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

Naísa Camila Garcia Tosti

Corpos Abelianos Reais e Forma Quadrática.

São José do Rio Preto

2017

Naísa Camila Garcia Tosti

Corpos Abelianos Reais e Forma Quadrática.

Dissertação apresentada para obtenção do título de Mestre em Matemática, Área de Álgebra, junto ao Programa de Pós Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus São José do Rio Preto.

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

Financiadora: CAPES

São José do Rio Preto

2017

Garcia Tosti, N. C.
Corpos abelianos reais e forma quadrática / Naísa Camila Garcia Tosti. -- São José do Rio Preto, 2017
95 f. : il., tabs.

Orientador: Trajano Pires da Nóbrega Neto
Dissertação (mestrado) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Instituto de Biociências, Letras e Ciências Exatas

1. Matemática. 2. Álgebra comutativa. 3. Teoria dos números. 4. Teoria dos reticulados. 5. Homomorfismos (Matemática) I. Tosti, Naísa Camila Garcia. II. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU – 512.71

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

Naísa Camila Garcia Tosti

Corpos Abelianos Reais e Forma Quadrática.

Dissertação apresentada para obtenção do título de Mestre em Matemática, Área de Álgebra, junto ao Programa de Pós Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus São José do Rio Preto.

BANCA EXAMINADORA

Prof. Dr. Trajano Pires da Nóbrega Neto
Professor Adjunto
UNESP - Universidade Estadual Paulista - São José do Rio Preto
Orientador

Prof. Dr. Antonio Aparecido de Andrade
Professor Adjunto
UNESP - Universidade Estadual Paulista - São José do Rio Preto

Prof. Dr. José Valter Lopes Nunes
Professor Associado
UFC - Universidade Federal do Ceará - Fortaleza

São José do Rio Preto, 17 de fevereiro de 2017.

Agradecimentos

A Deus, o que seria de mim sem a fé que eu tenho nEle?

A minha família que, com muita paciência, carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da minha vida.

Ao Professor Dr. Trajano Pires da Nóbrega Neto pela orientação e paciência, pelos conhecimentos compartilhados e, principalmente, pela confiança depositada.

Aos professores Antonio Aparecido de Andrade e José Valter Lopes Nunes por aceitarem compor a banca examinadora.

Ao professor José Carmelo Interlando, que mesmo sem nos encontrarmos pessoalmente, contribuiu virtualmente para a elaboração deste trabalho.

Aos meus professores de graduação e pós-graduação, pelos ensinamentos e experiências compartilhadas durante esses anos.

A todos os meus amigos de graduação e pós-graduação, em especial, ás irmãs que a matemática me proporcionou Sabrina Suelen Amaral e Letícia Ellen Dal'Canton.

Ao Anderson Tosti pela paciência, apoio e companheirismo.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, pelo suporte financeiro.

" A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."

(Albert Einstein)

Resumo

O propósito deste trabalho é estudar alguns corpos abelianos, mais especificamente, as extensões reais maximais contidas nos corpos ciclotômicos de grau 8 e, os subcorpos dos corpos ciclotômicos $\mathbb{Q}(\zeta_7)$ e $\mathbb{Q}(\zeta_{17})$. Em tais corpos, determinamos base integral, discriminante, grupo de Galois e construimos submódulos de posto máximo do anel dos inteiros algébricos com sua respectiva representação geométrica. Além disso, calculamos a densidade de centro destes reticulados.

Palavras-chave: Reticulados. Homomorfismo de Minkowski. Corpos abelianos reais.

Abstract

The purpose of this work is to investigate some Abelian Number Fields, especifically the maximal extension contained in the cyclotomic fields of degree 8, and the subfields of the cyclotomic fields $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{17})$. In such fields, we compute: integral bases, discriminant, Galois group and submoduli with maximal rank in the ring of algebraic integers, its geometrical realization with the respective center density.

Keywords: Lattices. Minkowski homomorphism. Real Abelian fields.

Lista de Símbolos

$\mathbb{N}$: Conjunto dos números naturais

$\mathbb{Z}$: Conjunto dos números inteiros

$\mathbb{Q}$: Conjunto dos números racionais

$\mathbb{R}$: Conjunto dos números reais

$\mathbb{C}$: Conjunto dos números complexos

$S(x_0, r)$: Esfera de raio r e centro em x_0

$\sum$: Somatório

$\prod$: Produtório

$Re(z)$: Parte real do elemento z

$Im(z)$: Parte imaginária do elemento z

$\varphi(n)$: Função de Euler aplicada a n

$\mathcal{I}$: Ideal

$\mathcal{M}$: Módulo

G, H: Grupos

$o(G)$: ordem do grupo G

$H < G$: H é subgrupo de G

$(G : H)$: Índice de H em G

R, A, B: Anéis

A': Conjunto dos elementos de R que são integrais sobre A

$\mathbb{L}, \mathbb{K}, \mathbb{M}$: Corpos

$\mathcal{O}_{\mathbb{K}}$: Elementos de $\mathbb{K}$ que são integrais sobre $\mathbb{Z}$

$[\mathbb{L} : \mathbb{K}]$: Dimensão de $\mathbb{L}$ sobre $\mathbb{K}$, ou, grau da extensão

$\mathbb{K}[\alpha]$: Conjunto de todas as expressões polinomiais em α com coeficientes em $\mathbb{K}$

$\mathbb{Q}(\zeta_n)^+$: Subcorpo real maximal de um corpo ciclotômico

$Aut(\mathbb{L})$: Conjunto dos automorfismos de $\mathbb{L}$

$\mathbb{K}^H$: Corpo fixo associado a H

$\partial(p)$: Grau do polinômio $p(X)$

$\Phi_n(X)$: n-ésimo polinômio ciclotômico

ρ: Raio de empacotamento

$\delta(\Lambda)$: Densidade de centro do reticulado Λ

$\Delta(\Lambda)$: Densidade de empacotamento do reticulado Λ

Sumário

Apresentação

O Problema Clássico do Empacotamento Esférico, consiste em dispor esferas idênticas n-dimensionais em $\mathbb{R}^n$, não sobrepostas, de maneira que, o maior volume possível seja ocupado. Este problema matemático desperta o interesse de pesquisadores, e futuros pesquisadores, pois ainda possui grandes questões sem soluções.

Em terceira dimensão, um exemplo desse desafio é o problema de disposição das laranjas do feirante. Em dimensão mais alta, uma de suas aplicações pode ser encontrada em sistemas de telecomunicações.

Neste trabalho, estaremos interessados nos empacotamentos esféricos cujo conjunto dos centros, constitui um subgrupo discreto de $\mathbb{R}^n$, o qual denominamos reticulados. Mais ainda, nosso objetivo será determinar reticulados, via homomorfismo de Minkowski, de corpos abelianos, mais especificamente, trabalharemos com os subcorpos reais maximais de corpos ciclotômicos de grau 8, o qual denotamos por $\mathbb{Q}(\zeta_n)^+$ e n assume um dos seguintes valores: 15, 16, 20, 24 e 30, e também, com os subcorpos de $\mathbb{Q}(\zeta_7)$ e $\mathbb{Q}(\zeta_{17})$. Para isto, divimos esta dissertação em três capítulos.

Os conceitos elementares utilizados neste trabalho estão agrupados no primeiro capítulo. Neste, abordamos conceitos substanciais da Teoria dos Números, tais como elemento integral sobre um anel e elementos algébricos sobre um corpo. Na sequência definimos os corpos de números e apresentamos um caso específico, os corpos quadráticos, no qual aplicamos toda teoria desenvolvida neste capítulo, com o intuito de auxiliar na compreensão do leitor, definimos também norma, traço, discriminante e base integral, fazemos uma breve revisão sobre o corpo dos números complexos e por fim, apresentamos alguns resultados da Teoria de Galois. Neste capítulo, a principal referencia utilizada foi [10].

No segundo capítulo, apresentamos outro exemplo de corpo de números, os corpos ciclotômicos pois, como já mencionamos, estes serão o foco deste trabalho. Além disso, abordamos com mais detalhes os conceitos matemáticos envolvidos no problema do empacotamento esférico. Definimos o raio de empacotamento, e as densidades de empacotamento e de centro, definimos também, o homomorfismo de Minkowski, bem como, resultados que nos garante obter reticulados via este

homomorfismo. Isto posto, apresentamos algumas propriedades, de tais conceitos postos, à corpos totalmente real ou totalmente imaginários. Em seguida, apresentamos a forma quadrática. Por fim, exibimos algumas propriedades da função traço e as aplicamos em raízes n-ésimas primitivas da unidade, mostramos também como é o *compositum* e a interseção de dois corpos ciclotômicos.

O terceiro e último capítulo, tem como objetivo aplicar todos os resultados até então desenvolvidos no trabalho à todos os subcorpos de $\mathbb{Q}(\zeta_7)$ e $\mathbb{Q}(\zeta_{17})$ e, aos subcorpos reais maximais de corpos ciclotômicos de grau 8. O iniciamos explicitando o grupo de Galois de um corpo ciclotômico qualquer, posteriormente, definimos base integral normal e apresentamos um resultado que nos auxilia no cálculo do discriminante, válido apenas para corpos abelianos. Em seguida, com o objetivo de detalhar a teoria desenvolvida para corpos abelianos de condutor primo, exibimos uma base integral normal de $\mathbb{Q}(\zeta_p)$, p primo, bem como para seus subcorpos, para estes, além de sua explicitação, discutimos em quais casos estes são totalmente real ou totalmente imaginário. Apresentamos também a forma quadrática e sua minimização, e finalmente, aplicamos a teoria desenvolvida em $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{17})$ e seus respectivos subcorpos. A ultima seção, tem como foco os subcorpos reais maximais de corpos ciclotômicos de grau 8, para estes, determinamos o seu anel de inteiros e exibimos uma base integral. Além disso, em cada caso, explicitamos o n-ésimo polinômio ciclotômico, apresentamos a respectiva ação do grupo de Galois e calculamos o discriminante de cada subcorpo. Obtivemos também, reticulados a partir da imagem de um $\mathbb{Z}$-módulo de $\mathbb{Q}(\zeta_n)^+$, considerando $n = 15$ e 24, pelo homomorfismo de Minkowski, e determinamos seus respectivos raio de empacotamento e densidade de centro. Por fim, para todos os subcorpos citados, determinamos reticulados via homomorfismo de Minkowski aplicado no anel dos inteiros, bem como seu respectivo raio de empacotamento e densidade de centro.

Capítulo

1

Corpos de Números

O presente capítulo, abrange conceitos elementares de Teoria dos Números. Primeiramente, nosso objetivo será mostrar que o conjunto dos elementos integrais sobre um anel constitui um anel. Em seguida, particularizamos o conceito anterior, isto é, abordamos os denominados elementos algébricos sobre um corpo. Definimos corpos de números e exploramos algumas de suas propriedades, neste momento, os principais resultados são a Proposição Multiplicidade de Graus e o Teorema do Elemento Primitivo. Depois disto, exibimos os corpos quadráticos, um exemplo de corpos de números, para o qual explicitamos seu anel dos elementos integrais. Além disto, conforme a teoria deste capitulo é desenvolvida, retornamos a este corpo para aplicar os novos conceitos. Os referidos conceitos são tais como a norma, o traço, o discriminante e a base integral, em todos os casos, além da aplicação já mencionada, as propriedades fundamentais serão estudas. Neste capítulo também, revisamos os corpos dos números complexos e alguns resultados da Teoria de Galois.

Nosso objetivo, além de, proporcionar ao leitor familiarização com a notação adotada, é oferecer as ferramentas necessárias para a compreensão do restante do trabalho. A principal referência deste capítulo é [10], no entanto, também consultamos [6] e [11].

1.1 Elemento Integral sobre um Anel

O objetivo principal desta seção, é mostrar que o conjunto constituído pelos elementos integrais sobre um anel, é um anel. Para isto, primeiramente, definiremos o que são elementos integrais sobre um anel, posteriormente, apresentaremos alguns resultados importantes para a compreensão deste conceito e que serão necessários para a demonstração do resultado principal, além de algumas consequências relevantes.

Definição 1.1.1. *Sejam R um anel e A um subanel de R. Dizemos que um elemento x de R é integral sobre A, se este é raiz de um polinômio mônico com coeficientes em A. Em outras palavras, x satisfaz a seguinte equação:*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0,$$

onde $a_i \in A, \forall i = 1, ..., n-1$.

A referida equação é denominada Equação de Dependência Integral de x.

Exemplos 1.1.2. *1. Considerando $R = \mathbb{R}$, $A = \mathbb{Z}$ e $x = \sqrt{2} + \sqrt{3}$, temos que x é integral sobre A, onde $x^4 - 10x^2 + 1 = 0$ é sua equação de dependência integral.*

2. Considerando $R = \mathbb{R}$, $A = \mathbb{Z}$ e $x = \sqrt{3} + \sqrt[3]{5}$, temos que x é integral sobre A.

De fato, x é raiz do polinômio mônico $p(X) = X^6 - 9X^4 - 10X^3 + 27X^2 - 90X - 2$.

3. Os números racionais da forma $\frac{1}{n}$, $n \in \mathbb{N}^*$ são integrais sobre $\mathbb{Q}$ pois satisfazem a seguinte equação:

$$x - \frac{1}{n} = 0.$$

4. Os números racionais $q \in \left\{\frac{1}{k};\quad k \in \mathbb{N},\quad k \geq 2\right\}$ não são integrais sobre $\mathbb{Z}$.

De fato, suponha por absurdo que $q = \frac{1}{k}$, com $k \in \mathbb{N}$ e $k \geq 2$, seja integral sobre $\mathbb{Z}$, então existem $a_i's \in \mathbb{Z}$, $i = 0, 1, \cdots, n-1$ tais que:

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

Multiplicando a equação por k^n, temos:

$$1 + a_{n-1}k + \cdots + a_1k^{n-1} + a_0k^n = 0.$$

Colocando k em evidência, temos que:

$$1 + k(a_{n-1} + \cdots + a_1k^{n-2} + a_0k^{n-1}) = 0.$$

Isto significa que 1 é multiplo de k, $k \geq 2$, o que é um absurdo.

O elemento $x = \sqrt[7]{7} - \sqrt[5]{5} + \sqrt[4]{4} \in \mathbb{R}$ é integral sobre $\mathbb{Z}$. No entanto, encontrar sua equação de dependência integral, não é uma tarefa simples. Para este caso e similares, podemos garantir que um elemento é integral sobre um anel, sem mostrar explicitamente sua referida equação. Essa garantia

nos é concedida pelo seguinte teorema, cuja demonstração será omitida mas, pode ser encontrada na referência citada:

Teorema 1.1.3. *([10], pág: 27) Sejam R um anel, A um subanel de R e $x \in R$. Então, as seguintes condições são equivalentes:*

(i) x é integral sobre A;

(ii) O anel $A[x]$ é um A-módulo finitamente gerado;

(iii) Existe um subanel B de R tal que, B é um A-módulo finitamente gerado contendo A e x.

Com este resultado, podemos refazer o exemplo 4. Seja $q \in \left\{\frac{1}{n};\ \ n \in \mathbb{N},\ \ n \geq 2\right\}$, e suponhamos por absurdo que q é integral sobre $\mathbb{Z}$. Então pelo Teorema 1.1.3, $\mathbb{Z}[q]$ é um $\mathbb{Z}$-módulo finitamente gerado. Logo, existe um conjunto finito, $\{\frac{c_1}{n^{t1}}, \frac{c_2}{n^{t2}}, \cdots, \frac{c_k}{n^{tk}}\}$ com $c_1, \cdots, c_k \in \mathbb{Z}$ e $t_1, \cdots, t_k \in \mathbb{N}$, que gera $\mathbb{Z}[q]$. Seja $t = t_1 + \cdots + t_k$, é claro que $\frac{1}{n^t} \in \mathbb{Z}[q]$, assim, $\frac{1}{n^t}$ é combinação linear dos elementos que geram $\mathbb{Z}[q]$, isto é,

$$\frac{1}{n^t} = \frac{d_1 c_1}{n^{t_1}} + \frac{d_2 c_2}{n^{t_2}} + \cdots + \frac{d_k c_k}{n^{t_k}},$$

multiplicando por n^t em ambos lados da igualdade temos:

$$1 = d_1 c_1 n^{t-t_1} + d_2 c_2 n^{t-t_2} + \cdots + d_k c_k n^{t-t_k},$$

isto é, 1 é multiplo de n, $n \geq 2$, o que é um absurdo, e portanto, q não é integral sobre $\mathbb{Z}$.

Agora, para alcançar nosso objetivo principal, mostrar que o conjunto dos elementos integrais sobre um anel é um anel, a seguinte proposição e seus corolários serão fundamentais, suas demonstrações serão omitidas mas podem ser encontras em [10].

Proposição 1.1.4. *([10], pág: 28) Sejam R um anel, A um subanel de R e $x_1, \ldots, x_n$ elementos de R tais que x_i é integral sobre $A[x_1, \cdots, x_{i-1}]$, $i = 1, ..., n$. Então $A[x_1, \cdots, x_n]$ é um A-módulo finitamente gerado.*

Corolário 1.1.5. *([10], pág: 29) Sejam R um anel, A um subanel de R, x e y elementos de R que são integrais sobre A. Então, $x + y$, $x - y$ e xy são integrais sobre A.*

Corolário 1.1.6. *([10], pág: 29) Sejam R um anel, A um subanel de R. Então, o conjunto A' dos elementos de R que são integrais sobre A é um subanel de R que contém A .*

Segue que, o conjunto A', dos elementos que são integrais sobre um anel é um anel. Agora, definiremos algumas terminologias.

Definição 1.1.7. *Sejam R um anel e A um subanel de R.*

(i) O anel A' dos elementos de R que são integrais sobre A é chamado fecho integral de A em R.

(ii) Sejam A um domínio e R seu corpo de frações. O fecho integral de A em R é chamado simplesmente de fecho integral de A.

(iii) Dizemos que um anel A é integralmente fechado quando A é um domínio e é seu próprio fecho integral, isto é, $A = A'$. Em outras palavras, um anel A é integralmente fechado se todo elemento do seu corpo de frações que é integral sobre A está em A.

(iv) Dizemos que R é integral sobre A se cada elemento de R é integral sobre A, isto é, se o fecho integral de A em R é o próprio R.

Exemplos.

1. *Sejam $R = \mathbb{Z}[\sqrt{5}]$ e $A = \mathbb{Z}$. Então, R é integral sobre A.*

É possível provar que $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5};\ a, b \in \mathbb{Z}\}$.

Observe que a, b são integrais sobre $\mathbb{Z}$ pois, satisfazem $X - a = 0$ e $X - b = 0$ respectivamente, além disso, $\sqrt{5}$ é raiz de $p(X) = X^2 - 5$ e portanto, $\sqrt{5}$ é integral sobre $\mathbb{Z}$. Como o conjunto dos elementos integrais sobre um anel é um anel, segue que $\mathbb{Z}[\sqrt{5}]$ é integral sobre $\mathbb{Z}$.

2. *Sejam $R = \mathbb{Z}\left[\frac{1}{2}\right]$ e $A = \mathbb{Z}$. Então, $A' = \mathbb{Z}$.*

Já mostramos que $\frac{1}{2}$ não é integral sobre $\mathbb{Z}$ portanto, $\left(\frac{1}{2}\right)^n$, com $n \in \mathbb{N}^*$, não pode ser integral sobre $\mathbb{Z}$. De fato, suponha por absurdo que $\left(\frac{1}{2}\right)^n$ é integral sobre $\mathbb{Z}$ então, como o conjunto dos elementos integrais sobre um anel é um anel e, 2^{n-1} é integral sobre $\mathbb{Z}$, segue que, $2^{n-1}\left(\frac{1}{2}\right)^n = \frac{1}{2}$ é integral sobre $\mathbb{Z}$, o que é um absurdo.

Portanto, os elementos de $\mathbb{Z}\left[\frac{1}{2}\right]$ que são integrais sobre $\mathbb{Z}$ são apenas os elementos que pertencem a $\mathbb{Z}$.

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

4. *Sejam $R = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ e $A = \mathbb{Z}$. Então, $A' = \mathbb{Z}[\sqrt{5}]$.*

De modo análogo ao Exemplo 1, podemos provar que

$$\mathbb{Z}\left[\tfrac{1+\sqrt{5}}{2}\right] = \left\{a + b\left(\tfrac{1}{2}\right) + c\left(\tfrac{\sqrt{5}}{2}\right) + d\sqrt{5};\ a, b, c, d \in \mathbb{Z}\right\}.$$

Pelo Exemplo 3, o anel dos inteiros é integralmente fechado, assim, a, b, c, d são integrais sobre $\mathbb{Z}$, além disso, $\sqrt{5}$ é integral sobre $\mathbb{Z}$ pois satisfaz a seguinte equação $X^2 - 5$. Porém, vimos que $\frac{1}{2}$ não é integral sobre $\mathbb{Z}$ e portanto, $\frac{\sqrt{5}}{2}$ também não é pois, do contrário, teríamos que $\left(\frac{\sqrt{5}}{2}\right)\sqrt{5} - 2 = \frac{1}{2}$ sería integral sobre $\mathbb{Z}$, o que é um absurdo. Portanto, o conjunto dos elementos de $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ que são integrais sobre $\mathbb{Z}$ são os da forma $a + b\sqrt{5}$, com $a, b \in \mathbb{Z}$, ou seja, $\mathbb{Z}[\sqrt{5}]$.

