sendo assim, há $\frac{n-2}{2}$ expoentes pares e $\frac{n-2}{2}$ expoentes ímpares, isto é, $\frac{2^k-2}{2} = \frac{2(2^{k-1}-1)}{2} = 2^{k-1}-1$ de cada. Como $k \geq 1$, há uma quantidade ímpar de expoentes ímpares e, consequentemente, o valor fica negativo.

Com isso, provamos o resultado. □

6.3 Exemplos

Por meio dos resultados apresentados nos Teoremas 6.9 e 6.11, determinamos uma base do anel de inteiros algébricos e o discriminante do anel de inteiros algébricos de alguns corpos de números do tipo $\mathbb{Q}(\sqrt[2^k]{d})$. Os valores que encontraremos por meio das fórmulas podem ser verificados fazendo uso de algum software como, por exemplo, Magma ou Wolfram Mathematica. As bases dadas pelo Magma são exatamente iguais às encontradas nos exemplos abaixo, enquanto as obtidas pelo Wolfram Mathematica são diferentes, porém, são equivalentes, uma vez que fornecem o mesmo discriminante.

Exemplo 1. Seja $\mathbb{L} = \mathbb{Q}(\sqrt[64]{17})$. Como $d = 17$ é inteiro e livre de quadrados, e $d \equiv 1 \pmod{16}$ de modo que 16 é a maior potência de 2 que divide $d-1$, segue, de acordo com o Teorema 6.9, que uma base integral de $\mathbb{L}$ é dada por

$$\{1, \theta, \ldots, \theta^{31}, \omega_1, \omega_1\theta, \ldots, \omega_1\theta^{15}, \omega_2, \omega_2\theta, \ldots, \omega_2\theta^7, \omega_3, \omega_3\theta, \omega_3\theta^2, \omega_3\theta^3, \omega_3\theta^4, \omega_3\theta^5, \omega_3\theta^6, \omega_3\theta^7\}.$$

onde $\theta = \sqrt[64]{17}, \omega_1 = \frac{1+\theta^{32}}{2}, \omega_2 = \frac{1+\theta^{16}+\theta^{32}+\theta^{48}}{4}$ e $\omega_3 = \frac{1+\theta^8+\theta^{16}+\theta^{24}+\theta^{32}+\theta^{40}+\theta^{48}+\theta^{56}}{8}$.

Ademais, de acordo com o Teorema 6.11, o discriminante do anel de inteiros algébricos de $\mathbb{L}$ é dado por

$$-2^{2^{(k-(l-2))}(2^{l-2}k-(2^{l-1}-1))}d^{n-1}.$$

Assim, como $l = 4, k = 6, d = 17$ e $n = 64$, substituindo esses valores na fórmula obtemos $-2^{16\times17}17^{63} = -2^{272}17^{63}$.

Exemplo 2. Seja $\mathbb{L} = \mathbb{Q}(\sqrt[128]{257})$. Como $d = 257$ é inteiro e livre de quadrados, e

$d \equiv 1 \pmod{256}$ de modo que $2^8 = 256$ é a maior potência de 2 que divide $d-1$, segue, de acordo com o Teorema 6.9, que uma base integral de $\mathbb{L}$ é dada por

$$\Big\{1, \theta, \theta^2, \ldots, \theta^{63}, \omega_1, \omega_1\theta, \omega_1\theta^2, \ldots, \omega_1\theta^{31}, \omega_2, \omega_2\theta, \omega_2\theta^2, \ldots, \omega_2\theta^{15}, \omega_3, \omega_3\theta, \omega_3\theta^2, \ldots, \omega_3\theta^7,$$

$$\omega_4, \omega_4\theta, \omega_4\theta^2, \omega_4\theta^3, \omega_5, \omega_5\theta, \omega_6, \omega_7\Big\}.$$