5. Sejam $R = \mathbb{Q}[\sqrt{5}]$ e $A = \mathbb{Q}$. Então, R é integral sobre A.

A demonstração deste é análoga a do Exemplo 1.

O próximo resultado garante a transitividade do conceito integral sobre um subanel:

Proposição 1.1.8 (Transitividade)**.** *([10], pág: 29) Sejam R um anel, B um subanel de R e A um subanel de B. Se R é integral sobre B e B é integral sobre A, então R é integral sobre A.*

Demonstração. Seja $x \in R$, como R é integral sobre B existem $b_0, \cdots, b_{n-1} \in B$ tais que

$$b_0 + b_1 x + ... + b_{n-1}x^{n-1} + x^n = 0$$

Denotando $C = A[b_0, ..., b_{n-1}]$, segue pela equação acima que x é integral sobre C. Usando a hipótese de que $b_0, \cdots, b_{n-1}$ são integrais sobre A temos que $b_0, \cdots, b_{n-1}, x$ são integrais sobre $C = A[b_0, ..., b_{n-1}]$, e portanto estamos nas hipótese da Proposição 1.1.4, que nos garante que $C[x]$ é um A-módulo finitamente gerado.

Portanto temos que, $A[x] \subset C[x] \subset R$ e pelo item (iii) do Teorema 1.1.3 segue que x é integral sobre A, como isto é válido para todo $x \in R$, segue que R é integral sobre A. □

Exemplo. *Sejam $R = \mathbb{Z}\left[\sqrt[4]{5}\right]$, $B = \mathbb{Z}\left[\sqrt{5}\right]$ e $A = \mathbb{Z}$. Temos que R é integral sobre B e B é integral sobre A assim, pelo Teorema anterior, segue que R é integral sobre A.*

De fato, podemos mostrar que $R = \mathbb{Z}\left[\sqrt[4]{5}\right] = \{a + b\sqrt[4]{5} + c\sqrt{5} + d\left(\sqrt[4]{5}\right)^3;\ a, b, c, d \in \mathbb{Z}\}$. Portanto, para que R seja integral sobre B é suficiente mostrar que $\sqrt[4]{5}$, $\sqrt{5}$, $\left(\sqrt[4]{5}\right)^3$ e a, tal que $a \in \mathbb{Z}$, sejam integrais sobre B.

$\sqrt[4]{5}$ é raiz de $X^2 - \sqrt{5} \in \mathbb{Z}[\sqrt{5}][X]$.

$\sqrt{5}$ é raiz de $X - \sqrt{5} \in \mathbb{Z}[\sqrt{5}][X]$.

$\left(\sqrt[4]{5}\right)^3$ é raiz de $X^2 - 5\sqrt{5} \in \mathbb{Z}[\sqrt{5}][X]$.

a; $a \in \mathbb{Z}$, é raiz de $X - a \in \mathbb{Z}[\sqrt{5}][X]$.

Donde, $R = \mathbb{Z}\left[\sqrt[4]{5}\right]$ é integral sobre $B = \mathbb{Z}[\sqrt{5}]$. Lembre-se, que mostramos anteriormente $B = \mathbb{Z}[\sqrt{5}]$ é integral sobre $A = \mathbb{Z}$. E portanto, pelo Teorema anterior, R é integral sobre A.

O próximo resultado assegura quando um anel de integridade, ou domínio, é também um corpo, usando seu anel de elementos integrais. Sua demonstração pode ser encontrada na referência citada:

Proposição 1.1.9. *([10], pág: 29) Sejam R um domínio e A um subanel de R tal que R é integral sobre A. Para que R seja um corpo é necessário e suficiente que A seja um corpo.*

Exemplos. *1. $\mathbb{Z}[\sqrt{5}]$ não é corpo pois, $\mathbb{Z}[\sqrt{5}]$ é integral sobre $\mathbb{Z}$ que não é corpo.*

2. $\mathbb{Q}[\sqrt{5}]$ é corpo pois, $\mathbb{Q}[\sqrt{5}]$ é integral sobre $\mathbb{Q}$ que é corpo.

1.2 Elementos Algébricos sobre um Corpo

Nesta seção, restringiremos o conceito de elemento integral sobre um anel, para corpos, neste caso, os denominamos, elementos algébricos sobre um corpo. Posteriormente, definiremos os corpos de números e exibiremos alguns resultados fundamentais, tais como, a Proposição Multiplicidade de Graus como o Teorema do Elemento Primitivo.

Definição 1.2.1. *Sejam $\mathbb{L}$ um corpo e $\mathbb{K}$ um subcorpo de $\mathbb{L}$.*

(i) Um elemento $x \in \mathbb{L}$ é chamado algébrico sobre $\mathbb{K}$ se existem: $a_0, \cdots, a_n \in \mathbb{K}$, não todos nulos, tais que $a_n x^n + \cdots + a_1 x + a_0 = 0$, $a_n \neq 0$. Em outras palavras, x é raiz de um polinômio não nulo, com coeficientes em $\mathbb{K}$.

(ii) Se todo elemento de $\mathbb{L}$ for algébrico sobre $\mathbb{K}$, dizemos que $\mathbb{L}$ é algébrico sobre $\mathbb{K}$.

(iii) Um elemento de $\mathbb{L}$ que não é algébrico sobre $\mathbb{K}$ é chamado transcendente sobre $\mathbb{K}$.

(iv) Um corpo $\mathbb{K}$ é chamado algebricamente fechado se, todo polinômino não constante, $p(X) \in \mathbb{K}[X]$ pode ser escrito como um produto de fatores lineares, todos pertencentes a $\mathbb{K}[X]$.

Exemplos. *1. π é transcendente sobre $\mathbb{Q}$.*

2. O conjunto dos números reais não é algebricamente fechado.

De fato, $p(X) = X^2 + 1 \in \mathbb{R}[X]$ no entanto, não pode ser escrito como produto de fatores lineares pertencentes a $\mathbb{R}[X]$.

3. $\mathbb{C}$ é um corpo algebricamente fechado.

Proposição 1.2.2. *([10], pág: 30) Sobre um corpo, o conceito de elemento algébrico coincide com o de elemento integral.*

Segue da Proposição acima que, os resultados vistos para elementos integrais valem para elementos algébricos sobre um corpo.

Exemplos. *1.* $\frac{1}{2}$ *é algébrico sobre* $\mathbb{R}$ *pois é raiz do polinômio* $p(X) = 2X - 1$. *Além disso,* $\frac{1}{2}$ *é integral sobre* $\mathbb{R}$ *pois é raiz do polinômio* $q(X) = X - \frac{1}{2}$.

2. Note que a hipótese de $\mathbb{K}$ *ser corpo é indispensável pois, para anel a proposição não é válida.*

De fato, do contrário teríamos que $\frac{1}{2}$ *é algébrico sobre* $\mathbb{Z}$ *pois é raiz de* $p(X) = 2X - 1$. *No entanto, sabemos que* $\frac{1}{2}$ *não é integral sobre* $\mathbb{Z}$. *Este é um caso particular do Exemplo 1.1.2 item 4.*

3. Sejam $\mathbb{H}$ *o anel dos quatérnios (formado por todos os números da forma* $q = a + bi + cj + dk$, *onde* $a, b, c, d \in \mathbb{R}$ *e* i, j, k *satisfazem as relações* $i^2 = j^2 = k^2 = -1$, $ij = k$ *e* $ji = -k$*) e* $\mathbb{R}$, *o conjunto dos números reais, subcorpo de* $\mathbb{H}$. *Temos que* $\mathbb{H}$ *é algébrico sobre* $\mathbb{R}$.

Com efeito, o corpo dos números reais é em particular um anel, além disso, todo número quatérnio é integral sobre $\mathbb{R}$. *Pois, basta tomar para* i, j, k *a equação de dependência integral* $X^2 + 1$ *daí, como o conjunto dos elementos integrais sobre um anel é um anel, segue que* $a + bi + cj + dk$ *é integral sobre* $\mathbb{R}$ *para todo* $a, b, c, d \in \mathbb{R}$, *donde* $\mathbb{H}$ *é integral sobre* $\mathbb{R}$. *Usando a Proposição anterior, segue que* $\mathbb{H}$ *é algébrico sobre* $\mathbb{R}$.

Vale ressaltar que, embora $\mathbb{H}$ *não seja corpo, isto não contradiz a Proposição (1.1.9) pois,* $\mathbb{H}$ *não é anel comutativo e portanto não pode ser domínio integral.*

Dados $\mathbb{K} \subset \mathbb{L}$ corpos e $\alpha \in \mathbb{L}$, denotamos por $\mathbb{K}[\alpha]$ o conjunto de todas as expressões polinomiais em α com coeficientes em $\mathbb{K}$.

Assim, aplicando o item (iii) do Teorema (1.1.3) para uma extensão $\mathbb{L}|\mathbb{K}$ temos que: $x \in \mathbb{L}$ e x é algébrico sobre $\mathbb{K}$ se, e somente se, $[\mathbb{K}[x] : \mathbb{K}]$ é finito.

Logo, se o grau de $\mathbb{L}$ sobre $\mathbb{K}$ é finito, então $\mathbb{L}$ é uma extensão algébrica de $\mathbb{K}$, isto é, todo elemento de $\mathbb{L}$ é algébrico sobre $\mathbb{K}$.

Definição 1.2.3. *Definimos um corpo de números como sendo uma extensão finita de* $\mathbb{Q}$, *isto é,* $\mathbb{K}$ *é um corpo de números se* $[\mathbb{K} : \mathbb{Q}]$ *é finito.*

Decorre da definição que todo elemento de $\mathbb{K}$ é algébrico sobre $\mathbb{Q}$.

O próximo resultado é a equivalência da Proposição da Transitividade, para extensões finitas, sua demonstração pode ser encontrada na seguinte referência:

Proposição 1.2.4. *(Multiplicidade de graus) ([10], pág: 31) Sejam* $\mathbb{K}$ *um corpo,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$, *e* $\mathbb{M}$ *uma extensão finita de* $\mathbb{L}$. *Então* $\mathbb{M}$ *é uma extensão finita de* $\mathbb{K}$. *Além disso,* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Na seção anterior, provamos que o conjuntos dos elementos integrais sobre um anel é um anel. A proposição seguinte é a correspondente para o conjunto dos elementos algébricos.

Proposição 1.2.5. *([10], pág: 31) Sejam $\mathbb{L}$ um corpo e $\mathbb{K}$ um subcorpo de $\mathbb{L}$. Então o conjunto $\mathbb{K}'$ dos elementos de $\mathbb{L}$ algébricos sobre $\mathbb{K}$ é um subcorpo de $\mathbb{L}$ contendo $\mathbb{K}$.*

A demonstração segue do Corolário 1.1.6 da Proposição 1.1.4, e da Proposição 1.1.9.

É importante ressaltar que a Proposição anterior é válida considerando subcorpos, não podemos considerar subaneis, primeiramente pois a definição de elemento algébrico considera um subcorpo. Além disso, escolhendo $\mathbb{L} = \mathbb{Q}$ e $\mathbb{K} = \mathbb{Z}$, teríamos que o conjunto dos elementos $\mathbb{Q}$ algébricos sobre $\mathbb{Z}$ seria um subcorpo, ou seja, $\mathbb{Z}$ seria um subcorpo de $\mathbb{Q}$, o que é um absurdo.

Definiremos na sequência polinômio minimal e irredutível, além de apresentarmos algumas características do primeiro. Posteriormente, apresentaremos um teorema relevante para a continuidade deste trabalho, o Teorema do Elemento Primitivo.

Definição 1.2.6. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$. O polinômio $p(X) \in \mathbb{K}[X] - \{0\}$, mônico de menor grau tal que $p(\alpha) = 0$ é chamado polinômio minimal de α. Notação: $p(X) = \min(\alpha, \mathbb{K})$.*

Definição 1.2.7. *Sejam $\mathbb{K}$ um corpo e $p(X) \in \mathbb{K}[X]$, de maneira que o $\partial(p) \geq 1$. Dizemos que $p(X)$ é irredutível sobre $\mathbb{K}$ se, $p(X) = f(X)g(X)$ implicar que $f(X) = a \in \mathbb{K}$ ou $g(X) = b \in \mathbb{K}$, onde $f(X), g(X) \in \mathbb{K}[X]$*

Observação. *O polinômio minimal $p(X) = \min(\alpha, \mathbb{K})$ é único, além disso, é irredutível sobre $\mathbb{K}$.*

Com efeito, suponhamos que o polinômio minimal não seja único, isto é, que existam $p(X)$ e $g(X)$ polinômios minimais distintos de α sobre $\mathbb{K}$, tais que $\partial(p) = \partial(g) = n$ com $n \geq 1$. Assim, $p(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ e $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + X^n$. Além disso, como estes polinômios são distintos, temos que $h(X) = p(X) - g(X) \neq 0$, $\partial(h) \leq n-1$ e $h(\alpha) = 0$, o que é um absurdo pela minimalidade do grau de $p(X)$.

Suponhamos agora que $p(X) = l(X)t(X)$, com $\partial(l) \geq 1$, $\partial(t) \geq 1$ e $\partial(p) = n$. Usando o fato de que $\mathbb{K}$ é corpo, temos que $\partial(p) = \partial(l) + \partial(t)$. No entanto, $p(\alpha) = 0$ e assim, $l(\alpha)t(\alpha) = 0$ ou seja, $l(\alpha) = 0$ ou $t(\alpha) = 0$ absurdo, pois, $1 \leq \partial(l) \leq n-1$ e $1 \leq \partial(t) \leq n-1$ o que contradiz a minimalidade de $\partial(p)$. Portanto, $p(X) = l(X)t(X)$ implica que $l(X) = c$ ou $t(X) = c$, isto é, $p(X)$ é irredutível.

Teorema 1.2.8 (Teorema do Elemento Primitivo)**.** *([11], pág: 40) Seja $\mathbb{K}$ um corpo de números. Então existe $u \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(u)$, além disso, u é chamado elemento primitivo.*

Demonstração. Seja $\mathbb{K}$ um corpo de números, então $\mathbb{K}$ é infinito e podemos supor $\mathbb{K} = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$.

Faremos a demonstração por indução sobre n. Se $n = 1$, temos $\mathbb{K} = \mathbb{Q}(\alpha_1)$ logo, basta escolhermos $u = \alpha_1$. Note que, é suficiente mostrar que $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(u)$ pois, esta afirmação associada a hipótese de indução sobre s, $s \leq n-1$ equivale:

$$\mathbb{K} = \mathbb{Q}(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) = \mathbb{Q}(\beta)(\alpha_n) = \mathbb{Q}(\beta, \alpha_n) = \mathbb{Q}(u).$$

Considere $\mathbb{K} = \mathbb{Q}(\alpha_1, \beta_1)$, e sejam $p(X)$ e $q(X)$ polinômios minimais de α_1 e β_1 respectivamente. Tomemos as fatorações de $p(X)$ e $q(X)$ em $\mathbb{C}$:

$$\begin{aligned} p(X) &= (X - \alpha_1) \cdots (X - \alpha_n) \\ q(X) &= (X - \beta_1) \cdots (X - \beta_m). \end{aligned}$$

Para cada $i = 1, \cdots, n$ e $j = 2, \cdots, m$, considere

$$x_{ij} = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}.$$

Podemos escolher $c \in \mathbb{Q}$, de forma que $c \neq x_{ij}$ para todo i e j, pois $\mathbb{Q}$ possui infinitos elementos. Escolha u, de forma que $u = \alpha_1 + c\beta_1$, mostraremos que $\mathbb{Q}(u) = \mathbb{Q}(\alpha_1, \beta_1)$. Observe que u é uma combinação linear de α_1 e β_1 com coeficientes em $\mathbb{Q}$, logo $\mathbb{Q}(u) \subseteq \mathbb{Q}(\alpha_1, \beta_1)$.

Para mostramos que α_1, β_1 estão em $\mathbb{Q}(u)$ é suficiente provar que $\beta_1 \in \mathbb{Q}(u)$, pois $\alpha_1 = u - c\beta_1$.

Seja $r(X) = p(u - cX) \in \mathbb{Q}(u)[X]$. Note que β_1 é raiz de $r(X)$, pois

$$r(\beta_1) = p(u - c\beta_1) = p(\alpha) = 0.$$

Entretanto, para que $r(X)$ e $q(X)$ tenham somente uma raíz em comum γ, é preciso que γ seja um dos $\beta_1, \cdots, \beta_m$ e $u - c\beta_1$ seja um dos $\alpha_1, \cdots, \alpha_n$. Mas, pela escolha de c, $\gamma = \beta_1$. Seja $h(X)$ o polinômio minimal de β_1 com coeficientes em $\mathbb{Q}(u)$. Então, $h(X)$ divide $q(X)$ e $r(X)$, pelo fato de $q(X)$ e $r(X)$ ter exatamente uma raiz comum em $\mathbb{C}$ e, todo polinômio irredutível em $\mathbb{C}$ não ter raízes repetidas, tem-se que o grau de h é um, isto é, $h(X) = X - \beta$, logo β pertence a $\mathbb{Q}(u)$.

Portanto, $\mathbb{Q}(\alpha_1, \beta_1) \subseteq \mathbb{Q}(u)$ e assim, $\mathbb{Q}(u) = \mathbb{Q}(\alpha_1, \beta_1)$.

□

1.3 Corpos Quadráticos

Nesta seção, estudaremos um caso particular dos corpos de números, os corpos quadráticos. Além de sua definição, verificaremos que todo corpo quadrático é um corpo obtido por adjunção de um elemento específico a $\mathbb{Q}$. Posteriormente, caracterizaremos como são os elementos integrais sobre esses corpos.

Definição 1.3.1. *Todo corpo de números de grau 2 sobre o corpo dos números racionais $\mathbb{Q}$, é denominado corpo quadrático.*

Se $\mathbb{K}$ é um corpo quadrático, $\mathbb{K}$ é um corpo de números, além disso, todo elemento $\alpha \in \mathbb{K} - \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$, assim, α é um elemento primitivo de $\mathbb{K}$, isto é, $\mathbb{K} = \mathbb{Q}(\alpha)$ e $\{1, \alpha\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$.

Suponha que $p(X) = X^2 + bX + c$, com $b, c \in \mathbb{Q}$, seja o polinômio minimal de α. Resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$ temos que, $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$. Logo, $\mathbb{K} = \mathbb{Q}(\sqrt{b^2 - 4c})$.

Notemos que $b^2 - 4c$ é um número racional, portanto podemos escrevê-lo como uma fração irredutível de números inteiros, $\frac{u}{v} = \frac{uv}{v^2}$ com $u, v \in \mathbb{Z}$. Donde, $\mathbb{K} = \mathbb{Q}(\sqrt{uv})$, com $u, v \in \mathbb{Z}$.

Consequentemente, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, ou seja, d é mais ou menos o produto de distintos primos. Assim, temos a seguinte proposição, cuja demonstração está concluída:

Proposição 1.3.2. *([10], pág: 34) Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*

Vale ressaltar que este elemento d é único. De fato, suponhamos que $\mathbb{K} = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{c})$, com d e c inteiros livre de quadrados, então, em particular temos que $\sqrt{d} \in \mathbb{Q}(\sqrt{c})$, isto é, $\sqrt{d} = a + b\sqrt{c}$, com $a, b \in \mathbb{Q}$. Portanto,

$$\begin{aligned}
\sqrt{d} &= a + b\sqrt{c} \\
a &= \sqrt{d} - b\sqrt{c} \\
a^2 &= d - 2b\sqrt{dc} + b^2c \\
2b\sqrt{dc} &= d + b^2c - a^2 \\
\sqrt{dc} &= \frac{d + b^2c - a^2}{2b} \\
dc &= \left(\frac{d + b^2c - a^2}{2b}\right)^2
\end{aligned}$$

Denote por $x = d + b^2c - a^2$ e $y = 2b$, logo, $x, y, \in \mathbb{Q}$. Seja $\frac{u}{v}$ a fração irredutível equivalente a $\frac{x}{y}$. Com isto, temos que:

$$dc = \left(\frac{u}{v}\right)^2$$

Note que, $d, c \in \mathbb{Z}$ e assim, $dc \in \mathbb{Z}$, consequentemente $v = 1$. Fatorando u em números primos temos que $u = (p_1 \cdots p_n)$ logo, $u^2 = (p_1 \cdots p_n)^2$, ou seja, os elementos primos que decompõe u^2 tem expoente no minimo 2. Por outro lado, fatorando dc em números primos obtemos $dc = (q_1 \cdots q_n)(q'_1 \cdots q'_m)$ podendo, eventualmente ter algum número primo se repentindo, tal repetição pode ocorrer apenas uma vez pois, ambos são inteiros livres de quadrado, e portanto, os primos que decompõe dc tem grau no máximo 2. De maneira que, os fatores primos que decompõe $dc = u^2$ possuem, sem exceção, expoente dois e portanto, $d = c$.

Nosso próximo objetivo, será caracterizar os elementos integrais sobre um corpo quadrático.

Seja $\mathbb{K}$ um corpo quadrático então, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ onde d é inteiro e livre de quadrados. Denote por $\mathcal{O}_\mathbb{K}$ o anel dos elementos de $\mathbb{K}$ que são integrais sobre $\mathbb{Z}$, nossa intenção é descrever $\mathcal{O}_\mathbb{K}$.

Note que $\sqrt{d}$ é raíz do polinômio irredutível $p(X) = X^2 - d$, ou seja, $\sqrt{d}$ é integral sobre $\mathbb{Z}$. Portanto, se $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, $\alpha \in \mathbb{Z}[\sqrt{d}]$, além disso, $\alpha \in \mathcal{O}_\mathbb{K}$. Donde, $\mathbb{Z}[\sqrt{d}]$ está contido em $\mathcal{O}_\mathbb{K}$.