onde $\theta = \sqrt[128]{257}$, $\omega_1 = \frac{1+\theta^{64}}{2}$, $\omega_2 = \frac{1+\theta^{32}+\theta^{64}+\theta^{96}}{4}$, $\omega_3 = \frac{1+\theta^{16}+\theta^{32}+\theta^{48}+\theta^{64}+\theta^{80}+\theta^{96}+\theta^{112}}{8}$,
$\omega_4 = \frac{1+\theta^8+\theta^{16}+\theta^{24}+\theta^{32}+\theta^{40}+\theta^{48}+\theta^{56}+\theta^{64}+\theta^{72}+\theta^{80}+\theta^{88}+\theta^{96}+\theta^{104}+\theta^{112}+\theta^{120}}{16}$,
$\omega_5 = \frac{1+\theta^4\theta^8+\theta^{12}+\cdots+\theta^{112}+\theta^{116}+\theta^{120}+\theta^{124}}{32}$, $\omega_6 = \frac{1+\theta^2+\theta^4+\theta^6+\theta^8+\cdots+\theta^{120}+\theta^{122}+\theta^{124}+\theta^{126}}{64}$ e
$\omega_7 = \frac{1+\theta+\theta^2+\theta^3+theta^4+\cdots+\theta^{124}+\theta^{125}+\theta^{126}+\theta^{127}}{128}$.

Ademais, de acordo com o Teorema 6.11, o discriminante do anel de inteiros algébricos de $\mathbb{L}$ é dado por

$$-2^{2^{(k-(l-2))}(2^{l-2}k-(2^{l-1}-1))}d^{n-1}.$$

Assim, como $l = 8, k = 7, d = 247$ e $n = 128$, substituindo esses valores na fórmula obtemos $-2^{2^1(2^6\times 7-(2^7-1))}247^{127} = -2^{642}247^{127}$.

6.4 Considerações finais

O problema de determinar explicitamente bases para anéis de inteiros algébricos acarreta em diversos desafios, pois são poucas as ferramentas disponíveis para sua resolução e, por essa razão, são poucos os trabalhos que abordam esse problema para além do corpo monogênico ou casos particulares. Esse capítulo, no entanto, fornece a resposta para uma família inteira de corpos, onde uma base do anel de inteiros algébricos é descrita de maneira extremamente simples, tal qual a fórmula apresentada para o cálculo do discriminante. A possibilidade de determinar facilmente e rapidamente uma base integral e o discriminante do anel de inteiros algébricos de um corpo puro cujo grau é uma potência de 2 tem vantagens em várias áreas da Matemática e da Ciência da Computação, dada a importância dessa família de corpos e também devido às diversas aplicações que podem ser feitas pelo conhecimento dessas duas informações: base integral e discriminante.

7 Conclusão e perspectivas futuras

Neste trabalho, apresentamos uma base integral e o discriminante do anel de inteiros algébricos dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. Provamos que o corpo $\mathbb{L}$ de grau $n = 2^k$ possui $k+1$ estruturas de bases integrais distintas, a qual é determinada pelo valor de d, sendo uma quando $d \not\equiv 1(mod\ 4)$, e k possibilidades quando $d \equiv 1(mod\ 2^l)$, uma para cada valor de l, onde $2 \leq l \leq k+1$, sendo 2^l a maior potência de 2 que divide $d-1$, exceto quando $l = k+1$, pois este corresponde ao maior valor de l que altera a estrutura da base. Desse modo, conhecendo o valor do grau $n = 2^k$ e o valor de d, é possível estabelecer uma base integral e o discriminante a ela associado para qualquer corpo $\mathbb{L}$ desse tipo.

No primeiro capítulo fizemos uma breve revisão de alguns conceitos da Teoria Algébrica dos Números, onde destacamos a Proposição 1.39, cuja importância no desenvolvimento das demonstrações ficou evidente em cada caso.

O segundo capítulo foi totalmente voltado aos corpos monogênicos, onde utilizando o conceito de índice e baseando-se em [10], descrevemos valores de d tais que o anel de inteiros algébricos do corpo $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ possui base potente. Esse tipo de abordagem tem sido muito utilizada e dentro deste escopo é possível desenvolver vários trabalhos distintos, fixando alguma família de corpos de números e buscando os valores tal que uma base do anel de inteiros algébricos é uma base potente, por exemplo, podemos determinar os valores de d que tornam o corpo de números $\mathbb{L} = \mathbb{Q}(\sqrt[n]{d})$, onde $n = 3.5^k.2^r$, monogênico. Ainda dentro dessa perspectiva, é possível analisar os valores de d tal que uma base do anel de inteiros algébricos é potente, não necessariamente sobre o conjunto dos números inteiros, mas sobre outros corpos intermediários. Observando os resultados apresentados neste trabalho, podemos constatar que dado $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, tal que $d \equiv 2^l + 1(mod\ 2^{l+1})$ para todo $2 \leq l \leq k-1$, então $\mathbb{L}$ é monogênico sobre $\mathbb{K} = \mathbb{Q}(\sqrt[2^{k-1}]{d})$, já que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$. Uma análise similar pode ser feita para diversos corpos em que é conhecida uma base integral sobre $\mathbb{Z}$.