Suponhamos agora que $\alpha = a + b\sqrt{d} \in \mathcal{O}_\mathbb{K}$.

Se $b = 0$, $\alpha = a$ é integral sobre $\mathbb{Z}$ por hipótese, dado que $\mathbb{Z}$ é integralmente fechado, segue que $\alpha \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{d}]$. Portanto, se $b = 0$, $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\sqrt{d}]$.

Se $b \neq 0$, α satisfaz a seguinte equação: $X^2 - 2aX + a^2 - db^2 = 0$ onde, $2a \in \mathbb{Z}$ e $a^2 - db^2 \in \mathbb{Z}$. Desta última, temos:

$$4(a^2 - db^2) = (2a)^2 - d(2b)^2 \in 4\mathbb{Z} \tag{1.1}$$

Em particular, da equação de dependência integral de α, obtemos que $(2a)^2 \in \mathbb{Z}$ e $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Consequentemente, $(2a)^2 - [(2a)^2 - d(2b)^2] = d(2b)^2 \in \mathbb{Z}$. Mais ainda, $2b \in \mathbb{Z}$, pois do contrário, poderíamos escrever $2b = \frac{x}{y}$, com $\frac{x}{y}$ irredutível. Assim, decompondo-os em fatores primos teríamos:

$$(q_1 \cdots q_r)\left(\frac{p_1 \cdots p_n}{p'_1 \cdots p'_n}\right)^2 \in \mathbb{Z}.$$

Todavia, os fatores primos de d são todos de grau 1 enquanto que, os fatores do denominador possuem grau 2, para que este produto seja inteiro obrigatóriamente devemos ter $y = 1$. Donde,

$2b \in \mathbb{Z}$.

Sejam $u = 2a$ e $v = 2b$ com isso, $a = \frac{u}{2}$ e $b = \frac{v}{2}$ donde, $\alpha = \frac{u+v\sqrt{d}}{2}$. Reescrevendo (1.1) em termos de u e v temos que, $u^2 - dv^2 \in 4\mathbb{Z}$. Em outras palavras, $u^2 - dv^2 \equiv 0 \mod 4$.

Atentemos para os seguintes fatos, se n é par, $n = 2t$, para algum $t \in \mathbb{Z}$, além disso $n^2 = 4t^2 \equiv 0 \mod 4$. Se n é ímpar, $n = 2t + 1$, para algum $t \in \mathbb{Z}$, além disso $n^2 = 4(t^2 + t) + 1 \equiv 1 \mod 4$.

Temos então os seguintes casos a considerar:

(i) u e v são pares. Temos que:

$u^2 \equiv 0 \mod 4$ e $v^2 \equiv 0 \mod 4$. Portanto, $u^2 - dv^2 = 0 - d0 \equiv 0 \mod 4$ para todo d.

(ii) u é par e v ímpar. Então,

$u^2 - dv^2 = 0 - d1 = -d \equiv 0 \mod 4$. Ou seja, $d \in 4\mathbb{Z}$, isto é, $d = 4n = 2^2n$ para algum $n \in \mathbb{Z}$, o que é um absurdo já que d é livre de quadrados.

(iii) u é ímpar e v par.

$u^2 - dv^2 = 1 - d0 = 1 \equiv 0 \mod 4$. Portanto, $1 \in 4\mathbb{Z}$, com isso, $1 = 4n$ para algum $n \in \mathbb{Z}$, o que é um absurdo.

(iv) u e v são ímpares.

$u^2 - dv^2 = 1 - d1 = 1 - d \equiv 0 \mod 4$. Isto ocorre se, e somente se, $d \equiv 1 \mod 4$.

Além disso, se $d \equiv 1 \mod 4$, usando a hipótese que $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$ temos que $2a, 2b \in 2\mathbb{Z}$ donde, $2a \equiv 2b \equiv 0 \mod 2$. Portanto, como $u = \frac{a}{2}$ e $v = \frac{b}{2}$ segue que u e v tem a mesma paridade. Logo, $u - v = 2w$ e com isso, $u = v + 2w$, donde

$$\alpha = \frac{u + v\sqrt{d}}{2} = \frac{1}{2}(u + v\sqrt{d}).$$

Consequentemente, se $d \not\equiv 1 \mod 4$, resta que $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$ (já que d é inteiro livre de quadrados e portanto, $d \not\equiv 0 \mod 4$) com isso, u e v são pares, logo $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

Com isto, demonstramos o seguinte resultado:

Teorema 1.3.3. *([10], pág:35) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados (portanto, $\not\equiv 0 \mod 4$).*

a) Se $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$, o anel $\mathcal{O}_{\mathbb{K}}$ dos integrais de $\mathbb{K}$ sobre $\mathbb{Z}$ consiste de todos os elementos da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$.

b) Se $d \equiv 1 \mod 4$, $\mathcal{O}_{\mathbb{K}}$ *é formado por todos os elementos da forma* $\frac{1}{2}(u + v\sqrt{d})$ *com* $u, v \in \mathbb{Z}$ *de mesma paridade.*

Observação 1.3.4. *Note que, no caso em que* $d \equiv 2 \mod 4$ *ou* $d \equiv 3 \mod 4$, $(1, \sqrt{d})$ *é uma base para* $\mathcal{O}_{\mathbb{K}}$ *como um* $\mathbb{Z}$*-módulo enquanto que, se* $d \equiv 1 \mod 4$, $\left(1, \frac{1}{2}(1 + \sqrt{d})\right)$ *é uma base para* $\mathcal{O}_{\mathbb{K}}$ *como um* $\mathbb{Z}$*-módulo. Além disso, se* $d > 0$, $\mathbb{Q}(\sqrt{d})$ *é chamado Corpo quadrático real, se* $d < 0$, $\mathbb{Q}(\sqrt{d})$ *é chamado Corpo quadrático imaginário.*

Exemplos. *1. Seja* $\mathbb{K} = \mathbb{Q}\left[\sqrt{6}\right]$*, visto que* $6 \equiv 2 \mod 4$ *então,* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\sqrt{6}\right]$.

2. Seja $\mathbb{K} = \mathbb{Q}\left[\sqrt{5}\right]$*, sendo que* $5 \equiv 1 \mod 4$ *logo,* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

1.4 Norma e Traço

Em álgebra linear, dado um corpo $\mathbb{K}$ e V um $\mathbb{K}$-espaço vetorial de dimensão finita n, à todo operador linear de V existe uma matriz quadrada $(n \times n)$ associada a este operador. De acordo com esta matriz, define-se o traço, a norma, o determinante e o polinômio característico do operador linear em questão.

Sejam A um anel, E um A-módulo livre de posto finito e σ um automorfismo de E, isto é, σ é um homomorfismo cujo domínio e contra-domínio são E. Se dada uma base (e_i) de E, $A = (a_{ij})$ for a matriz de σ em relação a esta base então, o traço, o determinante e o polinômio característico de A são, respectivamente,

$$Tr(\sigma) = \sum_{i=1}^{n} a_{ii}, \quad \det(\sigma) = \det(a_{ij}), \quad e \quad \det(X \cdot I_E - \sigma) = \det(X\delta_{ij} - a_{ij}).$$

Estes valores independem da base escolhida. Além disso, é consequência imediata que:

$$\begin{aligned} Tr(\sigma + \sigma') &= Tr(\sigma) + Tr(\sigma'), \\ \det(\sigma\sigma') &= \det(\sigma)\det(\sigma') \\ \det(X \cdot I_E - \sigma) &= X^n - (Tr(\sigma))X^{n-1} + \cdots + (-1)^n \det(\sigma). \end{aligned}$$

Neste momento, nosso intuito é definir traço, norma e polinômio característico para uma extensão de anéis, para isto, sejam B um anel e A um subanel de B, onde B é um A-módulo livre de posto n. Observe que, para todo $x \in B$, a multiplicação por x, m_x, que associa todo $y \in B$ a $m_x(y) = xy$, é um automorfismo do A-módulo B.

Note que, para $x, x' \in B$ e $a \in A$, tem-se:

- $(m_x + m_{x'})(y) = xy + x'y = (x + x')(y) = m_{x+x'}(y)$ para todo $y \in B$, e portanto, $m_x + m_{x'} = m_{x+x'}$;
- $m_x \circ m_{x'}(y) = m_x(x'y) = xx'y = m_{xx'}(y)$ para todo $y \in B$, e portanto, $m_x \circ m_{x'} = m_{xx'}$;
- $m_{ax}(y) = (ax)(y) = a(xy) = am_x(y)$ para todo $y \in B$, e portanto, $m_{ax} = am_x$.

Além disso, a matriz de m_a com respeito a qualquer base de B sobre A é a matriz diagonal, isto é, todos os elementos da diagonal são a e o restante são nulos.

Definição 1.4.1. *Definimos o traço (respectivamente, norma e polinômio característico) de $x \in B$, relativo a B e A, como sendo o traço (respectivamente, determinante e polinômio característico) do automorfismo m_x.*

Observação: O traço (respectivamente, norma) de x é denotado por $Tr_{B/A}(x)$ (respectivamente, $N_{B/A}(x)$) ou $Tr(x)$ (respectivamente, $N(x)$) quando não há duvidas entre os anéis envolvidos.

As propriedades do traço (e norma) de x são análogas as propriedades do traço (e norma) de um automorfismo. Mais precisamente, temos:

Proposição 1.4.2. *([10], pág: 36) Sejam B um anel e A um subanel de B, onde B é um A-módulo livre de posto n. Se x, x' pertencem a B e a pertence a A, então:*

(i) $Tr(x + x') = Tr(x) + Tr(x')$;

(ii) $Tr(ax) = aTr(x)$;

(iii) $Tr(a) = na$;

(iv) $N(xx') = N(x)N(x')$;

(v) $N(a) = a^n$;

(vi) $N(ax) = a^n N(x)$.

A seguinte proposição nos diz como determinar o traço e a norma de um elemento, conhecendo as raízes do seu polinômio minimal. Sua demonstração pode ser obtida na seguinte referência:

Proposição 1.4.3. *([10], pág: 36) Sejam $\mathbb{K}$ um corpo de característica zero (isto é, não existe n inteiro positivo tal que $n \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$) ou um corpo finito, $\mathbb{L}$ uma extensão algébrica de grau n de $\mathbb{K}$, x um elemento de $\mathbb{L}$ e $x_1, \cdots, x_n$ raízes do polinômio minimal de x sobre $\mathbb{K}$, onde cada um se repete $[\mathbb{L} : \mathbb{K}[x]]$ vezes. Então, $Tr_{\mathbb{L}/\mathbb{K}}(x) = x_1 + \cdots + x_n$, $N_{\mathbb{L}/\mathbb{K}}(x) = x_1 \cdots x_n$ e o polinômio característico de x, relativo a $\mathbb{L}$ e $\mathbb{K}$ é $(X - x_1) \cdots (X - x_n)$.*

Assim, o polinômio característico é a $[\mathbb{L} : \mathbb{K}[x]]$-ésima potência do polinômio minimal de x sobre $\mathbb{K}$.

Exemplo. *Sejam $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$, um corpo quadrático, onde d é um inteiro livre de quadrados e $\alpha = a + b\sqrt{d} \in \mathbb{K}$. Então, uma das duas coisas ocorre:*

a) Se $b = 0$ então, $\alpha = a \in \mathbb{Q}$ e portanto, $p(X) = X - a$ é o polinômio minimal de α. Assim, $Tr(\alpha) = a$ e $N(\alpha) = a$.

b) Se $b \neq 0$, o polinômio minimal de α é $q(X) = X^2 - 2aX + a^2 - db^2$ e suas raízes são $a + b\sqrt{d}$ e $a - b\sqrt{d}$. Assim, $Tr(\alpha) = 2a$ e $N(\alpha) = a^2 - db^2$.

Agora, nosso objetivo será relacionar os conceitos que definimos há pouco, com elemento integral sobre um anel, isto será feito por meio da seguinte proposição e seu corolário.

Proposição 1.4.4. *([10], pág: 38) Sejam A um domínio integral, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e x um elemento de $\mathbb{L}$ integral sobre A. Assumindo que $\mathbb{K}$ tem característica zero então, os coeficientes do polinômio característico $P(X)$ de x relativo a $\mathbb{L}$ e $\mathbb{K}$, são integrais sobre A. Em particular, $Tr_{\mathbb{L}/\mathbb{K}}(x)$ e $N_{\mathbb{L}/\mathbb{K}}(x)$ são integrais sobre A.*

Corolário 1.4.5. *([10], pág: 38) Seja A um anel integralmente fechado. Então, os coeficientes do polinômio característico de x, em particular $Tr_{\mathbb{L}/\mathbb{K}}(x)$ e $N_{\mathbb{L}/\mathbb{K}}(x)$, são elementos de A.*

Demonstração. Por definição os coeficientes do polinômio característico de x são elementos de $\mathbb{K}$. Pela Proposição (1.4.4) são integrais sobre A. Portanto, são elementos de A, pois A é integralmente fechado. □

Concluimos esta seção com a seguinte observação: Suponhamos $\alpha \in \mathbb{Q}[\sqrt{d}]$, onde d é inteiro livre de quadrados, tal que α é integral sobre $\mathbb{Z}$. Sabemos que $\mathbb{Z}$ é integramente fechado, portanto, pelo Corolário (1.4.5), $Tr(\alpha)$ e $N(\alpha)$ pertencem a $\mathbb{Z}$. Por outro lado, se $Tr(\alpha)$ e $N(\alpha)$ são números inteiros, tem-se que α é raíz do polinômio $p(X) = X^2 - Tr(\alpha) + N(\alpha)$ pois, mostramos que se $\alpha = a + b\sqrt{d}$ então, $Tr(\alpha) = 2a$ e $N(\alpha) = a^2 - db^2$. Donde, α é integral sobre $\mathbb{Z}$. Consequentemente, temos que um elemento de um corpo quadrático é integral sobre $\mathbb{Z}$ se, e somente se, seu traço e sua norma são números inteiros.

1.5 Discriminante

Nesta seção, definiremos o conceito discriminante, bem como, algumas de suas propriedades e sua relação com o conceito norma, definido na seção anterior.

Definição 1.5.1. *Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. Dados $(x_1, \cdots, x_n) \in B^n$ define-se seu discriminante por:*

$$D_{B/A}(x_1, \cdots, x_n) = \det(Tr_{B/A}(x_i x_j)).$$

Exemplo 1.5.2. *Seja $\mathbb{K}$ um corpo quadrático então, $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$ onde d é inteiro livre de quadrados. Considere $\{1, \sqrt{d}\}$ uma base de $\mathbb{Q}[\sqrt{d}]$ sobre $\mathbb{Q}$. Temos que $D(1, \sqrt{d}) = 4d$.*

De fato,

$$D(1, \sqrt{d}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr((\sqrt{d})^2) \end{vmatrix}$$

Vamos calcular $Tr(1)$, $Tr(\sqrt{d})$ e $Tr((\sqrt{d})^2)$.

Temos que: $m_1(1) = 1 = 1 \cdot 1 + 0 \cdot \sqrt{d}$ e $m_1(\sqrt{d}) = \sqrt{d} = 0 \cdot 1 + 1 \cdot \sqrt{d}$. Portanto, a matriz de m_1 é a seguinte:

$$m_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

E portanto, $Tr(m_1) = Tr(1) = 1 + 1 = 2$.

Analogamente,

$$m_{\sqrt{d}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad m_d = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}$$

Assim, $Tr(m_{\sqrt{d}}) = Tr(\sqrt{d}) = 0$ e $Tr(m_d) = Tr(d) = 2d$

Donde,

$$D(1, \sqrt{d}) = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

Proposição 1.5.3. *([10], pág: 38) Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. Se $(y_1, \cdots, y_n) \in B^n$ é um conjunto de elementos de B tais que $y_i = \sum_{j=1}^{n} a_{ij} x_j$ com $a_{ij} \in A$ e $x_j \in B$, então*

$$D(y_1, \cdots, y_n) = (\det(a_{ij}))^2 D(x_1, \cdots, x_n).$$

Observação. *Note que a Proposição anterior implica que o discriminante das bases de B sobre A são*

associadas, isto é, a matriz (a_{ij}) *que expressa uma base em termos da outra tem uma matriz inversa com entradas em A. Portanto, ambos* $\det(a_{ij})$ *e* $\det(a_{ij})^{-1}$ *são inversíveis em A. Com isto temos a seguinte definição:*

Definição 1.5.4. *Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. O discriminante de B sobre A, denotado por* $\mathcal{D}_{B/A}$*, é o ideal principal de A, gerado pelo discriminante de qualquer base de B sobre A.*

O próximo resultado caracteriza bases de B sobre A em termos do discriminante $\mathcal{D}_{B/A}$, considerando algumas hipóteses específicas.

Proposição 1.5.5. *([10], pág:39) Suponha que* $\mathcal{D}_{B/A}$ *contem um elemento que não é um divisor de zero (isto é, existe* $\alpha \in \mathcal{D}_{B/A}$ *tal que* $\alpha \cdot x = 0$ *se e somente se,* $x = 0$*). Então, para que o conjunto* $(x_1, \cdots, x_n) \subset B^n$ *seja uma base de B sobre A é necessário e suficiente que* $D(x_1, \cdots, x_n)$ *gere* $\mathcal{D}_{B/A}$*.*

O próximo resultado nos mostra como calcular o discriminante em casos mais gerais, quando ao invés de anéis temos corpos, a demonstração será omitida mas pode ser encontrada em [10].

Proposição 1.5.6. *([10], pág: 39) Sejam* $\mathbb{K}$ *um corpo finito ou de característica zero,* $\mathbb{L}$ *uma extensão finita de grau n sobre* $\mathbb{K}$ *e* $\sigma_1, \cdots, \sigma_n$ *os distintos* $\mathbb{K}$*-isomorfismos de* $\mathbb{L}$ *em um corpo algebricamente fechado* $\mathbb{M}$ *contendo* $\mathbb{K}$*. Então, se* $\{\alpha_1, \cdots \alpha_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$*,*

$$D(\alpha_1, \cdots \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0.$$

Com o objetivo de relacionar os conceitos Norma e Discriminante, apresentaremos o próximo resultado, cuja demonstração pode ser encontrada em [11].

Proposição 1.5.7. *([11], pág: 55) Sejam* $\mathbb{K} = \mathbb{Q}(\alpha)$ *um corpo de números e* $p(X)$ *o polinômio minimal de* α *sobre* $\mathbb{K}$*, onde* $p(X)$ *tem grau n. Então, a* $\mathbb{Q}$*-base* $\{1, \alpha, \cdots, \alpha^{n-1}\}$ *tem discriminante*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{K}/\mathbb{Q}}(p'(\alpha)),$$

onde $p'(X)$ *é a derivada de* $p(X)$*.*

1.6 Base Integral

Considere $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n, onde θ é integral sobre $\mathbb{Z}$, ou seja, θ é raiz de um polinômio mônico com coeficientes inteiros, considere também, $\mathcal{O}_{\mathbb{K}}$ o anel dos elementos de $\mathbb{K}$ que são integrais sobre $\mathbb{Z}$.

Temos que $\mathcal{O}_{\mathbb{K}}$ é um grupo abeliano sobre a adição. Além disso, uma $\mathbb{Z}$-base para $(\mathcal{O}_{\mathbb{K}}, +)$ é denominada base integral para $\mathbb{K}$.

Assim, $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral se, e somente se, todo α_i é integral sobre $\mathbb{Z}$, ou seja, $\alpha_i \in \mathcal{O}_{\mathbb{K}}$ para $i = 1, \cdots, n$ e, cada elemento de $\mathcal{O}_{\mathbb{K}}$ é unicamente determinado por

$$a_1\alpha_1 + \cdots + a_n\alpha_n$$

com $a_i \in \mathbb{Z}$, para $i = 1, \cdots, n$.

Observação. *Toda base integral de $\mathcal{O}_{\mathbb{K}}$ é uma $\mathbb{Q}$-base de $\mathbb{K}$ mas, nem toda $\mathbb{Q}$-base de $\mathbb{K}$ constituida de elementos integrais sobre $\mathbb{Z}$ é uma base integral de $\mathcal{O}_{\mathbb{K}}$.*

Exemplo. *O conjunto $\{1, \sqrt{5}\}$ é uma $\mathbb{Q}$-base de $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ no entanto, não pode ser uma base integral de $\mathbb{K}$ pois o elemento $\frac{1+\sqrt{5}}{2}$ é raiz de $X^2 - X - 1$ e portanto, é integral sobre $\mathbb{Z}$ mas, não pode ser escrito como combinação linear de 1 e $\sqrt{5}$ com coeficientes em $\mathbb{Z}$.*

Isto posto, nosso objetivo será mostrar que a base integral sempre existe.

Teorema 1.6.1. *([10], pág: 40) Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ com grau n, e A' o fecho integral de A em $\mathbb{L}$. Suponha que $\mathbb{K}$ é de caracteristica zero. Então, A' é um A-submódulo de um A-módulo livre de grau n.*

Corolário 1.6.2. *([10], pág: 40) Adicionando nas hipóteses do Teorema (1.6.1) que A é anel principal. Então, A' é um A-módulo livre de grau n.*

Note que para o caso particular, em que, $A = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\theta)$ e $A' = \mathcal{O}_{\mathbb{Q}(\theta)}$ a demonstração decorre do Teorema (1.1.3). Para consultar a demonstração do caso geral veja ([10]). Assim, $\mathcal{O}_{\mathbb{Q}(\theta)}$ é um $\mathbb{Z}$-módulo livre, consequentemente, sempre existe uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{Q}(\theta)}$, a qual denominamos anteriormente base integral.