No terceiro capítulo, em cada seção, apresentamos as bases integrais e os discriminantes a elas associados dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ para algum caso particular, ou seja, especificando

o valor de k. Para cada valor de k analisado, designadamente, $4, 8, 16$ e 32, percorremos todos os valores inteiros de $d \neq 1$ livre de quadrados e explicitamos tanto uma base do anel de inteiros algébricos como o discriminante, ambos em função do valor de d. Dessa forma, foi possível identificar o padrão que as bases seguem para cada valor de d, as quais se repetem periodicamente modulo 2^{k+1}, além de adquirir familiaridade com a técnica utilizada nas demonstrações, já que todos os casos foram detalhadamente demonstrados (exceto grau 32 por ser similar aos demais). Seguindo nessa linha, existem vários trabalhos na literatura que fixam um determinado grau e exploram os valores e congruências de d a fim de obter bases integrais para esses tipos de corpos, como por exemplo no artigo [31], onde dado o corpo $\mathbb{L} = \mathbb{Q}(\sqrt[6]{d})$, com $d \neq 1$ um inteiro livre de quadrados, foram apresentadas 6 estruturas de bases integrais distintas conforme a variação do valor de d. Nesse contexto, podemos considerar, por exemplo, o corpo de grau 10, ou seja, $\mathbb{L} = \mathbb{Q}(\sqrt[10]{d})$, com $d \neq 1$ um inteiro livre de quadrados e apresentar uma base integral de $\mathbb{L} = \mathbb{Q}(\sqrt[10]{d})$ para certos valores de d. Além disso, é possível analisar casos onde d não é livre de quadrados, como foi realizado, por exemplo, no artigo [18], onde foram determinadas bases integrais do corpo $\mathbb{L} = \mathbb{Q}(\sqrt[3]{d})$, onde $d \neq 1$ não é livre de quadrados e é livre de cubos. Nesse sentido, considerando graus maiores, existem vários casos a serem explorados.

No quarto capítulo, focamos em determinar uma base integral do corpo $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ para uma família de valores de d formada pelos elementos tais que $d \equiv 5(mod\ 8)$, a qual é englobada em todos os corpos cujo grau é uma potencia de 2, exceto no caso de grau 2. Além de explicitar uma base integral, também fornecemos uma fórmula que permite o cálculo do discriminante do anel de inteiros algébricos de $\mathbb{L}$ conhecendo-se apenas os valores de k e d. O quinto capítulo segue o mesmo raciocínio, porém a família de valores de d que analisamos são as formadas pelos elementos tal que $d \equiv 9(mod\ 16)$. Dentro dessa linha outros trabalhos podem ser analisados e generalizados. Podemos considerar, por exemplo, os corpos cujo grau é uma potência de 3 do tipo $\mathbb{L} = \mathbb{Q}(\sqrt[3^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados, pois através de uma análise de suas bases intergrais é visível que seu anel de inteiros algébricos também possui um certo padrão em sua formação, onde o valor que determina a estrutura da base é o resto da divisão de d por 9 e de d por outras potências de 3. Assim, uma possibilidade de iniciar o estudo dos corpos cujo grau é uma potência de 3, é fixando, por exemplo, os corpos $\mathbb{L} = \mathbb{Q}(\sqrt[3^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e tal que $d \equiv 10(mod\ 27)$ determinando uma base do anel de inteiros algébricos restrito a esse caso. Uma vez que se tenha respondido a essa questão, pode-se avançar para a família de valores de $d \neq 1$ tal que $d \equiv 28(mod\ 81)$, e assim, sucessivamente.

Agora, no sexto capítulo, estendemos os resultados feitos nos capítulos anteriores

apresentando uma base integral e o discriminante do anel de inteiros algébricos para qualquer corpo puro da forma $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. Partindo desse mesmo raciocínio, outras famílias de corpos podem ser analisadas a fim de encontrar uma base do anel de inteiros algébricos e o seu discriminante, como por exemplo, os corpos $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$, onde $d \neq 1$ não é livre de quadrados ou os corpos puros de grau 3.2^k, com $k \in \mathbb{N}$, da forma $\mathbb{L} = \mathbb{Q}(\sqrt[3.2^k]{d})$, uma vez que o grau da extensão $\mathbb{K} \subset \mathbb{L}$ para $\mathbb{K} = \mathbb{Q}(\sqrt[3.2^{k-1}]{d})$ também é 2, possibilitando utilizar o mesmo raciocínio utilizado nesse trabalho. Analisar famílias de corpos desta natureza é pertinente, já que existem vários artigos explorando os corpos de grau 6 e, neste caso, o estudo dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[3.2^k]{d})$ representa uma generalização.

Finalmente, vale ressaltar também, que a presente tese foi desenvolvida sempre direcionando a análise da parte teórica. Neste sentido, existem várias possibilidades de estudos de corpos puros da forma $\mathbb{L} = \mathbb{Q}(\sqrt[n]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados, tanto na parte teórica quanto na parte de aplicações. Nesta linha, encaminhando-se agora para a parte das aplicações, utlizando os resultados aqui apresentados, é possível analisar a teoria de reticulados algébricos via o homomorfismo canônico tanto na busca de reticulados em relação à densidade de centro, quanto na busca de reticulados bem arredondados cujo grau é uma potência de 2, ou seja, buscar reticulados de grau 2^k que possuem boas propriedades. Entretanto, como nesse caso o corpo $\mathbb{L}$ é misto, ou seja, possui monomorfismos reais e complexos, existe a necessidade de explorar uma forma traço para o seu cálculo, uma vez que a forma traço conhecida é dada para corpos totalmente imaginários ou corpos totalmente reais. Assim, determinar essa fórmula é mais um dos possíveis trabalhos que podem ser desenvolvidos futuramente.

Referências

[1] ANDRADE, A. A. et al. Constructions of dense lattices over number fields. *TEMA Tend. Mat. Apl. Comput.*, v. 21, n. 1, p. 57–63, 2020. ISSN 1677-1966,2179-8451. Disponível em: <https://doi.org/10.5540/tema.2020.021.01.57>.

[2] ARAUJO, R. R. de. *Reticulados algébricos e aplicações a códigos e criptografia*. Tese (Doutorado) — Unicamp, 2018.

[3] SICUTI, P. G. *Um estudo sobre reticulados algébricos bem arredondados*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2020.

[4] MUSIN, O. R. The kissing number in four dimensions. *Ann. of Math. (2)*, v. 168, n. 1, p. 1–32, 2008. ISSN 0003-486X,1939-8980. Disponível em: <https://doi.org/10.4007/annals.2008.168.1>.

[5] FERRARI, A. J.; SOUZA, T. M. R. Rotated A_n-lattice codes of full diversity. *Adv. Math. Commun.*, v. 16, n. 3, p. 439–447, 2022. ISSN 1930-5346,1930-5338. Disponível em: <https://doi.org/10.3934/amc.2020118>.

[6] FUKSHANSKY, L.; PETERSEN, K. On well-rounded ideal lattices. *Int. J. Number Theory*, v. 8, n. 1, p. 189–206, 2012. ISSN 1793-0421,1793-7310. Disponível em: <https://doi.org/10.1142/S179304211250011X>.

[7] LANGE, T.; STEINWANDT, R. (Ed.). *Post-quantum cryptography. 9th international conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9–11, 2018. Proceedings*. [S.l.]: Cham: Springer, 2018. v. 10786. (Lect. Notes Comput. Sci., v. 10786). ISSN 0302-9743. ISBN 978-3-319-79062-6; 978-3-319-79063-3.

[8] YAKKOU, H. B.; FADIL, L. E. On monogenity of certain pure number fields defined by $x^{p^r} - m$. *Int. J. Number Theory*, v. 17, n. 10, p. 2235–2242, 2021. ISSN 1793-0421,1793-7310. Disponível em: <https://doi.org/10.1142/S1793042121500858>.

[9] HAMEED, A. et al. On existence of canonical number system in certain classes of pure algebraic number fields. *J. Prime Res. Math.*, v. 7, p. 19–24, 2011. ISSN 1817-2725.

[10] HAMEED, A.; NAKAHARA, T. Integral bases and relative monogenity of pure octic fields. *Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér.*, v. 58, n. 4, p. 419–433, 2015. ISSN 1220-3874.