Na Observação 1.3.4, formalizamos como são as bases de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático, como um $\mathbb{Z}$-módulo, ou seja, definimos as bases integrais de um corpo quadrático. Portanto, a referida Observação pode ser reescrita da seguinte forma: no caso em que $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$, $\{1, \sqrt{d}\}$ é uma base integral para $\mathbb{K}$ enquanto que, se $d \equiv 1 \mod 4$, $\{1, \frac{1}{2}(1 + \sqrt{d})\}$ é uma base integral para $\mathbb{K}$.

Portanto, considerando o exemplo anterior, temos que $\left\{1, \frac{1}{2}\left(1 + \sqrt{5}\right)\right\}$ constitui uma base integral para $\mathbb{Q}(\sqrt{5})$, e também, forma uma $\mathbb{Q}$-base .

Definição 1.6.3. *Dado um ideal não nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$, definimos a norma de $\mathcal{I}$ sendo o número $card(\mathcal{O}_{\mathbb{K}}/\mathcal{I})$.*

Observação 1.6.4. *Se $< \alpha >$ for um ideal principal de $\mathcal{O}_{\mathbb{K}}$ então, $N(< \alpha >) = |N(\alpha)|$. Para a demonstração veja ([10]), página 52.*

1.7 Corpo dos Números Complexos

Os números complexos surgiram da necessidade de encontrar raízes de equação do tipo $X^2 + 1 = 0$ pois, não existe número real que satisfaça tal equação. Assim, convencionou-se que o número imaginário i teria esta propriedade, ou seja, $i^2 = -1$. Construiu-se assim, um novo corpo, extensão do corpo dos números reais, pela adição do elemento i, o qual chamamos de corpo dos números complexos e denotamos por $\mathbb{C}$, em notação matemática, $\mathbb{C} = \mathbb{R}[i] = \{a + bi;\ a, b \in \mathbb{R}\}$.

Nesta seção faremos uma breve revisão de alguns conceitos do Corpo dos Números Complexos, tais como as representações de seus elementos, forma algébrica, polar e exponencial, assim como calcular potência e raízes naturais de números complexos.

Tradicionalmente, representamos um número complexo pela sua forma algébrica, isto é, $z \in \mathbb{C}$ então, $z = a + bi$ para algum $a, b \in \mathbb{R}$. No entanto, conhecer apenas esta representação, algumas vezes é insuficiente. Por exemplo, a radiciação de números complexos não é uma tarefa simples tratando-se deste tipo de representação todavia, na forma polar, esta operação é elementar como veremos mais adiante.

Dado um número complexo na sua forma algébrica, $z = a + bi$, o escrevemos na sua forma polar, dada por $z = \rho\cos(\theta) + i\rho\,\mathrm{sen}(\theta) = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$, onde $\rho = \sqrt{a^2 + b^2} = |z|$, $a = \rho\cos(\theta)$ e $b = \rho\,\mathrm{sen}(\theta)$. Observe que este número θ não é unico, pois, o substituindo por $\theta_1 = \theta + 2k\pi$ com $k \in \mathbb{Z}$ teremos o mesmo elemento z, sendo assim, deste momento em diante, sempre que falarmos em forma polar estaremos nos referindo a $\theta \in (-\pi, \pi]$. Relacionada com esta representação, temos a forma exponencial dada por $z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta)) = \rho e^{i\theta}$.

Nosso objetivo agora, será formalizar potência e raízes n-ésimas de números complexos. Para isto, será necessário o seguinte Teorema e seu Corolário.

Teorema 1.7.1. *(Fórmula de DeMoivre) Seja $n \in \mathbb{N}$, então*

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta) \text{ para todo } \theta \in \mathbb{R}.$$

Corolário 1.7.2. *Se $n < 0$, a Fórmula de DeMoivre é válida, isto é,*

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta) \text{ para todo } \theta \in \mathbb{R}.$$

Agora temos as ferramentas necessárias para definir uma potência de números complexos.

Definição 1.7.3. *Dado $n \in \mathbb{Z}$ e $z \in \mathbb{C}$, $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$, definimos a n-ésima potência de z como sendo o número $z^n = \rho^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta))$.*

Analogamente, dado $z \in \mathbb{C}$ e $n > 0$, definimos a raiz n-ésima de z como sendo o número complexo w, representado por $z^{\frac{1}{n}}$ ou $\sqrt[n]{z}$, que satisfaz $w^n = z$. Assim, pela definição de potência de números complexos, se $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$ então, $w = \sqrt[n]{\rho}\left(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta+2k\pi}{n}\right)\right)$ com $k = 0, 1, \cdots, n-1$. Os n números complexos assim obtidos, são denominados as n raízes distintas de z.

1.8 Teoria de Galois

Nesta seção, faremos uma breve síntese sobre a Teoria de Galois, tal teoria será de grande importância para o decorrer deste trabalho.

Dados $(\mathbb{L}, +, \cdot)$ e $(\mathbb{K}, \oplus, \odot)$ corpos, uma aplicação $f : \mathbb{L} \to \mathbb{K}$ é um *homomorfismo* se: $f(x+y) = f(x) \oplus f(y)$ e $f(x \cdot y) = f(x) \odot f(y)$ para todo $x, y \in \mathbb{L}$. Um homomorfismo bijetor, é denominado *isomorfismo* e, um isomorfismo cujo domínio e contra-domínio coincidem é denominado *automorfismo*. Além disso, o conjunto dos automorfismos sobre o corpo $\mathbb{L}$, $Aut(\mathbb{L}) = \{f : \mathbb{L} \to \mathbb{L};\ f \text{ é automorfismo}\}$, com a operação composição de aplicações é um grupo, isto é, $(Aut(\mathbb{L}), \circ)$ é um grupo.

Seja $\mathbb{L}|\mathbb{K}$ uma extensão de corpos. O grupo formado por todos os automorfismos que fixam $\mathbb{K}$ com a operação composição, $\{f \in Aut(\mathbb{L}); f|_{\mathbb{K}} = id\}$, é um subgrupo de $Aut(\mathbb{L})$. Com efeito, dados f e g pertencentes ao referido grupo, tem-se que $f|_{\mathbb{K}} = id$ e $g|_{\mathbb{K}} = id$, disso, $g^{-1}|_{\mathbb{K}} = id$, portanto, $f \circ g^{-1}|_{\mathbb{K}} = id$. Donde, prova-se a afirmação.

Definição 1.8.1. *O subgrupo $Gal(\mathbb{L}|\mathbb{K}) = \{\sigma \in Aut(\mathbb{L}); \sigma|_{\mathbb{K}} = id\}$ é denominado Grupo de Galois da extensão $\mathbb{L}|\mathbb{K}$.*

Observação 1.8.2. *É importante resaltar que, se $\alpha \in \mathbb{L}$ é raiz de um polinômio $p(X) \in \mathbb{K}[X]$ então, $\sigma(\alpha)$, $\sigma \in Gal(\mathbb{L}|\mathbb{K})$, é também uma raiz de $p(X)$. De fato, suponha que $p(X) = a_0 + a_1X + \cdots + a_nX^n$, como α é raiz de $p(X)$ tem-se que $p(\alpha) = 0$, isto é, $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, aplicando σ em ambos lados da igualdade, temos: $\sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha^n) = \sigma(0)$, usando que $\sigma|_{\mathbb{K}} = id$, e que $\sigma(\alpha^n) = \sigma(\alpha)^n$, pois σ é automorfismo, obtemos: $a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n = 0$. Donde, $p(\sigma(\alpha)) = 0$ e assim, $\sigma(\alpha)$ é raiz de $p(X)$.*

Definição 1.8.3. *Uma extensão finita $\mathbb{L}|\mathbb{K}$ é Galoiseana ou de Galois, se $\mathbb{L} = \mathbb{K}(R_p)$, para algum polinômio separável $p(X) \in \mathbb{K}[X]$. Onde, R_p é o conjunto de todas as raízes de p, além disso, um polinômio é dito separável se suas raízes são distintas.*

Se $\mathbb{L}|\mathbb{K}$ é uma extensão Galoisiana então a ordem do grupo de Galois da extensão (sua cardinalidade) coincide com o grau da extensão, isto é, $o(Gal(\mathbb{L}|\mathbb{K})) = [\mathbb{L} : \mathbb{K}]$.

Pelo feito anteriormente, a toda extensão de corpos $\mathbb{L}|\mathbb{K}$, associamos o grupo de Galois, $Gal(\mathbb{L}|\mathbb{K})$. Agora nosso objetivo será o recíproco, associar a cada subgrupo H de $Gal(\mathbb{L}|\mathbb{K})$, $H < Gal(\mathbb{L}|\mathbb{K})$, uma extensão de $\mathbb{K}$.

Para isto, considere $\mathbb{L}$ um corpo e $H < Aut(\mathbb{L})$ o conjunto $\mathbb{L}^H = \{\alpha \in \mathbb{L}; \sigma(\alpha) = \alpha, \forall \sigma \in H\}$ é um subcorpo de $\mathbb{L}$. Com efeito, tome $\alpha_1, \alpha_2 \in \mathbb{L}^H$ então, para todo $\sigma \in H$, $\sigma(\alpha_1 \pm \alpha_2) = \sigma(\alpha_1) \pm \sigma(\alpha_2) = \alpha_1 \pm \alpha_2$, onde a primeira igualdade ocorre pois σ é homomorfismo e, a segunda igualdade ocorre pois, α_1 e $\alpha_2 \in \mathbb{L}^H$. Donde, $\alpha_1 \pm \alpha_2 \in \mathbb{L}^H$. Analogamente, $\sigma(\alpha_1 \cdot \alpha_2) = \sigma(\alpha_1) \cdot \sigma(\alpha_2) = \alpha_1 \cdot \alpha_2$, e portanto, $\alpha_1 \cdot \alpha_2 \in \mathbb{L}^H$. Além disso, para todo $\alpha \in \mathbb{L}^H$, $\alpha \neq 0$, e para todo $\sigma \in H$ tem-se: $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$ e assim, $\alpha^{-1} \in \mathbb{L}^H$. Logo, $\mathbb{L}^H$ é subcorpo de $\mathbb{L}$.

Definição 1.8.4. *O subcorpo $\mathbb{L}^H = \{\alpha \in \mathbb{L}; \sigma(\alpha) = \alpha, \forall \sigma \in H\}$ de $\mathbb{L}$ é nomeado Corpo Fixo Associado a H.*

Agora, apresentaremos alguns resultados cujas demonstrações serão omitidas mas, podem ser encontradas em [6].

Lema 1.8.5. *([6], pág:18 - adaptado) Seja $\mathbb{L}$ um corpo.*

(i) Se $\mathbb{K}_1 \subseteq \mathbb{K}_2$ são subcorpos de $\mathbb{L}$, então, $Gal(\mathbb{L}|\mathbb{K}_2) \subseteq Gal(\mathbb{L}|\mathbb{K}_1)$.

(ii) Se $\mathbb{K}$ é um subcorpo de $\mathbb{L}$, então $\mathbb{K} \subseteq \mathbb{L}^{Gal(\mathbb{L}|\mathbb{K})}$.

(iii) Se $H_1 \subseteq H_2$ são subgrupos de $Aut(\mathbb{L})$, então $\mathbb{L}^{H_2} \subseteq \mathbb{L}^{H_1}$.

(iv) Se H é um subgrupo de $Aut(\mathbb{L})$, então $H \subseteq Gal(\mathbb{L}|\mathbb{L}^H)$.

(v) Se $\mathbb{K} = \mathbb{L}^H$ para algum $H \leq Aut(\mathbb{L})$, então $\mathbb{K} = \mathbb{L}^{Gal(\mathbb{L}|\mathbb{K})}$.

(vi) Se $H = Gal(\mathbb{L}|\mathbb{K})$ para algum subcorpo $\mathbb{K}$ de $\mathbb{L}$, então $H = Gal(\mathbb{L}|\mathbb{L}^H)$.

Proposição 1.8.6. *([6], pág: 21) Seja G um grupo finito de automorfismos de L. Então, $o(G) = [\mathbb{L} : \mathbb{L}^G]$ e assim, $G = Gal(\mathbb{L}|\mathbb{L}^G)$.*

O próximo resultado nos garante a reciprocidade que desejávamos.

Teorema 1.8.7. *(Teorema Fundamental da Teoria de Galois)([6], pág: 51) Sejam $\mathbb{L}|\mathbb{K}$ uma extensão finita de Galois e $G = Gal(\mathbb{L}|\mathbb{K})$. Então, existe uma correspondência (biúnica) entre os corpos intermediários entre $\mathbb{K}$ e $\mathbb{L}$ e os subgrupos de G, dadas por $\mathbb{M} \mapsto Gal(\mathbb{L}|\mathbb{M})$ e $H \mapsto \mathbb{L}^H$, onde $\mathbb{M}$ é um corpo intermediário entre $\mathbb{K}$ e $\mathbb{L}$, e H é subgrupo de G. Mais ainda, se $\mathbb{M} \leftrightarrow H$, então $[\mathbb{L} : \mathbb{M}] = o(H)$ e $[\mathbb{M} : \mathbb{K}] = (G : H)$. Além disso, H é subgrupo normal de G se, e somente se, a extensão $\mathbb{M}|\mathbb{K}$ é de Galois. Quando isto ocorre, temos $Gal(\mathbb{M}|\mathbb{K}) \simeq G/H$.*

Capítulo

2

Corpos Ciclotômicos e Reticulados

Considere a seguinte situação: Tem-se uma sala no formato de um paralelepípedo e, com cubos idênticos, deseja-se ocupar o maior volume possível da sala. Com cálculos elementares, conseguimos encontrar as dimensões de tais cubos, de maneira que a área preenchida seja 100%, pois os cubos se encaixam de tal modo, que não sobram espaços vagos entre eles. Agora, imaginemos o mesmo problema, porém, ao invés de cubos, queremos preencher a sala com esferas. Pergunta-se: é possível preencher completamente a sala? Sabemos que não. Então, qual o maior volume que esta sala pode ser preenchida por esferas idênticas?

Generalizando o último problema, desejamos cobrir a maior área do espaço $\mathbb{R}^3$ com esferas idênticas. Similarmente, podemos generalizar este problema para o $\mathbb{R}^n$. Este problema é conhecido como Problema Clássico do Empacotamento Esférico, com grandes questões em aberto até hoje.

Este capítulo, está dividido em duas grandes partes: Os corpos ciclotômicos e os reticulados pois, o capítulo posterior terá como objetivo principal aplicar os conceitos abordados dos reticulados à corpos ciclotômicos. Iniciaremos portanto, apresentando os corpos ciclotômicos e suas propriedades, além de determinar conceitos vistos no primeiro capítulo tais como: base integral e discriminante. Abordamos também o subcorpo real maximal de um corpo ciclotômico, apresentamos uma maneira de representá-lo bem como sua base integral.

Posteriormente, estudaremos os conceitos matemáticos descritos na situação problema anterior. Nosso interesse principal é obter o maior raio para as esferas, de modo a maximizar o espaço preenchido pelas mesmas. Neste trabalho, restringimos os conjuntos de centros aos reticulados. Apresentamos também, uma fórmula para calcular a proporção do espaço coberta pela união das esferas e, a solução deste problema para as dimensões 1 e 2. Em seguida, indicamos uma maneira de obtermos reticulados,

via homomorfismo de Minkowski, bem como, para casos especificos, a fórmula para calcular o volume do reticulado assim obtido. Além disso, se estivermos no caso em que o corpo é totalmente real ou, totalmente imaginário, o comprimento dos vetores da imagem pelo homomorfismo de Minkowski pode ser descrito usando a forma traço, essa descrição também pode ser encontrada neste capítulo. Por fim, calculamos os valores da função traço da raiz n-ésima da unidade.

2.1 Corpos Ciclotômicos

Nesta seção, estudaremos os corpos e os polinômios ciclotômicos, além de suas respectivas definições, mostraremos alguns exemplos e propriedades para uma melhor compreensão destes conceitos, que serão a essência da continuidade deste trabalho. Posteriormente, apresentaremos o subcorpo real maximal de um corpo ciclotômico, a respeito destes corpos, mostraremos o respectivo anel dos elementos integrais e apresentaremos uma base integral.

Consideremos $\mathbb{K}$ um corpo e $n \in \mathbb{N}^*$. Definimos como raiz n-ésima da unidade, todo elemento ζ de $\mathbb{K}$ tal que $\zeta^n = 1$. Consequentemente, ζ é raiz do polinômio $X^n - 1 \in \mathbb{K}[X]$.

Denote por U o conjunto de todas as raízes distintas de $X^n - 1$ em $\mathbb{K}$, em outras palavras, $U = \{\zeta \in \mathbb{K};\ \zeta^n = 1\}$. Temos que o conjunto U é um grupo multiplicativo, subgrupo de $(\mathbb{K}, \cdot)$.

Usando o fato de que todo grupo multiplicativo finito num corpo é cíclico, temos que U é cíclico. Sendo assim, podemos representar as n raízes n-ésimas da unidade por $\zeta, \zeta^2, \cdots, \zeta^n$, donde ζ é um gerador do grupo U.

Além disso, temos que se $|U| = n$ e $U = \langle\zeta\rangle$ então, ζ^k será outro gerador de U se, e somente se, k e n são primos entre sí, isto é, $mdc(k, n) = 1$. As raízes n-ésimas da unidade que possuem esta propriedade, de gerar U, são denominadas raízes n-ésimas primitivas da unidade. O número das raízes n-ésimas primitivas da unidade é obtido pela função de Euler, $\varphi : \mathbb{N}^* \to \mathbb{N}$ definida por, $\varphi(n) = |\{m \in \mathbb{N}; 1 \leq m \leq n \text{ e } mdc(m, n) = 1\}|$ no qual tem-se $n = \sum_{d|n} \varphi(d)$, onde d são os divisores de n. Ou, equivalentemente, podemos definir a função de Euler por: $\varphi(n) = (p_1 - 1)(p_2 - 1)\cdots(p_s - 1)p_1^{(a_1-1)}p_2^{(a_2-1)}\cdots p_s^{(a_s-1)}$, onde, $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$, com $p_1, p_2, \cdots, p_s$ números primos e $a_1, a_2, \cdots, a_s$ números naturais.

Dado n um número inteiro positivo, definimos ζ_n como sendo $e^{\frac{2\pi i}{n}}$, isto é, ζ_n é uma raiz primitiva n-ésima da unidade, e o corpo $\mathbb{Q}(\zeta_n)$ é chamado o n-ésimo corpo ciclotômico.

Definição 2.1.1. *O n-ésimo polinômio ciclotômico, é o polinômio mônico cujas raízes são as raízes primitivas da unidade, isto é,*

$$\Phi_n(X) = \prod_{\substack{i=1,\\ mdc(i,n)=1}}^{n} (X - \zeta_n^i).$$

É imediato da definição que $\partial(\Phi_n(X)) = \varphi(n)$. Além disso, o n-ésimo polinômio ciclotômico é irredutível sobre $\mathbb{Q}$. De fato, sabemos que existe um único polinômio minimal $p(X)$ tal que $p(\zeta_n) = 0$. Além disso, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, donde, $\partial(p(X)) = \partial(\Phi_n(X))$, temos também que $\Phi_n(\zeta_n) = 0$. Portanto, $p(X) = \Phi_n(X)$ e assim, $\Phi_n(X)$ é irredutível sobre $\mathbb{Q}$.

Agora, demonstraremos um lema que nos ajudará a construir exemplos de polinômios ciclotômicos.

Lema 2.1.2. *([5], pág: 100) Se n é um inteiro positivo, então*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Demonstração. Sejam $1 = d_1 < d_2 < \cdots < d_s = n$ todos os divisores de n. Então,

$$X^n - 1 = \prod_{\substack{i=0,\\ mdc(i,n)=d_1=1}}^{n-1} (X - \zeta_n^i) \cdot \prod_{\substack{i=0,\\ mdc(i,n)=d_2}}^{n-1} (X - \zeta_n^i) \cdots \prod_{\substack{i=0,\\ mdc(i,n)=d_s}}^{n-1} (X - \zeta_n^i),$$

onde,

$$\prod_{\substack{i=0,\\ mdc(i,n)=d_1=1}}^{n-1} (X - \zeta_n^i) = \Phi_{\frac{n}{d_1}}(X) = \Phi_n(X).$$

Note que, se $d = mdc(j, n)$ então $\zeta_n^j = \zeta_{n/d}^{j/d}$. Logo,

$$\prod_{\substack{i=0,\\ mdc(i,n)=d}}^{n-1} (X - \zeta_n^i) = \prod_{\substack{j=0,\\ mdc(j,t)=1}}^{t-1} \left(X - \zeta_{t/d}^{j/d}\right) = \prod_{\substack{j=0,\\ mdc(j,t)=1}}^{t-1} \left(X - \zeta_t^j\right) = \Phi_t(X),$$

com $t = \frac{n}{d}$ e $j = \frac{i}{d}$.

Repetindo o mesmo argumento em todos os fatores, obtemos:

$$X^n - 1 = \Phi_{\frac{n}{d_1}}(X)\Phi_{\frac{n}{d_2}}(X) \cdots \Phi_{\frac{n}{d_s}}(X),$$

uma vez que $\frac{n}{d_1}, \cdots, \frac{n}{d_s}$ são todos os divisores de n, segue o resultado.

□

O Lema demonstrado nos garante que

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X)\Phi_{\frac{n}{d2}}(X) \cdots \Phi_{\frac{n}{ds}}(X)$$

onde, $1, d_2, \cdots, d_s$ são todos os possíveis divisores de n. Logo,

$$\Phi_n(X) = \frac{X^n - 1}{\Phi_{\frac{n}{d2}}(X) \cdots \Phi_{\frac{n}{ds}}(X)}.$$

Portanto, uma consequência direta do Lema (2.1.2) é:

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{d|n;\ d<n} \Phi_d(X)}.$$

Desta forma,

$$\Phi_1(X) = X - 1;$$

$$\Phi_2(X) = \frac{X^2 - 1}{\Phi_1(X)} = \frac{X^2 - 1}{X - 1} = X + 1;$$

$$\Phi_3(X) = \frac{X^3 - 1}{\Phi_1(X)} = \frac{X^3 - 1}{X - 1} = X^2 + X + 1;$$

$$\Phi_4(X) = \frac{X^2 - 1}{\Phi_1(X)\Phi_2(X)} = \frac{X^4 - 1}{(X - 1)(X + 1)} = X^2 + 1.$$

E assim por diante. Quando n é primo, ou uma potência de primo, podemos generalizar o resultado.

Exemplos. *1. Seja $n = p$ primo então, $X^p - 1 = \Phi_1(X)\Phi_p(X)$, já que 1 e p são os únicos divisores de p, portanto,*

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = \frac{(X - 1)(X^{p-1} + X^{p-2} + \cdots + X + 1)}{(X - 1)} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

o qual é chamado p-ésimo polinômio ciclotômico.

2. Quando $n = p^r$, $r \in \mathbb{Z}$ tal que $r > 1$ e p é primo. Pelo Lema (2.1.2) tem-se

$$X^{p^r} - 1 = \Phi_1(X)\Phi_p(X)\Phi_{p^2}(X) \cdots \Phi_{p^{r-1}}(X)\Phi_{p^r}(X)$$

onde,

$$X^{p^{r-1}} - 1 = \Phi_1(X)\Phi_p(X)\Phi_{p^2}(X) \cdots \Phi_{p^{r-1}}(X).$$

Logo,

$$\Phi_{p^r}(X) = \frac{X^{p^r}-1}{\Phi_1(X)\Phi_p(X)\Phi_{p^2}(X)\cdots\Phi_{p^{r-1}}(X)} = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = X^{(p-1)p^{r-1}}+X^{(p-2)p^{r-1}}+\cdots+X^{p^{r-1}}+1.$$

Este polinômio é denominado p^r-ésimo polinômio ciclotômico.

Agora, nosso intuito será explicitar o anel dos elementos de $\mathbb{Q}(\zeta_p)$ que são integrais sobre $\mathbb{Z}$, onde p é um número primo qualquer.

Vimos que o p-ésimo polinômio ciclotômico é o polinômio $\Phi_p(X) = X^{p-1}+X^{p-2}+\cdots+X+1$. E portanto, $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}$ são as raízes de $\Phi_p(X)$.

Vimos também que o traço de x sobre $\mathbb{Q}$, $Tr(x) = Tr_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(x)$, pode ser obtido através da soma das raízes do polinômio minimal de x sobre $\mathbb{Q}$ ou, pelo traço da matriz do operador m_x. Portanto, temos:

$$Tr(\zeta_p) = -1 \text{ e } Tr(1) = p-1.$$

Além disso, $Tr(\zeta_p^j) = -1$ para $j = 1, \cdots, p-1$ e portanto,

$$Tr(1-\zeta_p^j) = Tr(1) - Tr(\zeta_p^j) = p-1-(-1) = p \text{ para } j = 1, \cdots, p-1.$$

Vimos também que a norma de x sobre $\mathbb{Q}$, $N(x) = N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(x)$, pode ser obtida através do produto das raízes do polinômio minimal de x sobre $\mathbb{Q}$. Logo,

$$N(1-\zeta_p^k) = (1-\zeta_p)\cdots(1-\zeta_p^k) = \Phi_p(1) = p \text{ para } k = 1, \cdots, p-1,$$

ou seja,

$$(1-\zeta_p)\cdots(1-\zeta_p^{p-1}) = \Phi_p(1) = p. \tag{2.1}$$

Denote por $\mathbb{A}$ o anel dos elementos de $\mathbb{Q}(\zeta_p)$ que são integrais sobre $\mathbb{Z}$. Queremos mostrar que $\mathbb{A}(1-\zeta_p)\cap\mathbb{Z} = p\mathbb{Z}$.

É claro que $\mathbb{A}$ contem ζ_p e suas potências. Portanto, por 2.1, temos que $p \in \mathbb{A}(1-\zeta_p)$. Consequentemente, $p\mathbb{Z} \in \mathbb{A}(1-\zeta_p)\cap\mathbb{Z}$. Para mostrar a outra inclusão, suponha por absurdo que $p\mathbb{Z}$ está contido propriamente em $\mathbb{A}(1-\zeta_p)\cap\mathbb{Z} \subset \mathbb{Z}$. Usando o fato de que $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$ temos que, $\mathbb{A}(1-\zeta_p)\cap\mathbb{Z} = \mathbb{Z}$. Além disso, como $1 \in \mathbb{Z}$, segue que $1 = (1-\zeta_p)a$, para algum $a \in \mathbb{A}$. Logo, $1-\zeta_p$ é inversível em $\mathbb{A}$, e assim $1-\zeta_p^j$ são inversíveis em $\mathbb{A}$ para $j = 2, \cdots p-1$. Donde, $(1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$ é inversível em $\mathbb{A}\cap\mathbb{Z}$, o que é um absurdo. Logo, $\mathbb{A}(1-\zeta_p)\cap\mathbb{Z} = p\mathbb{Z}$.

Agora, vamos mostrar que, para todo $y \in \mathbb{A}$, $Tr(y(1-\zeta_p)) \in p\mathbb{Z}$.

Cada conjugado $y_i(1-\zeta_p^i)$ de $y(1-\zeta_p)$ é um múltiplo de $1-\zeta_p^i$ em $\mathbb{A}$, para $i=1,\cdots,p-1$. Como $1-\zeta_p^i=(1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1})$ segue que $1-\zeta_p^i$ é um múltiplo de $1-\zeta_p$ em $\mathbb{A}$.

Sendo o traço a soma dos conjugados, segue que $Tr(y(1-\zeta_p))=y_1(1-\zeta_p)+\cdots+y_{p-1}(\zeta_p^{p-1})=$ $=\alpha(1-\zeta_p)$, com $\alpha\in\mathbb{A}$. Portanto, $Tr(y(1-\zeta_p))\in\mathbb{A}(1-\zeta_p)$. Além disso, sabemos que $\mathbb{Z}$ é integralmente fechado e, pelo Corolário (1.4.5) segue que $Tr(y(1-\zeta_p))\in\mathbb{Z}$. Assim, $Tr(y(1-\zeta_p))\in\mathbb{A}(1-\zeta_p)\cap\mathbb{Z}=p\mathbb{Z}$ a igualdade ocorre do que provamos anteriormente.

Agora temos as ferramentas necessárias para determinar o anel dos elementos de $\mathbb{Q}(\zeta_p)$ que são integrais sobre $\mathbb{Z}$.

Teorema 2.1.3. *([10], pág: 43) Seja p um número primo e ζ_p uma p-ésima raiz primitiva da unidade em $\mathbb{C}$. Então, o anel $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ dos elementos integrais de um corpo ciclotômico $\mathbb{Q}(\zeta_p)$ é $\mathbb{Z}[\zeta_p]$, além disso, $\left\{1,\zeta_p,\zeta_p^2,\cdots,\zeta_p^{p-2}\right\}$ é uma base do $\mathbb{Z}$-módulo $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, ou seja, o referido conjunto determina uma base integral de $\mathbb{Q}(\zeta_p)$.*

Demonstração. Seja $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ o anel dos elementos integrais de $\mathbb{Q}(\zeta_p)$. Uma vez que $\mathbb{Z}[\zeta_p]\subset\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, precisamos mostrar que $\mathcal{O}_{\mathbb{Q}(\zeta_p)}\subset\mathbb{Z}[\zeta_p]$.

Seja $\alpha\in\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, então $\alpha\in\mathbb{Q}(\zeta_p)$, e assim, podemos escrever

$$\alpha=a_0+a_1\zeta_p+\cdots+a_{p-2}\zeta_p^{p-2}, \tag{2.2}$$

com $a_1\in\mathbb{Q}$, para $i=0,1,\cdots,p-2$.

Multiplicando ambos membros da equação por $(1-\zeta_p)$ temos:

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

Aplicando o traço nesta equação, temos que:

$$Tr(\alpha(1-\zeta_p))=a_0Tr(1-\zeta_p)+\cdots+a_{p-2}Tr(\zeta_p^{p-2}-\zeta_p^{p-1}).$$

Usando que $Tr(\zeta_p^i-\zeta_p^{i+1})=0$ para $i=1,\cdots,p-2$, segue que $Tr(\alpha(1-\zeta_p))=a_0Tr(1-\zeta_p)$, e usando o que já provamos, $Tr(1-\zeta_p)=p$, temos $Tr(\alpha(1-\zeta_p))=a_0p$. Além disso, mostramos que $Tr(y(1-\zeta_p))\in p\mathbb{Z}$, consequentemente, $a_0p\in p\mathbb{Z}$, donde, $a_0\in\mathbb{Z}$.

Como $\zeta_p^{-1}=\zeta_p^{p-1}$, segue que $\zeta_p^{-1}\in\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ e portanto, pela equação (2.2) segue que:

$$(\alpha-a_0)\zeta_p^{-1}=a_1+a_2\zeta_p+\cdots+a_{p-2}\zeta_p^{p-3}\ \in\mathcal{O}_{\mathbb{Q}(\zeta_p)}.$$

Usando o mesmo argumento anterior, $a_1\in\mathbb{Z}$. Aplicando o mesmo argumento sucessivas vezes

tem-se que $a_i \in \mathbb{Z}$, $i = 0, \cdots, p-2$.

Portanto, $\mathcal{O}_{\mathbb{Q}(\zeta_p)} \subseteq \mathbb{Z} + \mathbb{Z}_{\zeta_p} + \cdots + \mathbb{Z}_{\zeta_p^{p-2}}$, ou seja, $\mathcal{O}_{\mathbb{Q}(\zeta_p)} \subseteq \mathbb{Z}[\zeta_p]$. Deste modo, concluimos que $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$.

Além disso, como $1, \zeta_p, \cdots, \zeta_p^{p-2}$ são linearmentes independentes sobre $\mathbb{Z}$, pois o são sobre $\mathbb{Q}$ e como $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z} + \mathbb{Z}_{\zeta_p} + \cdots + \mathbb{Z}_{\zeta_p^{p-2}}$, segue que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$.

□

O próximo Teorema é uma generalização trivial do teorema anterior, quando n é uma potência de um número primo. Para sua demonstração precisaremos dos resultados que seguem.

Primeiramente, vale ressaltar que o seguinte resultado, demonstrado para o caso em que p é um número primo, estende-se naturalmente para os p^r-ésimos corpos ciclotômicos, $\mathbb{Q}(\zeta_{p^r})$, ou seja, valem:

i) $(1 - \zeta_{p^r})\mathbb{A} \cap \mathbb{Z} = p\mathbb{Z}$;

ii) $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}((1 - \zeta_{p^r})y) \in p\mathbb{Z}, \quad \forall y \in \mathbb{A}$;

onde $\mathbb{A}$ é o anel dos elementos de $\mathbb{Q}(\zeta_{p^r})$ que são integrais sobre $\mathbb{Z}$.

Lema 2.1.4. *([4], pág:30) Sejam p um número primo e r um número natural. Então, $\mathbb{Z}[1 - \zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$ e $D_{\mathbb{Q}(\zeta_{p^r}/\mathbb{Q})}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\varphi(p^r)-1}) = D_{\mathbb{Q}(\zeta_{p^r}/\mathbb{Q})}(1, 1 - \zeta_{p^r}, \cdots, (1 - \zeta_{p^r})^{\varphi(p^r)-1})$, para todo $p^r \geq 3$.*

Demonstração. Para todo $\alpha \in \mathbb{Z}[1 - \zeta_{p^r}]$ temos:

$$\begin{aligned} \alpha &= a_0 + a_1(1 - \zeta_{p^r}) + a_2(1 - \zeta_{p^r})^2 + \cdots + a_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}} \\ &= (a_0 + a_1 + a_2 + \cdots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2)\zeta_{p^r} + \cdots \end{aligned}$$

Assim, $\alpha = b_0 + b_1\zeta_{p^r} + b_2\zeta_{p^r}^2 + \cdots + b_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$ e portanto, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$.

Por outro lado, se $\alpha \in \mathbb{Z}[\zeta_{p^r}]$, então, $\alpha = a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$, como $\zeta_{p^r} = 1 - (1 - \zeta_{p^r})$, podemos reescrever α da seguinte forma:

$$\begin{aligned} \alpha &= a_0 + a_1(1 - (1 - \zeta_{p^r})) + a_2(1 - (1 - \zeta_{p^r}))^2 + \cdots + a_{(p-1)p^{r-1}}(1 - (1 - \zeta_{p^r}))^{(p-1)p^{r-1}} \\ &= a_0 + a_1 - a_1(1 - \zeta_{p^r}) + a_2(1 - 2(1 - \zeta_{p^r}) + (1 - \zeta_{p^r})^2) + \cdots \\ &= (a_0 + a_1 + a_2 + \cdots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2 - \cdots - ((p-1)p^{r-1})a_{(p-1)p^{r-1}})(1 - \zeta_{p^r}) + \cdots, \end{aligned}$$

donde, $\alpha = b_0 + b_1(1 - \zeta_{p^r}) + b_2(1 - \zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}}$, e assim, $\alpha \in \mathbb{Z}[1 - \zeta_{p^r}]$. Consequentemente, vale a primeira igualdade.

Para mostrarmos a segunda igualdade, note que, como os conjugados de ζ_{p^r} são os elementos $\zeta_{p^r}^k$, com $k = 1, \cdots, p^r - 1$ e $mdc(k, p^r) = 1$, segue que os elementos $1 - \zeta_{p^r}^k$ são os conjugados de $1 - \zeta_{p^r}$. Além disso, como $\det(\sigma_j(\zeta_{p^r}^i))$ é o determinante de uma matriz de Vandermonde (isto é, os termos de cada linha estão em progressão geométrica), segue que:

$$\begin{aligned} D_{\mathbb{Q}(\zeta_{p^r}/\mathbb{Q})}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\varphi(p^r)-1}) &= \prod_{t<k}(\zeta_{p^r}^k - \zeta_{p^r}^t)^2 \\ &= \prod_{t<k}((1 - \zeta_{p^r}^k) - (1 - \zeta_{p^r}^t))^2 \\ &= D_{\mathbb{Q}(\zeta_{p^r}/\mathbb{Q})}(1, 1 - \zeta_{p^r}, \cdots, (1 - \zeta_{p^r})^{\varphi(p^r)-1}). \end{aligned}$$

□

Lema 2.1.5. *([4], pág:31) Sejam p um número primo e r um número natural. Então,*

$$\prod_k (1 - \zeta_{p^r}^k) = p,$$

com $1 \leq k \leq p^r$, tal que, $p \nmid k$.

Demonstração. Temos que $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$, portanto, todos os $\zeta_{p^r}^k$, com $1 \leq k \leq p^r$, tal que, $p \nmid k$ são raízes de $\Phi_{p^r}(X)$ uma vez que são raízes de $X^{p^r} - 1$ mas não são de $X^{p^{r-1}} - 1$. Deste modo, $\Phi_{p^r}(X) = \prod_k (X - \zeta_{p^r}^k)$ e existem exatamente $\varphi(p^r) = (p-1)p^{r-1}$ valores de k pois $\partial(\Phi_{p^r}(X)) = (p-1)p^{r-1}$. Tomando $X = 1$, obtemos que

$$\Phi_{p^r}(1) = \prod_{k=1,\ p\not| k}^{p^r} (1 - \zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + 1^{2p^{r-1}} + \cdots + 1^{(p-1)p^{r-1}} = p.$$

□

Lema 2.1.6. *([4], pág:29) Sejam $\mathbb{K}$ uma extensão finita de grau n sobre $\mathbb{Q}$, $\{\alpha_1, \cdots \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, onde $\alpha_i \in \mathcal{O}_\mathbb{K}$ e $D_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \cdots \alpha_n) = d$. Então, todo elemento de $\mathcal{O}_\mathbb{K}$ pode ser escrito na forma*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d},$$

onde $m_j \in \mathbb{Z}$ e m_j^2 é divisível por d, $j = 1, \cdots, n$.

Demonstração. Se $\alpha \in \mathcal{O}_\mathbb{K}$ então $\alpha \in \mathbb{K}$, uma vez que $\mathcal{O}_\mathbb{K} \subseteq \mathbb{K}$. Além disso, como $\{\alpha_1, \cdots \alpha_n\}$ é uma

base de $\mathbb{K}$ sobre $\mathbb{Q}$, existem $a_1, \cdots, a_n \in \mathbb{Q}$ tais que

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

Considere $\sigma_1, \cdots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Aplicando-os em α, obtemos um sistema de n equações dado por:

$$\sigma_i(\alpha) = a_1\sigma_i(\alpha_1) + a_2\sigma_i(\alpha_2) + \cdots + a_n\sigma_i(\alpha_n),$$

com $i = 1, \cdots, n$. Resolvendo esse sistema pela regra de Cramer, obtemos que as n raízes são dadas por $a_j = \frac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$. Além disso, temos que os γ_j, com $j = 1, \cdots, n$, e δ são inteiros algébricos, uma vez que, são obtidos a partir dos α_i's, que o são por hipótese.

Pela Proposição (1.5.6), temos que $\delta^2 = d$ e portanto, $da_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j$ é um inteiro algébrico. Usando que $\mathbb{Z}$ é integralmente fechado, segue que $da_j \in \mathbb{Z}$, $j = 1, \cdots, n$. Considere $m_j = da_j$, para $j = 1, \cdots, n$, se mostrarmos que $\frac{m_j^2}{d} \in \mathbb{Z}$, teremos que m_j^2 é divisível por d. No entanto, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, é suficiente mostrarmos que $\frac{m_j^2}{d}$ é um inteiro algébrico.

Temos que, $m_j = da_j = \delta\gamma_j$ portanto, $m_j^2 = d^2a_j^2 = \delta^2\gamma_j^2 = d\gamma_j^2$. Logo, $\frac{m_j^2}{d} = \gamma_j^2$ é um inteiro algébrico pois γ_j o é. Donde, $\frac{m_j^2}{d} \in \mathbb{Z}$ e assim, m_j^2 é divisível por d. Segue que,

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d},$$

com $m_j \in \mathbb{Z}$ e m_j^2 é divisível por d, $j = 1, \cdots, n$. □

Lema 2.1.7. *([4], pág:31) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um número natural não nulo. Se $D_{\mathbb{Q}(\zeta_{p^r}/\mathbb{Q})}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$ então, $d = p^s$ para algum $s \in \mathbb{N}$.*

Demonstração. O p^r-ésimo polinômio ciclotômico é dado por:

$$\Phi_{p^r}(X) = \frac{X^{p^r-1}}{X^{p^{r-1}} - 1},$$

portanto,

$$X^{p^r} - 1 = \Phi_{p^r}(X)g(X), \tag{2.3}$$

onde $g(X) = X^{p^r-1}$.

Derivando ambos os lados da Equação 2.3, temos:

$$p^r X^{p^r-1} = \Phi'_{p^r}(X)g(X) + \Phi_{p^r}(X)g'(X),$$

substituindo X por ζ_{p^r}, obtemos:

$$\begin{aligned} p^r \zeta_{p^r}^{p^r-1} &= \Phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}) + \Phi_{p^r}(\zeta_{p^r})g'(\zeta_{p^r}) \\ &= \Phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}), \end{aligned}$$

uma vez que, $\Phi_{p^r}(\zeta_{p^r}) = 0$.

Mais ainda, temos que $p^r = \zeta_{p^r}\Phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r})$, já que $\zeta_{p^r}^{p^r-1} = \zeta_{p^r}^{p^r}\zeta_{p^r}^{-1} = 1\zeta_{p^r}^{-1}$.

Agora, aplicando a norma temos:

$$p^{r(p-1)p^{r-1}} = N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\Phi'_{p^r}(\zeta_{p^r}))N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})),$$

Donde, pelo Teorema 1.5.7

$$p^{r(p-1)p^{r-1}} = \pm D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \cdots, \zeta_{p^r}^{(p-1)p^{r-1}-1})N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})),$$

Portanto, $d|p^{r(p-1)p^{r-1}}$, ou seja, $d = p^s$, $s \in \mathbb{N}$. □

Teorema 2.1.8. *([4], pág:30) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um número natural não nulo. Então, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ e $\left\{1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\right\}$ é uma base de $\mathbb{Z}[\zeta_{p^r}]$ como um $\mathbb{Z}$-módulo.*

Demonstração. Mostraremos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1 - \zeta_{p^r}]$.