[11] FUNAKURA, T. On integral bases of pure quartic fields. *Math. J. Okayama Univ.*, v. 26, p. 27–41, 1984. ISSN 0030-1566.

[12] ANDRADE, A. A.; FACINI, L. S.; ESTEVES, L. C. Algebraic intergers of pure quartic extensions. *International Journal of Apllied Mathematics*, v. 36, n. 1, p. 99–106, 2023. ISSN 1314-8060.

[13] HAMEED, A. *On Pure Octic Fields Related to a Problem of Hasse*. Tese (Doutorado) — National University of Computer and Emerging Sciences, 2015.

[14] YAKKOU, H. B.; KCHIT, O. On power integral bases of certain pure number fields defined by $x^{3^r} - m$. *São Paulo J. Math. Sci.*, v. 16, n. 2, p. 1072–1079, 2022. ISSN 1982-6907,2316-9028. Disponível em: <https://doi.org/10.1007/s40863-021-00251-2>.

[15] FACINI, L. S. *Uma introdução aos corpos não abelianos de grau menor ou igual a 6*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2021.

[16] YAKKOU, H. B. On nonmonogenic number fields defined by trinomials of type $x^n + ax^m + b$. *Rocky Mountain J. Math.*, v. 53, n. 3, p. 685–699, 2023. ISSN 0035-7596,1945-3795. Disponível em: <https://doi.org/10.1216/rmj.2023.53.685>.

[17] FADIL, L. E.; KCHIT, O. On monogenity of certain pure number fields defined by $x^{2^r \cdot 7^s} - m$. *Bol. Soc. Parana. Mat. (3)*, v. 41, p. 1–9, 2023. ISSN 0037-8712,2175-1188. Disponível em: <https://doi.org/10.5269/bspm.62352>.

[18] ANDRADE, A.; FACINI, L.; ESTEVES, L. Algebraic integers of certain cubic extensions: Inteiros algébricos de certas extensões cúbicas. *Brazilian Journal of Development*, v. 8, n. 8, p. 56768–56786, 2022.

[19] GAáL, I.; REMETE, L. Non-monogenity in a family of octic fields. *Rocky Mountain J. Math.*, v. 47, n. 3, p. 817–824, 2017. ISSN 0035-7596,1945-3795. Disponível em: <https://doi.org/10.1216/RMJ-2017-47-3-817>.

[20] CHANG, M.-L. Non-monogeneity in a family of sextic fields. *J. Number Theory*, v. 97, n. 2, p. 252–268, 2002. ISSN 0022-314X,1096-1658. Disponível em: <https://doi.org/10.1016/S0022-314X(02)00004-5>.

[21] MARCUS, D. A. *Number theory*. 1. ed. New York: Springer-Verlag, 1977.

[22] SAMUEL, P. *Algebraic theory of numbers*. 1. ed. Paris: Hermann, 1970.

[23] ALACA, S.; WILLIAMS, K. S. *Introductory algebraic number theory*. 1. ed. New York: Cambridge University Press, 2004.

[24] ANDRADE, A. A. de. *Uma introdução a teoria algébrica dos números*. 1. ed. São José do Rio Preto - SP: Amazon.com, 2021.

[25] ARAUJO, R. R. de. *Anéis de inteiros de corpos de números e aplicações*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho" - IBILCE, 2015.

[26] NARKIEWICS, W. *Elmentary and analytic theory of algebraic numbers*. 3. ed. Breslávia: Springer-Verlag, 2004.

[27] VICENTE, J. P. G. *Reticulados de posto 3 em corpos de números*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2000.

[28] RODRIGUES, V. C. da S. *Reticulados de posto 4 em corpos de números*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2001.

[29] RIBEIRO, A. C. *Reticulados sobre corpos de números*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2003.

[30] REMETE, L. Integral bases of pure fields with square-free parameter. *Studia Sci. Math. Hungar.*, v. 57, n. 1, p. 91–115, 2020. ISSN 0081-6906,1588-2896. Disponível em: <https://doi.org/10.1556/012.2020.57.1.1450>.

[31] ANDRADE, A. A.; FACINI, L. S.; ESTEVES, L. C. Algebraic intergers of pure sextic extensions. *Journal of Prime Reaserch in Mathematics*, v. 18, n. 2, p. 112–124, 2022.

Índice Remissivo