Suponhamos, por absurdo, que $\mathcal{O}_{\mathbb{K}} \neq \mathbb{Z}[1 - \zeta_{p^r}]$ e, consideremos $\alpha \in \mathcal{O}_{\mathbb{K}}$, então, pelo Lema 2.1.6 podemos escrever α da seguinte maneira:

$$\alpha = \frac{m_1 + m_2(1 - \zeta_{p^r}) + \cdots + m_n(1 - \zeta_{p^r})^{n-1}}{d},$$

onde, $n = \varphi(p^r)$ e $m_i \in \mathbb{Z}$ para $i = 1, \cdots, n$.

Pelo Lema 2.1.7 temos que $d = p^s$ para algum $s \in \mathbb{N}$. Logo, existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ de modo que nem todos os m_j's são divisíveis por p^s.

Considere $i \leq n$ de modo que, m_i não seja divisível por p^s. Assim, temos que $m_i = p^s q + r$, com $q, r \in Z$ e $0 < r < p^s$. Com isto, podemos reescrever α da seguinte forma:

$$\alpha = \frac{m_1 + m_2(1 - \zeta_{p^r}) + \cdots + (p^s q + r)(1 - \zeta_{p^r})^{i-1} + \cdots + m_n(1 - \zeta_{p^r})^{n-1}}{p^s}.$$

Desse modo, $\mathcal{O}_{\mathbb{K}}$ contém um elemento da forma:

$$\gamma = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^i + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p^s},$$

multiplicando ambos os lados por p^{s-1}, obtemos que

$$\gamma p^{s-1} = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^i + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p},$$

o qual, podemos reescrever como:

$$\beta = \frac{a_i(1-\zeta_{p^r})^{i-1} + a_{i+1}(1-\zeta_{p^r})^i + \cdots + a_n(1-\zeta_{p^r})^{n-1}}{p}$$

com $a_j \in \mathbb{Z}$ e a_i não divisível por p.

Pelo Lema 2.1.5, temos que $\frac{p}{(1-\zeta_{p^r})^n} \in \mathbb{Z}[\zeta_{p^r}]$ pois, $(1-\zeta_{p^r})^k$ é divisível, em $\mathbb{Z}[\zeta_{p^r}]$, por $(1-\zeta_{p^r})$. Assim, $\frac{p}{(1-\zeta_{p^r})^i} \in \mathbb{Z}[\zeta_{p^r}]$ e portanto, temos que $\frac{\beta p}{(1-\zeta_{p^r})^i} \in \mathcal{O}_{\mathbb{K}}$. Subtraindo termos que estão em $\mathcal{O}_{\mathbb{K}}$, obtemos $\frac{a_i}{(1-\zeta_{p^r})} \in \mathcal{O}_{\mathbb{K}}$. Disto, segue que $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) | N_{\mathbb{K}/\mathbb{Q}}(a_i)$. Como $N_{\mathbb{K}/\mathbb{Q}}(a_i) = a_i^n$ e, pelo Lema 2.1.5 temos que $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = p$, segue que, $p | a_i^n$, o que é um absurdo pois, a_i não é divisível por p.

Donde, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$, a última igualdade segue pelo Lema 2.1.4.

□

O próximo resultado nos diz quem é o discriminante de $\mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um inteiro maior que 1. A demonstração será omitida mas, pode ser encontrada na referida referência.

Teorema 2.1.9. *([12], pág: 9): O discriminante de $\mathbb{Q}(\zeta_{p^r})$ é:*

$$\begin{cases} -p^{p^{r-1}(pr-r-1)}, & \text{se } p^n = 4 \text{ ou se } p \equiv 3(mod 4) \\ p^{p^{r-1}(pr-r-1)}, & \text{caso contrário.} \end{cases}$$

O próximo Teorema é a generalização dos resultados anteriores, quando n não é necessariamente primo, para sua demonstração será necessário o seguinte Lema, sua demonstração será omitida mas pode ser encontrada em [3].

Lema 2.1.10. *([3], pág: 68) Sejam $\mathbb{K}$ e $\mathbb{L}$ dois corpos de números. Assuma que seus discriminantes são relativamente primos e que os corpos são linearmente disjuntos, isto é, se $\{w_1, \cdots, w_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ e $\{v_1, \cdots, v_m\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, então $\{w_i v_j\}$ é uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$.*

Então,

$$\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} \quad e \quad D_{\mathbb{KL}} = D_{\mathbb{K}}^{m} D_{\mathbb{L}}^{n}.$$

Teorema 2.1.11. *([12], pág: 11)* $\mathbb{Z}[\zeta_n]$ *é o anel dos inteiros algébricos de* $\mathbb{Q}(\zeta_n)$

Demonstração. Inicialmente, observamos que, se n_1 e n_2 são primos entre sí então $\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}(\zeta_{n_1 n_2})$ uma vez que, $[\mathbb{Q}(\zeta_{n_1 n_2}) : \mathbb{Q}] = \varphi(n_1 n_2)$ e pela definição da função de Euler, usando que n_1 e n_2 são primos entre sí temos, $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$, donde, $[\mathbb{Q}(\zeta_{n_1 n_2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}]$ e, portanto, $\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}(\zeta_{n_1 n_2})$.

Consideremos $\mathbb{Q}(\zeta_n)$, onde n é um número qualquer. Decompondo n em potências de números primos, digamos, $n = a_1 \cdots a_s$, onde $a_i = p_i^{r_i}$, com p_i primo e r_i natural. Provaremos o resultado por indução sobre s.

Se $s = 1$ então $n = a_1 = p_1^{r_1}$ e, portanto, o resultado segue pelo Teorema 2.1.8.

Suponhamos válido para s, isto é, se $n = a_1 \cdots a_s$ então, $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

Provaremos para $s+1$, seja $m = a_1 \cdots a_s a_{s+1}$ então, pela observação inicial, temos que $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_{a_{s+1}})$, agora, usando o Lema 2.1.10, temos que $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathcal{O}_{\mathbb{Q}(\zeta_n)}\mathcal{O}_{\mathbb{Q}(\zeta_{a_{s+1}})}$ e portanto, $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_n]\mathbb{Z}[\zeta_{a_{s+1}}] = \mathbb{Z}[\zeta_m]$. Donde concluimos a demonstração. □

Observação 2.1.12. *Como consequência do teorema anterior, temos que a base integral de* $\mathbb{Q}(\zeta_n)$ *é o conjunto* $\mathcal{B} = \{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{\varphi(n)-1}\}$.

Nosso próximo objetivo será calcular o discriminante de corpos ciclotômicos.

Teorema 2.1.13. *([12], pág: 11) O discriminante de* $\mathbb{Q}(\zeta_n)$ *sobre* $\mathbb{Q}$ *é dado por:*

$$D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Demonstração. Pelo Lema 2.1.10, temos que, dados dois corpos de números linearmentes disjuntos, $\mathbb{K}$ e $\mathbb{L}$, tais que, seus discriminantes são relativamente primos, então:

$$D(\mathbb{KL}) = D(\mathbb{K})^{[\mathbb{L}:\mathbb{Q}]} \cdot D(\mathbb{L})^{\mathbb{K}:\mathbb{Q}}$$

Aplicando a função logaritmo em ambos os lados da igualdade acima, temos:

$$log|D(\mathbb{KL})| = \log\left(|D(\mathbb{K})|^{[\mathbb{L}:\mathbb{Q}]} \cdot |D(\mathbb{L})|^{[\mathbb{K}:\mathbb{Q}]}\right) = [\mathbb{L}:\mathbb{Q}]\log|D(\mathbb{K})| + [\mathbb{K}:\mathbb{Q}]\log|D(\mathbb{L})|,$$

dividindo ambos os lados da igualdade por $[\mathbb{KL}:\mathbb{Q}]$, obtemos:

$$\frac{log|D(\mathbb{KL})|}{[\mathbb{KL}:\mathbb{Q}]} = \frac{\log|D(\mathbb{K})|}{[\mathbb{K}:\mathbb{Q}]} + \frac{\log|D(\mathbb{L})|}{[\mathbb{L}:\mathbb{Q}]}$$

Agora, decompondo n em fatores primos, digamos, $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$, temos que $\mathbb{Q}(\zeta_{p_i^{a_i}})$ e $\mathbb{Q}(\zeta_{p_j^{a_j}})$ estão nas condições do Lema 2.1.10, para $i, j = 1, \cdots, s$ com $i \neq j$, e portanto vale a última igualdade. Portanto,

$$\begin{aligned}
\frac{\log|D(\mathbb{Q}(\zeta_n))|}{\varphi(n)} &= \frac{\log|D(\mathbb{Q}(\zeta_{p_1^{a_1}}))|}{\varphi(p_1^{a_1})} + \cdots + \frac{\log|D(\mathbb{Q}(\zeta_{p_s^{a_s}}))|}{\varphi(p_s^{a_s})} \\
&= \sum_{i=1}^{s} \frac{(\log p_i^{p_i^{a_i-1}(p_ia_i-a_i-1)})}{p_i^{a_i-1}(p_i-1)} \\
&= \sum_{i=1}^{s} \frac{p_i^{a_i-1}(p_ia_i-a_i-1)(\log p_i)}{p_i^{a_i-1}(p_i-1)} \\
&= \sum_{i=1}^{s} \frac{(p_ia_i-a_i-1)(\log p_i)}{(p_i-1)} = \sum_{i=1}^{s} \frac{(a_i(p_i-1)-1)(\log p_i)}{(p_i-1)} \\
&= \sum_{i=1}^{s} \left(a_i - \frac{1}{(p_i-1)}\right)(\log p_i) = \sum_{i=1}^{s} a_i \log p_i - \sum_{i=1}^{s} \frac{\log p_i}{(p_i-1)} \\
&= \sum_{i=1}^{s} \log p_i^{a_i} - \sum_{i=1}^{s} \log p_i^{\frac{1}{p_i-1}} = \log\prod_{i=1}^{s} p_i^{a_i} - \log\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}} \\
&= \log(n) - \log\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}.
\end{aligned}$$

Donde,

$$\log|D(\mathbb{Q}(\zeta_n))| = \varphi(n)\left(\log(n) - \log\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}\right) = \log\left(\frac{n}{\prod_{i=1}^{s} p_i^{p_i-1}}\right)^{\varphi(n)}$$

portanto,

$$|D(\mathbb{Q}(\zeta_n))| = \left(\frac{n}{\prod_{i=1}^{s} p_i^{p_i-1}}\right)^{\varphi(n)}$$

Com isto, temos:

$$D(\mathbb{Q}(\zeta_n)) = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

□

2.1.1 Subcorpos Reais Maximais de Corpos Ciclotômicos

Seja $\mathbb{Q}(\zeta_n)$, denotamos por $\mathbb{Q}(\zeta_n)^+ = \{x \in \mathbb{Q}(\zeta_n);\ x = \overline{x}\} = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ o subcorpo real maximal de $\mathbb{Q}(\zeta_n)$, isto é, $\mathbb{Q}(\zeta_n)^+$ é o maior subcorpo de $\mathbb{Q}(\zeta_n)$ que está contido nos reais.

Da Teoria de Galois, temos a seguinte associação:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & \text{———} & \{\sigma_1\} \\ | & & | \\ \mathbb{Q}(\zeta_n)^+ & \text{——} & H = \{\sigma_1, \sigma_{n-1}\} \\ | & & | \\ \mathbb{Q} & \text{———} & G \end{array}$$

Onde, σ_1, σ_{n-1} representam a identidade e a conjugação complexa respectivamente, isto pois, estes dois isomorfismos fixam qualquer subcorpo real. Além disso, temos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ e como $o(H) = 2$, pelo Teorema fundamental da teoria de Galois, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2$, donde, Pelo Teorema da multiplicidade de graus, $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \frac{\varphi(n)}{2}$.

Queremos nesta seção, explorar o corpo $\mathbb{Q}(\zeta_n)^+$, para isto, nosso primeiro objetivo será reescrevê-lo de uma maneira mais familiar.

Primeiramente, note que $\zeta_n^{n-1} = \zeta_n^{-1}$, já que $n-1$ e -1 estão na mesma classe de equivalência módulo n, além disso, ζ_n^{-1} é o conjugado de ζ_n. De fato,

$$\zeta_n^{-1} = \left[cos\frac{2\pi}{n} + isen\frac{2\pi}{n}\right]^{-1} = cos - \frac{2\pi}{n} + isen - \frac{2\pi}{n} = cos\frac{2\pi}{n} - isen\frac{2\pi}{n} = \overline{\zeta_n}.$$

Observemos que $\alpha = \zeta_n + \zeta_n^{-1}$ pertence a $\mathbb{Q}(\zeta_n)^+$, uma vez que $\sigma_1(\alpha) = \alpha$ e $\sigma_{n-1}(\alpha) = \left(\zeta_n + \zeta_n^{-1}\right)^{-1} = \zeta_n^{-1} + \zeta_n = \alpha$, onde w^{-1} representa o conjugado complexo de w, portanto, α é fixado por H, donde, $\alpha \in \mathbb{Q}(\zeta_n)^+$

Por outro lado, ζ_n é raiz do polinômio irredutível $p(X) = X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X]$, além disso, $p(X)$ é o polinômio minimal de ζ_n sobre $\mathbb{Q}(\alpha)$, pois do contrário, seu polinômio minimal $q(X)$ teria grau 1, isto é, $\zeta_n \in \mathbb{Q}(\alpha)$, o que é um absurdo pois ζ_n é um número complexo e $\mathbb{Q}(\alpha)$ é totalmente real, donde, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$. Assim, temos $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_n)^+$ e ambos com o mesmo grau sobre $\mathbb{Q}$ consequentemente, $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

O seguinte resultado determina uma base integral para $\mathbb{Q}(\zeta_n)^+$, válido para qualquer $n \in \mathbb{N}$.

Proposição 2.1.14. *([12], pág: 16) Seja $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ então, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}(\zeta_n + \zeta_n^{-1})$.*

Sendo assim, uma base integral para $\mathbb{Q}(\zeta_n)^+$ é dada por $\{1, (\zeta_n + \zeta_n^{-1}), (\zeta_n + \zeta_n^{-1})^2, \cdots, (\zeta_n + \zeta_n^{-1})^{\varphi(n)/2\ -1}\}$.

2.2 Reticulados no $\mathbb{R}^n$

O objetivo desta seção é formalizar os conceitos matemáticos envolvidos no problema de empacotamento esférico. Iniciamos estudando o conjunto dos centros das esferas em questão, exemplificamos casos em que são possiveis, e casos que não são possiveis, obter um empacotamento esférico. Destes que são possíveis, focamos nos denominados reticulados, apresentamos sua definição formal e algumas propriedades. Por fim, definimos densidade de empacotamento, abreviamos o problema inicial e mostramos a solução para esse problema em dimensões 1 e 2.

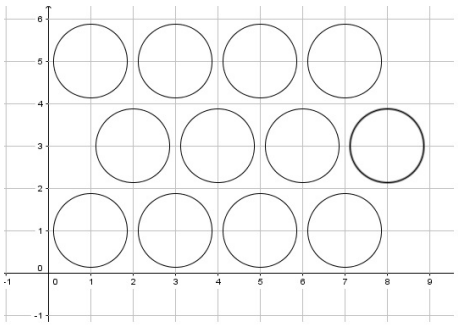
Definição 2.2.1. *Sejam $r > 0$ e $x_0 \in \mathbb{R}^n$. A esfera n-dimensional de raio r e centro em x_0 é denotada por $S(x_0, r)$ e definida por:*

$$S(x_0, r) = \{x \in \mathbb{R}^n;\ \|x - x_0\| \leq r\}.$$

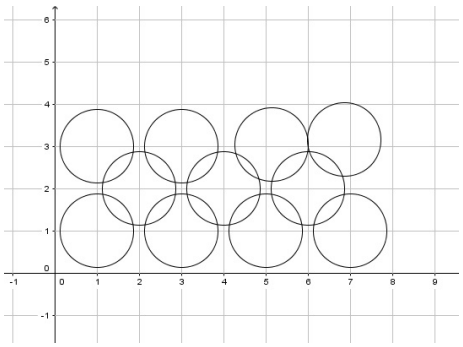
Definição 2.2.2. *Um empacotamento esférico em $\mathbb{R}^n$ é uma disposição de esferas n-dimensionais de mesmo raio em $\mathbb{R}^n$, de modo que a interseção de duas esferas quaisquer tenha no máximo um ponto.*

Exemplos. *1. Os intervalos fechados de comprimento 1 com centro nos números inteiros é um exemplo de empacotamento esférico em $\mathbb{R}$.*

2. A seguinte figura ilustra um exemplo de empacotamento esférico em $\mathbb{R}^2$:



3. A seguinte figura não é um empacotamento esférico em $\mathbb{R}^2$:



O interesse deste trabalho são os casos em que os centros, de tais esferas, formam um subgrupo discreto de $\mathbb{R}^n$.

Definição 2.2.3. *Sejam n um inteiro positivo e $\{v_1, \cdots, v_m\}$ um conjunto de vetores de $\mathbb{R}^n$, com $m \leq n$, linearmente independentes sobre $\mathbb{R}$. Definimos o reticulado Λ de posto m e base $\{v_1, \cdots, v_m\}$ como sendo o conjunto*

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

Antes de continuarmos falando sobre os reticulados, precisamos do próximo resultado, cuja demonstração encontra-se em [10]

Teorema 2.2.4. *([10], pág: 53) Seja $\mathcal{H}$ um subgrupo discreto de $\mathbb{R}^n$. Então, $\mathcal{H}$ é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$ com $r \leq n$.*

Segue do Teorema anterior que, todo subgrupo discreto de $\mathbb{R}^n$ é um reticulado.

Definição 2.2.5. *Um empacotamento reticulado é aquele cujo conjunto dos centros é um reticulado.*

Exemplo. *Se tomarmos $\Lambda = \mathbb{Z}^n$, com a base canônica, e o raio de tais esferas igual a $1/2$, temos um empacotamento reticulado.*

Definição 2.2.6. *Dado Λ um reticulado, de $\mathbb{R}^n$, e $\mathcal{B} = \{v_1, \cdots, v_n\}$ uma base de Λ, o conjunto*

$$\mathcal{R}(\mathcal{B}) = \left\{ x \in \mathbb{R}^n;\ x = \sum_{i=1}^{n} \lambda_i v_i;\ 0 \leq \lambda_i < 1 \right\},$$

é chamado de região fundamental de Λ com relação à base $\mathcal{B}$.

Dado um reticulado Λ de $\mathbb{R}^n$, existem diferentes maneiras de escolher uma base e uma região fundamental. No entanto, independente desta escolha, o volume sempre é o mesmo.

Lema 2.2.7. *([10], pág: 55) O volume da região fundamental $v(\mathcal{R})$ independe da base escolhida.*

Portanto, denotaremos $v(\mathcal{R})$ por $v(\Lambda)$.

Dado um reticulado em $\mathbb{R}^n$, ao maior raio, para o qual seja possível definir um empacotamento de Λ, denominamos *raio de empacotamento* de Λ e é dado por:

$$\rho = \frac{\min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\}}{2}.$$

Isto posto, define-se a *densidade de empacotamento* de Λ como sendo

$$\Delta(\Lambda) = \frac{\text{volume de uma esfera de raio } \rho}{\text{volume da região fundamental}}.$$

Assim, a densidade de empacotamento pode ser reescrita por:

$$\Delta(\Lambda) = \frac{v(S(\rho))}{v(\mathcal{R})} = v(S(1)) \cdot \frac{\rho^n}{v(\Lambda)},$$

onde $S(\rho)$ é a esfera de centro na origem e raio ρ.

Definição 2.2.8. *Definimos a densidade de centro $\delta(\Lambda)$ do reticulado Λ como sendo*

$$\delta(\Lambda) = \frac{\rho^n}{v(\Lambda)}.$$

Logo, o problema do Empacotamento Esférico, discutido no inicio do capítulo, equivale ao estudo da densidade de centro. Neste trabalho, restringimos aos empacotamentos reticulados.

Exemplos. *1. Seja Λ o reticulado em $\mathbb{R}$ gerado por 1, isto é, $\Lambda = \mathbb{Z}$. Temos que, $\min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\} = 1$. Assim, $\rho = 1/2$ é o raio de empacotamento de Λ. Além disso, $v(\Lambda) = 1$ e $v(S(1)) = 2$, portanto*

$$\Delta(\Lambda) = 1 \qquad e \qquad \delta(\Lambda) = \frac{1}{2}.$$

Este reticulado tem a maior densidade de empacotamento em $\mathbb{R}$.

2. Seja Λ o reticulado de $\mathbb{R}^2$ gerado pela base $\{(1,0),(1/2,\sqrt{3}/2)\}$, ou seja, $\Lambda = \mathbb{Z}(1,0) + \mathbb{Z}(1/2,\sqrt{3}/2)$. Assim sendo, $\min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\} = 1$, logo $\rho = 1/2$ é o raio de empacotamento de Λ. Além disso,

$$v(\Lambda) = \left|\det \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}\right| = \sqrt{3}/2.$$

Além do mais, $v(S(1)) = \pi$, e $\rho^2 = 1/4$, donde

$$\Delta(\Lambda) = \frac{\pi}{\sqrt{12}} \simeq 0,9069 \qquad e \qquad \delta(\Lambda) = \frac{1}{\sqrt{12}} \simeq 0,2886751.$$

Este reticulado tem a maior densidade de empacotamento em $\mathbb{R}^2$.

Logo, para as dimensões 1 e 2, o problema está solucionado.

2.3 Reticulados Algébricos

O principal objetivo desta seção, é identificar um $\mathbb{Z}$-módulo livre de posto n, contido num corpo de números $\mathbb{K}$ de grau n, com um reticulado de $\mathbb{R}^n$. Esta identificação é importante pois, nos permite apresentar algumas características do reticulado obtido, como o volume e a densidade de centro, através das propriedades do $\mathbb{Z}$-módulo.

Considere $\mathbb{K}$ um corpo de números de grau n. Usando o fato que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem exatamente n raízes em $\mathbb{C}$, pois $\mathbb{C}$ é algebricamente fechado, temos que existem n distintos monomorfismos $\sigma_i : \mathbb{K} \to \mathbb{C}$.

Se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, dizemos que σ_j é um *monomorfismo real* , caso contrário, dizemos que σ_j é um *monomorfismo imaginário*. Também, se todos os monomorfismos são reais, dizemos que $\mathbb{K}$ é um *corpo totalmente real*, similarmente, se todos os monomorfismos são imaginários, dizemos que $\mathbb{K}$ é um *corpo totalmente imaginário*. Além disso, se σ_j é um monomorfismo imaginário, seu conjugado complexo difere dele e é também um monomorfismo imaginário, consequentemente, sempre temos um número par de monomorfismos imaginários. Desse modo, denotando por r_1 o número de monomorfismos reais e por $2r_2$ o número de monomorfismos imaginários, segue que $n = r_1 + 2r_2$, além disso, podemos ordenar os monomorfismos de modo que $\sigma_1, \cdots, \sigma_{r_1}$ sejam os monomorfismos reais e $\sigma_{r_1+1}, \cdots, \sigma_{r_1+2r_2}$ correspondam aos monomorfismos imaginários, de maneira que $\sigma_{r_1+r_2+j}$ seja o conjugado de σ_{r_1+j} para $j = 1, \cdots, r_2$. Donde, temos a seguinte:

Definição 2.3.1. *O homomorfismo injetivo de anéis $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$, definido por:*

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

é chamado de homomorfismo de Minkowski, ou homomorfismo canônico, onde $Re(z)$ e $Im(z)$ representam, respectivamente, a parte real e imaginária de um número complexo z.

Exemplo. *1. Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_3)$. Tem-se que os monomorfismos σ_1 e σ_2 de $\mathbb{K}$ em $\mathbb{C}$, são dados por $\sigma_j(\zeta_3) = \zeta_3^j$, com $j = 1, 2$. Deste modo, $\mathbb{K}$ é totalmente imaginário ($r_1 = 0$ e $r_2 = 1$). Se $x = a + b\zeta_3 \in \mathbb{K}$, então, $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^2$ é dado por*

$$\sigma_{\mathbb{K}}(x) = \left(Re\left(\sigma_1(x)\right), Im\left(\sigma_1(x)\right)\right) = \left(Re\left(a - \frac{b}{2} + \frac{b\sqrt{3}i}{2}\right), Im\left(a - \frac{b}{2} + \frac{b\sqrt{3}i}{2}\right)\right) = \left(a - \frac{b}{2}, \frac{b\sqrt{3}}{2}\right).$$

O homomorfismo de Minkowski é a identificação que nos referíamos no inicio da seção. A garantia desta afirmação é a seguinte proposição.

Proposição 2.3.2. *([10], pág: 56) Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{M} \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_1, \cdots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$, então $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado em $\mathbb{R}^n$, cujo volume é:*

$$v(\sigma_{\mathbb{K}}(\mathcal{M})) = 2^{-r_2} \left| \det_{1 \leq i,\ j \leq n} (\sigma_i(x_j)) \right|$$

Proposição 2.3.3. *([10], pág: 57) Considere D o discriminante de $\mathbb{K}$ e $\mathcal{I}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Então, $\sigma_{\mathbb{K}}(\mathcal{I})$ é um reticulado no $\mathbb{R}^n$, cujo volume é:*

$$v(\sigma_{\mathbb{K}}(\mathcal{I})) = 2^{-r_2}|D|^{1/2}N(\mathcal{I}).$$

Segue da última Proposição que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ é dado por:

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathcal{I})))^n}{|D|^{1/2}N(\mathcal{I})},$$

onde, $\rho(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{1}{2}\min\{|\sigma_{\mathbb{K}}(x)|;\ x \in \mathcal{I},\ x \neq 0\}$. Observe ainda que, $N(\mathcal{I}) = 1$ se, e somente se, $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$.

Definição 2.3.4. *Se $\mathbb{K}$ é um corpo de números e $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. O reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ é denominado Realização Geométrica ou Reticulado Algébrico de $\mathcal{I}$.*

Exemplo. *Consideremos o Corpo Quadrático $\mathbb{K} = \mathbb{Q}(i)$ então, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ com $\mathbb{Z}$-base $\{1, i\}$. Além disso, os monomorfismos σ_1 e σ_2 de $\mathbb{K}$ em $\mathbb{C}$, são respectivamente, as aplicações identidade e conjugação complexa. Para $x = a + bi \in \mathbb{K}$, temos*

$$\sigma_{\mathbb{K}}(x) = (Re(\sigma_1(x)), Im(\sigma_1(x))) = (a, b).$$

Seja $\mathcal{I} =< 2 - i >$ um ideal principal de $\mathbb{Z}[i]$. Dado $x \in \mathcal{I}$, temos $x = (2 - i)(a + bi) = (2a + b) + (2b - a)i$, com $a, b \in \mathbb{Z}$. Logo, a imagem de $\sigma_{\mathbb{K}}(\mathcal{I}) \subseteq \mathbb{R}^2$ é dada por:

$$\sigma_{\mathbb{K}}(\mathcal{I}) = \{(2a + b, 2b - a) \in \mathbb{R}^2;\ a, b \in \mathbb{Z}\}.$$

Desse modo, $\sigma_{\mathbb{K}}(\mathcal{I})$ é um reticulado no $\mathbb{R}^2$, do qual $\{(2, -1), (1, 2)\}$ é uma base. Além disso, temos que $\mathbb{K} = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ assim, usando o Exemplo 1.5.2, temos $D = -4$, e portanto, $|D|^{\frac{1}{2}} = 2$. Pela Proposição 2.3.3,

$$v(\sigma_{\mathbb{K}}(\mathcal{I})) = 2^{-1} \cdot 2 \cdot N(\mathcal{I}) = N(\mathcal{I}).$$

pela Observação (1.6.4), temos $N(\mathcal{I}) = |N(2 - i)| = 5$ e, portanto,

$$v(\sigma_{\mathbb{K}}(\mathcal{I})) = 5.$$

Agora, se considerarmos o reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, temos

$$v(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-1} \cdot 2 \cdot N(\mathcal{O}_{\mathbb{K}}) = 1.$$

Os casos mais interessantes ocorrem quando $\mathbb{K}$ é totalmente real ou totalmente imaginário. Portanto, apresentaremos alguns resultados para estes casos específicos.

Proposição 2.3.5. *([1], pág: 225) Seja $\mathbb{K}$ um corpo de números, $x \in \mathbb{K}$ e $\sigma_{\mathbb{K}}$ o homomorfismo de Minkowski. Então,*

$$|\sigma_{\mathbb{K}}(x)|^2 = c \cdot Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), \quad c = \begin{cases} 1, & \text{se } \mathbb{K} \text{ for totalmente real;} \\ \frac{1}{2}, & \text{se } \mathbb{K} \text{ for totalmente imaginário.} \end{cases}$$

Considere $\mathbb{K}$ um corpo de números e $\mathcal{I}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, podemos reescrever o raio de empacotamento do reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ da seguinte forma:

$$\rho(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{1}{2}\min\{|\sigma_{\mathbb{K}}(x)|;\ x \in \mathcal{I},\ x \neq 0\} = \frac{1}{2}\min\left\{\sqrt{cTr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})};\ x \in \mathcal{I},\ x \neq 0\right\}. \tag{2.4}$$

Fazendo $t = \min\left\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x});\ x \in \mathcal{I},\ x \neq 0\right\}$ temos:

1. Considere $\mathbb{K}$, um corpo de números totalmente real, então:

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{\left(\frac{\sqrt{t}}{2}\right)^n}{|D|^{\frac{1}{2}}N(\mathcal{I})} = \frac{\left(\sqrt{t}\right)^n}{2^n|D|^{\frac{1}{2}}N(\mathcal{I})} = \frac{t^{\frac{n}{2}}}{2^n|D|^{\frac{1}{2}}N(\mathcal{I})}$$

2. Se $\mathbb{K}$ é um corpo de números totalmente imaginário, temos:

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{2^{\frac{n}{2}}\left(\frac{\sqrt{\frac{t}{2}}}{2}\right)^n}{|D|^{\frac{1}{2}}N(\mathcal{I})} = \frac{\frac{\left(2^{\frac{n}{2}}\right)(t)^{\frac{n}{2}}}{2^n 2^{\frac{n}{2}}}}{|D|^{\frac{1}{2}}N(\mathcal{I})} = \frac{\frac{t^{\frac{n}{2}}}{2^n}}{|D|^{\frac{1}{2}}N(\mathcal{I})} = \frac{t^{\frac{n}{2}}}{2^n|D|^{\frac{1}{2}}N(\mathcal{I})}$$

Isto posto, a expressão da densidade de centro é a mesma em ambos casos.

Observação 2.3.6. *Se $\mathbb{K}|\mathbb{Q}$ é uma extensão galoisiana então, $\mathbb{K}$ é totalmente real ou totalmente imaginário.*

Demonstração. Todo monomorfismo σ de $\mathbb{K}$ satisfaz $\sigma(\mathbb{K}) = \mathbb{K}$, já que $\mathbb{K}|\mathbb{Q}$ é uma extensão galoisiana. Se $\mathbb{K} \subset \mathbb{R}$ então $\sigma(\mathbb{K}) \subset \mathbb{R}$, para todo σ e portanto $\mathbb{K}$ é totalmente real. Analogamente, se $\mathbb{K}$ não está contido em $\mathbb{R}$, temos que $\mathbb{K}$ é totalmente imaginário.

□

Consequentemente, se $\mathbb{K}|\mathbb{Q}$ é uma extensão galoisiana, e $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ é dada por:

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{t^{\frac{n}{2}}}{2^n |D|^{\frac{1}{2}} N(\mathcal{I})},$$

onde $t = \min\left\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x});\ x \in \mathcal{I},\ x \neq 0\right\}$.

2.4 Forma Quadrática

Na seção anterior, mostramos alguns métodos para obter reticulados via homomorfismo de Minkowski, para estes, conhecemos uma fórmula para calcular seu volume correspondente. Nesta seção, nosso objetivo é reescrever o raio de empacotamento para tais reticulados, pois com isto, temos as ferramentas necessárias para calcular as respectivas densidade de centro.

Vimos na Proposição 2.3.2, que dado um corpo de números $\mathbb{K}$, a imagem do homomorfismo de Minkowski por um $\mathbb{Z}$-módulo de $\mathbb{K}$ é um reticulado. Isto posto, escolhemos elementos arbitrários do seu anel de inteiros, $\mathcal{O}_{\mathbb{K}}$, e seus respectivos conjugados. Para escolhas convenientes, este conjunto, $\mathcal{B} = \{\omega, \sigma(\omega), \beta, \sigma(\beta)\}$, constitui uma base de um $\mathbb{Z}$-módulo $\mathcal{M}$ de $\mathbb{K}$.

Suponha que o grau de $\mathbb{K}$ sobre $\mathbb{Q}$ seja igual a 4. Aplicando o homomorfismo de Minkowski temos:

$$\begin{aligned}
\sigma_{\mathbb{K}} : \mathcal{O}_{\mathbb{K}} &\longrightarrow \mathbb{R}^4 \\
\omega &\longmapsto \big(\omega, \sigma(\omega), \sigma^2(\omega), \sigma^3(\omega)\big) \\
\sigma(\omega) &\longmapsto \big(\sigma(\omega), \sigma^2(\omega), \sigma^3(\omega), \omega\big) \\
\beta &\longmapsto \big(\beta, \sigma(\beta), \sigma^2(\beta), \sigma^3(\beta)\big) \\
\sigma(\beta) &\longmapsto \big(\sigma(\beta), \sigma^2(\beta), \sigma^3(\beta), \beta\big)
\end{aligned}$$

A Proposição 2.3.2, nos dá uma fórmula de como calcular o volume do reticulado $\sigma_{\mathbb{K}}(\mathcal{M})$. Nosso objetivo será encontrar uma expressão para ρ. Para isto, dado $v \in \mathcal{M}$, existem $X_1, X_2, X_3, X_4 \in \mathbb{Z}$ tais que:

$$\sigma_{\mathbb{K}}(v) = \begin{pmatrix} \omega & \sigma(\omega) & \beta & \sigma(\beta) \\ \sigma(\omega) & \sigma^2(\omega) & \sigma(\beta) & \sigma^2(\beta) \\ \sigma^2(\omega) & \sigma^3(\omega) & \sigma^2(\beta) & \sigma^3(\beta) \\ \sigma^3(\omega) & \omega & \sigma^3(\beta) & \beta \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} X_1\omega + X_2\sigma(\omega) + X_3\beta + X_4\sigma(\beta) \\ X_1\sigma(\omega) + X_2\sigma^2(\omega) + X_3\sigma(\beta) + X_4\sigma^2(\beta) \\ X_1\sigma^2(\omega) + X_2\sigma^3(\omega) + X_3\sigma^2(\beta) + X_4\sigma^3(\beta) \\ X_1\sigma^3(\omega) + X_2\omega + X_3\sigma^3(\beta) + X_4\beta \end{pmatrix}$$

Donde, usando que $\sigma(\omega)^i = \sigma(\omega^i)$, $i = 2, 3$, temos:

$$\begin{aligned}
|\sigma_{\mathbb{K}}(v)|^2 &= X_1^2[\omega^2 + \sigma(\omega^2) + \sigma^2(\omega^2) + \sigma^3(\omega^2)] + X_2^2[\sigma(\omega^2) + \sigma^2(\omega^2) + \sigma^3(\omega^2) + \omega^2] + \\
&\quad + X_3^2[\beta^2 + \sigma(\beta^2) + \sigma^2(\beta^2) + \sigma^3(\beta^2)] + X_4^2[\sigma(\beta^2) + \sigma^2(\beta^2) + \sigma^3(\beta^2) + \beta^2] + \\
&\quad + 2X_1X_2[\omega\sigma(\omega) + \sigma(\omega)\sigma^2(\omega) + \sigma^2(\omega)\sigma^3(\omega) + \sigma^3(\omega)\omega] \\
&\quad + 2X_1X_3[\omega\beta + \sigma(\omega)\sigma(\beta) + \sigma^2(\omega)\sigma^2(\beta) + \sigma^3(\omega)\sigma^3(\beta)] \\
&\quad + 2X_1X_4[\omega\sigma(\beta) + \sigma(\omega)\sigma^2(\beta) + \sigma^2(\omega)\sigma^3(\beta) + \sigma^3(\omega)\beta] \\
&\quad + 2X_2X_3[\sigma(\omega)\beta + \sigma^2(\omega)\sigma(\beta) + \sigma^3(\omega)\sigma^2(\beta) + \omega\sigma^3(\beta)] \\
&\quad + 2X_2X_4[\sigma(\omega)\sigma(\beta) + \sigma^2(\omega)\sigma^2(\beta) + \sigma^3(\omega)\sigma^3(\beta) + \omega\beta] \\
&\quad + 2X_3X_4[\beta\sigma(\beta) + \sigma(\beta)\sigma^2(\beta) + \sigma^2(\beta)\sigma^3(\beta) + \sigma^3(\beta)\beta] \\
&= \left(Tr(\omega^2)\right)\left(X_1^2 + X_2^2\right) + \left(Tr(\beta^2)\right)\left(X_3^2 + X_4^2\right) \\
&\quad + \left(Tr(\omega\sigma(\omega))\right)(2X_1X_2) + \left(Tr(\omega\beta)\right)(2X_1X_3 + 2X_2X_4) \\
&\quad + \left(Tr(\omega\sigma(\beta))\right)(2X_1X_4) + \left(Tr(\sigma(\omega)\beta)\right)(2X_2X_3) + \left(Tr(\beta\sigma(\beta))\right)(2X_3X_4) \qquad (2.5)
\end{aligned}$$

Portanto, para determinar o raio de empacotamento, precisamos calcular os coeficientes da forma quadrática anterior.

Vale ressaltar que:

$$\begin{aligned}
|\sigma_{\mathbb{K}}(\alpha)|^2 &= \alpha^2 + \sigma_1(\alpha)^2 + \sigma_2(\alpha)^2 + \sigma_3(\alpha)^2 \\
&\geq 4\sqrt{\prod_{i=1}^{4}(\sigma_i(\alpha^2))} = 4\sqrt[4]{N(\alpha^2)} \geq 4, \qquad (2.6)
\end{aligned}$$

onde, a primeira desigualdade ocorre pois, de um lado, temos a média aritmética de elementos positivos que é sempre maior ou igual a média geométrica. A segunda desigualdade ocorre pois $N(x)$ é sempre maior ou igual a 1. Donde, $|\sigma_{\mathbb{K}}(v)|^2 \geq 4$, consequentemente, se conseguirmos um elemento $v \in \mathcal{M}$, cuja imagem pelo homomorfismo de Minkowski tenha comprimento exatamente igual a 2, este será o menor comprimento possível, neste caso, o raio de empacotamento será 1.

Nas mesmas hipóteses, pela Proposição 2.3.3, temos que $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é um reticulado e sabemos como calcular seu volume. Supondo que $\{b_1, b_2, b_3, b_4\}$ formam uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{K}}$, para todo β elemento de $\mathcal{O}_{\mathbb{K}}$, existem X_1, X_2, X_3 e X_4 pertencentes a $\mathbb{Z}$, tais que $\beta = X_1b_1 + X_2b_2 + X_3b_3 + X_4b_4$,

portanto,

$$\begin{aligned}\beta^2 &= X_1^2b_1^2 + X_2^2b_2^2 + X_3^2b_3^2 + X_4^2b_4^2 + 2X_1X_2b_1b_2 + 2X_1X_3b_1b_3 + 2X_1X_4b_1b_4 + \\ &\quad +2X_2X_3b_2b_3 + 2X_2X_4b_2b_4 + 2X_3X_4b_3b_4\end{aligned}$$

Usando a Equação 2.4, e supondo que $\mathbb{K}$ é totalmente real temos que $\rho(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{\sqrt{t}}{2}$ onde, $t = \min\left\{Tr_{\mathbb{K}/\mathbb{Q}}(\beta^2);\ \beta \in \mathcal{O}_{\mathbb{K}},\ \beta \neq 0\right\}$. Além disso,

$$\begin{aligned}Tr_{\mathbb{K}/\mathbb{Q}}(\beta^2) &= X_1^2Tr_{\mathbb{K}/\mathbb{Q}}(b_1^2) + X_2^2Tr_{\mathbb{K}/\mathbb{Q}}(b_2^2) + X_3^2Tr_{\mathbb{K}/\mathbb{Q}}(b_3^2) + X_4^2Tr_{\mathbb{K}/\mathbb{Q}}(b_4^2) + \\ &\quad +2X_1X_2Tr_{\mathbb{K}/\mathbb{Q}}(b_1b_2) + 2X_1X_3Tr_{\mathbb{K}/\mathbb{Q}}(b_1b_3) + 2X_1X_4Tr_{\mathbb{K}/\mathbb{Q}}(b_1b_4) + \\ &\quad +2X_2X_3Tr_{\mathbb{K}/\mathbb{Q}}(b_2b_3) + 2X_2X_4Tr_{\mathbb{K}/\mathbb{Q}}(b_2b_4) + 2X_3X_4Tr_{\mathbb{K}/\mathbb{Q}}(b_3b_4).\end{aligned}$$

Observação 2.4.1. *Se $b_1 = 1$ pertence a base integral de $\mathbb{K}$, podemos considerar $\beta = 1$, neste caso, $Tr_{\mathbb{K}/\mathbb{Q}}(\beta^2) = 4$ e, pela desigualdade 2.6, temos que o raio de empacotamento é 1.*

2.5 Outras Propriedades

Nesta seção, agrupamos resultados importantes para a continuidade deste trabalho. Iniciamos com um lema da Teoria de Galois, o qual nos permite deduzir propriedades da função traço. Posteriormente, explicitamos qual o valor da função traço aplicada na raiz n-ésima primitiva da unidade. Por fim, apresentamos quem é o *compositum* e a interseção de corpos ciclotômicos.

Lema 2.5.1. *([4], pág: 263) Sejam $\mathbb{L}$ e $\mathbb{K}$ extensões galoisianas de $\mathbb{M}$, tais que, $\mathbb{L} \cap \mathbb{K} = \mathbb{M}$. Então, o compositum de $\mathbb{L}$ e $\mathbb{K}$, $\mathbb{LK}$ é uma extensão galoisiana de $\mathbb{M}$ e $Gal(\mathbb{LK}/\mathbb{K})$ é isomorfo ao $Gal(\mathbb{L}/\mathbb{M})$.*

Faremos a demonstração deste Lema, para o caso particular, $\mathbb{L} \cap \mathbb{K} = \mathbb{Q}$. A demonstração geral pode ser encontrada em [4] págs: 263 -264.

Demonstração. Considere $\mathbb{K} = \mathbb{Q}(\alpha)$ então, $\mathbb{LK} = \mathbb{L}(\alpha)$, o qual é uma extensão galoisiana sobre $\mathbb{L}$ já que, os conjugados de α sobre $\mathbb{L}$ estão entre os conjugados de α sobre $\mathbb{K}$, pois $\mathbb{K}$ contém todos os conjugados de α por hipótese.

Além disso, a restrição dos automorfismos de $Gal(\mathbb{LK}/\mathbb{K})$ a $\mathbb{L}$ geram um isomorfismo. Em outras palavras,

$$\psi : Gal(\mathbb{LK}/\mathbb{K}) \to Gal(\mathbb{L}/\mathbb{Q})$$

é um homomorfismo e é imediato que $ker(\psi) = 0$, ou seja, ψ é injetora.

Agora, considere $H = \psi(Gal(\mathbb{LK}/\mathbb{K}))$, isto é, H é a imagem de ψ, temos que H fixa o corpo $\mathbb{L} \cap \mathbb{K} = \mathbb{Q}$. Então, pela correspondência de Galois, $H = Gal(\mathbb{L}/\mathbb{K} \cap \mathbb{L}) = Gal(\mathbb{L}/\mathbb{Q})$. Donde, ψ é sobrejetiva e portanto, ψ é um isomorfismo. □

Observação 2.5.2. *Decorre do Lema anterior que,* $[\mathbb{LK}/\mathbb{K} : \mathbb{K}] = [\mathbb{L} : \mathbb{L} \cap \mathbb{K}]$.

Observação 2.5.3. *É consequência imediata do Lema que, nas mesmas hipóteses, para todo elemento* α *de* $\mathbb{L}$*, temos:*

$$Tr_{\mathbb{LK}/\mathbb{K}}(\alpha) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha).$$

Teorema 2.5.4. *([4], pág: 23) Sejam* $\mathbb{K}, \mathbb{L}$ *e* $\mathbb{M}$ *corpos de números, tais que,* $\mathbb{L}$ *é uma extensão de* $\mathbb{K}$ *e* $\mathbb{M}$ *é uma extensão de* $\mathbb{L}$*. Então, para todo* $\alpha \in \mathbb{M}$*, temos:*

$$Tr_{\mathbb{L}/\mathbb{K}}\left(Tr_{\mathbb{M}/\mathbb{L}}(\alpha)\right) = Tr_{\mathbb{M}/\mathbb{K}}(\alpha).$$

Demonstração. Sejam $\sigma_1, \cdots, \sigma_n$ os automorfismos de $\mathbb{L}$ que fixam $\mathbb{K}$ e, sejam $\tau_1, \cdots, \tau_m$ os automorfismos de $\mathbb{M}$ que fixam $\mathbb{L}$.

Seja $\mathcal{N}$ uma extensão normal de $\mathbb{Q}$ (isto é, todo polinômio que pertence a $\mathbb{Q}[X]$ que possui uma raiz em $\mathcal{N}$, se decompõe em $\mathcal{N}$), de modo que $\mathcal{N}$ seja uma extensão finita de $\mathbb{M}$. Assim, os automorfismos σ_i e τ_j podem ser estendidos à automorfismos de $\mathcal{N}$, fixando ainda, $\mathbb{K}$ e $\mathbb{L}$ respectivamente. Denotando estes novos automorfismos, novamente, por σ_i e τ_j, podemos fazer a composição destas aplicações. Donde, para $\alpha \in \mathbb{M}$, temos:

$$Tr_{\mathbb{L}/\mathbb{K}}\left(Tr_{\mathbb{M}/\mathbb{L}}(\alpha)\right) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(\alpha) \right) = \sum_{i,j} (\sigma_i \circ \tau_j)(\alpha).$$

Resta mostrar que as aplicações $\sigma_i \circ \tau_j$, quando restritas a $\mathbb{M}$, resultam num automorfismo que fixa $\mathbb{K}$. Como todos os σ_i, τ_j fixam $\mathbb{K}$ (σ_i fixa $\mathbb{K}$ por definição e τ_j fixa $\mathbb{L}$ por definição e, portanto, fixa $\mathbb{K}$, já que, por hipótese $\mathbb{K} \subset \mathbb{L}$) e existem $m \cdot n$ automorfismos, é suficiente mostrar que eles são todos distintos quando restritos a $\mathbb{M}$.

Suponha por absurdo que $\sigma_i \circ \tau_j = \sigma_k \circ \tau_j$ com $\sigma_i \neq \sigma_k$. Então, para todo $\alpha \in \mathbb{M}$, temos:

$$\sigma_i \circ \tau_j(\alpha) = \sigma_k \circ \tau_j(\alpha) \Rightarrow \sigma_i(a) = \sigma_k(a)$$

donde, $\sigma_i = \sigma_k$, absurdo. Portanto, $\sigma_i \circ \tau_j$ são todos distintos, e assim, a demonstração está concluida.

□

O próximo resultado calcula o traço das raízes n-ésimas primitivas da unidade.

Teorema 2.5.5. *Seja n um número inteiro maior que 1, $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$, sua fatoração primária. Se $\zeta_n = e^{\frac{2\pi}{n}}$ é uma raiz primitiva n-ésima da unidade então:*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = \begin{cases} (-1)^s, & \text{se } n \text{ é livre de quadrados} \\ 0, & \text{caso contrário.} \end{cases}$$

Demonstração. Inicialmente, recordemos uma consequência da Proposição 1.4.3, se α é algébrico sobre $\mathbb{Q}$ então, o polinômio $p(X)$, minimal de α sobre $\mathbb{Q}$ é dado por:

$$p(X) = X^m + (-1)Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)X^{m-1} + \cdots + (\pm)N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha), \tag{2.7}$$

onde $m = [\mathbb{Q}(\alpha)/\mathbb{Q}]$.

Faremos a prova usando indução sobre s, isto é, sobre a quantidade de números primos que dividem n.

Provaremos para $s = 1$. Com esta hipótese temos dois casos a considerar:

1º Caso: n=p. Sabemos que o p-ésimo polinômio ciclotômico, que é o minimal de ζ_p sobre $\mathbb{Q}$, é dado por:

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

logo, por 2.7 temos:

$$1 = (-1)Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p),$$

e, portanto, $-1 = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p)$.

2º Caso: $n = p^r$, com $r > 1$. O p^r-ésimo polinômio ciclotômico, é dado por:

$$\Phi_p^r(X) = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1.$$

Portanto, por 2.7 temos que $Tr_{\mathbb{Q}(\zeta_p^r)/\mathbb{Q}}(\zeta_p^r) = 0$.

Segue do 1º e do 2º caso que, se $s = 1$ então o teorema é válido.

Suponha que o teorema seja válido quando n possui $s-1$ divisores primos e, provaremos para s. Antes, recordemos a Identidade de Bezout.

Identidade de Bezout: Se $(m, n) = 1$ então, existem $u, v \in \mathbb{Z}$, tais que, $un + vm = 1$.

Temos que $n = p_1^{a_1}p_2^{a_2}\cdots p_{s-1}^{a_{s-1}}p_s^{a_s} := p_1^{a_1}k$. Por Bezout, como $(p_1^{a_1}, k) = 1$, existem $u, v \in \mathbb{Z}$, tais que $up_1^{a_1} + vk = 1$, note que, $(v, p_1^{a_1}) = 1$ e $(u, k) = 1$. Logo, podemos reescrever ζ_n da seguinte forma:

$$\zeta_n = \zeta_n^{up_1^{a_1}+vk} = \zeta_n^{up_1^{a_1}}\zeta_n^{vk} = \zeta_k^u\zeta_{p_1^{a_1}}^v$$

Calculando o traço de ζ_n temos:

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) &= Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(\zeta_k^u \zeta_{p_1^{a_1}}^v\right) \\ &= Tr_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}\left(\zeta_k^u Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_k)}\left(\zeta_{p_1^{a_1}}^v\right)\right) \\ &= Tr_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}\left(\zeta_k^u Tr_{\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}}\left(\zeta_{p_1^{a_1}}^v\right)\right) \end{aligned}$$

onde, a segunda igualdade é válida pelo Teorema 2.5.4 e a terceira igualdade decorre do Lema 2.5.1. Além disso, como $\zeta_{p_1^{a_1}}^v$ é conjugado de $\zeta_{p_1^{a_1}}$, segue que o traço de ambos coincidem. Portanto,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}\left(\zeta_k^u Tr_{\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}}\zeta_{p_1^{a_1}}\right)$$

Pelo 2º caso, temos que

$$Tr_{\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}}\left(\zeta_{p_1^{a_1}}\right) = \begin{cases} -1, & \text{se } a_1 = 1 \\ 0, & \text{se } a_1 > 1 \end{cases}$$

Consequentemente, se $a_1 > 1$, teremos $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = 0$. No entanto, se $a_1 = 1$,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(-\zeta_k^u) = -Tr_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\zeta_k)$$

Pela hipótese de indução, se k é livre de quadrados $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = (-1)^{s-1}$ caso contrário, temos $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = 0$. Donde, $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = (-1)(-1)^{s-1} = (-1)^s$ se n é livre de quadrados e $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = 0$ caso contrário.

□

Observação. *O Teorema anterior calcula o traço de ζ_n. Sabemos que o traço de um elemento coincide com o traço de seu conjugado, além disso, já mostramos que o polinômino minimal de ζ_n é o n-ésimo polinômio ciclotômico, cujas raízes, os conjugados de ζ_n, são as demais raízes n-ésimas primitivas da unidade, logo, o Teorema anterior é válido para toda raiz n-ésima primitiva da unidade.*

O próximo resultado nos garante que, o *compositum* e a interseção de corpos ciclotômicos, é ainda um corpo ciclotômico.

Lema 2.5.6. *Dados m e n inteiros positivos, denote por d o máximo divisor comum e por f o mínimo múltiplo comum entre eles. Então, o compositum $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_f)$ e a interseção $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$.*

Demonstração. Da relação entre mínimo múltiplo comum e máximo divisor comum temos: $d = \frac{m \cdot n}{f}$, além disso, usando a identidade de Bezout, temos que existem a e b elementos inteiros tais que: $d = am + bn$, donde, $am + bn = \frac{m \cdot n}{f}$, e portanto, $\frac{a}{n} + \frac{b}{m} = \frac{1}{f}$. Desta forma,

$$\left(e^{\frac{2\pi i}{n}}\right)^a \cdot \left(e^{\frac{2\pi i}{m}}\right)^b = e^{\frac{2\pi i}{f}},$$

o que implica que $\mathbb{Q}(\zeta_f)$ está contido no *compositum* $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$. Além disso, é claro que $\mathbb{Q}(\zeta_m)$ e $\mathbb{Q}(\zeta_n)$ estão contidos em $\mathbb{Q}(\zeta_f)$ portanto, $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_f)$.

Agora, usando que $d = \frac{m \cdot n}{f}$, temos que

$$(\zeta_d)^{\frac{m}{f}} = \left(e^{\frac{2\pi i}{d}}\right)^{\frac{m}{f}} = e^{\frac{2\pi i}{n}} = \zeta_n \quad \text{e} \quad (\zeta_d)^{\frac{n}{f}} = \left(e^{\frac{2\pi i}{d}}\right)^{\frac{n}{f}} = e^{\frac{2\pi i}{m}} = \zeta_m,$$

ou seja, $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_n)$ e $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_m)$, donde, $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$.

Por outro lado, usando a Observação 2.5.2, temos: $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_f) : \mathbb{Q}(\zeta_n)] = \frac{\varphi(f)}{\varphi(n)} = \frac{\varphi(m)}{\varphi(d)}$. Logo,

$$[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(d).$$

Como $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \varphi(d)$, temos a igualdade $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$. □

Capítulo

3

Corpos Abelianos e Aplicações

O objetivo deste capítulo é aplicar os resultados desenvolvidos nos capítulos anteriores, em alguns corpos de números abelianos. O resultado abaixo garante:

Teorema 3.0.7. *(Kronecker-Weber)([12], pág: 341) Seja $\mathbb{K}$ um corpo de números abeliano. Então, $\mathbb{K}$ está contido em algum corpo ciclotômico.*

Os referidos corpos de números abelianos que trabalharemos são: os subcorpos reais maximais de corpos ciclotômicos de grau 8, os subcorpos de $\mathbb{Q}(\zeta_7)$ e os subcorpos de $\mathbb{Q}(\zeta_{17})$.

Iniciaremos este capítulo estudando o grupo de Galois de um corpo ciclotômico qualquer. Posteriormente, definiremos base integral normal e apresentaremos um resultado que nos auxilia no cálculo do dicriminante, válido para corpos de números abelianos. Na sequência, aplicamos os resultados até aqui obtidos em p-ésimos corpos ciclotômicos e por fim, faremos o mesmo para subcorpos reais maximais de corpos ciclotômicos de grau 8.

3.1 Grupo de Galois de Corpos Abelianos

Dado um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, nosso primeiro objetivo será determinar o grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$, o qual denotamos por G_n. Posteriormente, indicamos em quais situações G_n é um grupo cíclico, e apresentamos propriedades para estes casos.

Para σ em G_n arbitrário, temos:

$$\sigma\left(\sum a_i\zeta_n^i\right) = \sum \sigma(a_i\zeta_n^i) = \sum \sigma(a_i)\sigma(\zeta_n^i) = \sum a_i\sigma(\zeta_n)^i.$$

Consequentemente, conhecer $\sigma(\zeta_n)$ é suficiente para determinamos o grupo de Galois desejado.

Da Observação 1.8.2 temos que $\sigma(\zeta_n)$ é raiz do n-ésimo polinômio ciclotômico. Além disso, mostramos que as raízes de $\Phi_n(X)$ são os ζ_n^j onde $mdc(j,n)=1$. Portanto, $\sigma(\zeta_n)=\zeta_n^j$ para algum j, tal que, $mdc(j,n)=1$. Definindo $\sigma_j(\zeta_n)=\zeta_n^j$ para cada j que cumpra $mdc(j,n)=1$ segue que, $G_n=\{\sigma_j;\ j=1,2,\cdots,n;\ mdc(j,n)=1\}$. Vale ressaltar que $o(G_n)=\varphi(n)$.

Teorema 3.1.1. *([8], pág: 39) Sejam $n\in\mathbb{N}$ e G_n o grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$. Então, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \approx G_n$. O referido isomomorfismo é o isomomorfismo natural, que associa $\overline{j}$ a σ_j.*

Isto posto, pelo Teorema Fundamental da Teoria de Galois, Teorema 1.8.7, os subcorpos $\mathbb{K}$ de $\mathbb{Q}(\zeta_n)$ estão em bijeção com os subgrupos H de $(\mathbb{Z}/n\mathbb{Z})^*$, além disso, pelo mesmo Teorema, temos que uma extensão é galoisiana se o grupo de Galois correspondente é um subgrupo normal de G. Mais ainda, sabemos que todo grupo cíclico é abeliano, e todo subgrupo de um grupo abeliano é normal.

O próximo resultado nos garante quando o grupo de Galois, de uma extensão $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$, é cíclico, lembrando que, neste caso, todo subgrupo é cíclico. Sua demonstração será omitida mas, pode ser encontrada na referência citada.

Teorema 3.1.2. *([8], pág: 44) O grupo $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ é cíclico se, e somente se, $n=2,4,\ p^r$ ou $2p^r$, onde p é um primo ímpar e $r\geqslant 1$.*

O seguinte resultado nos informa a quantidade de subgrupos, que um grupo cíclico contém.

Teorema 3.1.3. *([9], pág: 28) Se G é um grupo cíclico de ordem n, então existe um único subgrupo de ordem d para cada divisor d de n.*

Demonstração. Seja $G=<a>$ assim, $a^n=1$. Note que o subgrupo gerado por $a^{\frac{n}{d}}$ tem ordem d pois, $\left(a^{\frac{n}{d}}\right)^d=a^n=1$.

Seja $H=<b>$ um subgrupo de G de ordem d, assim, $b^d=1$. Além disso, como b é, em particular, elemento de G, segue que $b=a^m$ para algum $m\in\mathbb{Z}$.

Portanto, temos que $1=b^d=(a^m)^d$ e $a^n=1$, isto implica que md é um multiplo de n, ou seja, existe um inteiro k tal que $md=nk$ e assim, $b=a^m=\left(a^{\frac{n}{d}}\right)^k$.

Logo, o grupo gerado por b, $<b>$ é subgrupo do grupo gerado por $<a^{\frac{n}{d}}>$. Mais ainda, estes grupos coincidem pois possuem a mesma ordem. Donde, existe um único subgrupo de ordem d para cada divisor de n. □

Proposição 3.1.4. *Sejam G um grupo cíclico de ordem n e d um divisor de n então, o subgrupo H de G, de ordem $c=\frac{n}{d}$ é o conjunto de todos os elementos $b\in G=<a>$ tais que $b^d=1$, isto é, $H=<a^d>$.*

Demonstração. Primeiramente, observe que, se d é um divisor de n então, $c = \frac{n}{d}$, logo, $d = \frac{n}{c}$ e portanto, c é um divisor de n assim, pelo Teorema anterior, existe um único subgrupo H de ordem c.

Suponha que H tenha ordem c, e considere $b \in H$ então, $b = a^{k \cdot c}$. Logo,

$$b^d = \left(a^{k \cdot c}\right)^d = \left(a^k\right)^n = 1.$$

Suponha agora que $b = a^m$ e $b^d = 1$. Assim, $a^{md} = 1$ e consequentemente, $m \cdot d = k \cdot n$. Portanto, $m = k \cdot \frac{n}{d} = k \cdot c$, donde, $b = (a^c)^k \in H$. □

3.2 Base Integral Normal e Discriminante

No primeiro capítulo definimos base integral e discriminante de um corpo, agora, apresentaremos um caso particular do primeiro conceito, a denominada base integral normal, e exibiremos um resultado que auxilia o cálculo do discriminante, válido para corpos de números abelianos. Por fim, aplicaremos o referido resultado em subcorpos reais maximais de corpos ciclotômicos de grau 8.

Definição 3.2.1. *Seja $\mathbb{K}/\mathbb{Q}$ uma extensão galoisiana finita, com*

$$Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_n\}.$$

Se existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\{\sigma_1(\alpha), \cdots, \sigma_n(\alpha)\}$ é uma base integral de $\mathbb{K}$, então ela é dita uma base integral normal de $\mathbb{K}$. O elemento α é dito um gerador dessa base.

Teorema 3.2.2. *Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_n)$, com n livre de quadrados, $[\mathbb{K} : \mathbb{Q}] = r$ e $Gal(\mathbb{K}/\mathbb{Q}) = \{\theta_1, \cdots, \theta_r\}$, então*

$$\{\theta_1(t), \cdots, \theta_r(t)\}$$

é uma base integral normal de $\mathbb{K}$, cujo gerador é $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$.

Neste momento, exibiremos o principal resultado desta seção, para isto, a seguinte definição é fundamental.

Definição 3.2.3. *Seja $\mathbb{K}$ um corpo de números abeliano. Definimos como condutor de $\mathbb{K}$, o menor inteiro m tal que, o m-ésimo corpo ciclotômico contém $\mathbb{K}$.*

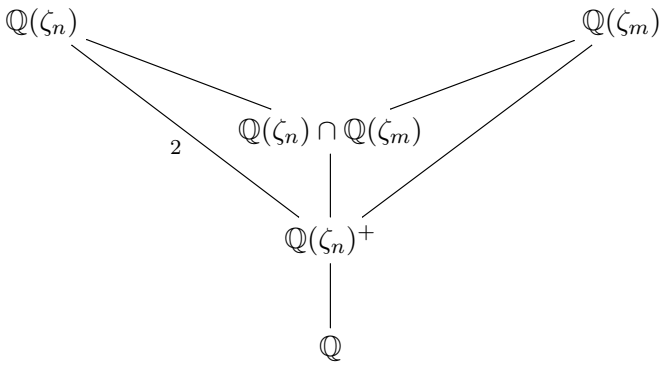
Teorema 3.2.4. *([2], pág: 39) Seja $\mathbb{K}$ um corpo de números abeliano de condutor $m = \prod_{i=1}^{s} p_i^{a_i}$, p_i's primos e a_i's $\in \mathbb{N}$. Então, o discriminante de $\mathbb{K}$ é dado por:*

$$|Disc(\mathbb{K})| = \begin{cases} \left(\dfrac{m}{\prod_{i=1}^{s} p_i^{\frac{p_i^{a_i-1}-1+\frac{p_i-1}{u_i}}{p_i^{a_i-1}(p_i-1)}}} \right)^{[\mathbb{K}:\mathbb{Q}]} & \text{se } m \neq 2^n,\ \forall n \in \mathbb{N}; \\ 2^{(n-1)2^{n-1}} & \text{se } \mathbb{K} = \mathbb{Q}(\zeta_{2^n}); \\ 2^{n2^{n-1}-1} & \text{se } m = 2^{n+1} \text{ para algum } n \in \mathbb{N} \text{ mas } \mathbb{K} \neq \mathbb{Q}(\zeta_{2^{n+1}}), \end{cases}$$

onde, $u_i = [\mathbb{K} \cdot \mathbb{Q}(\zeta_{m/p_i^{a_i}}) : \mathbb{Q}(\zeta_{m/p_i^{a_i}})]/p_i^{a_i-1}$.

Agora, usando o Teorema 3.2.4, calcularemos o discriminante dos subcorpos reais maximais de corpos ciclotômicos de grau 8.

Consideremos n e m números naturais, de modo que $\mathbb{Q}(\zeta_n)^+ \subset \mathbb{Q}(\zeta_m)$, temos portanto o seguinte diagrama:



Assim, temos duas possibilidades a considerar: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)] = 1$ ou 2. Se tivermos a segunda condição, então $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$, o que é um absurdo pois, pelo Lema 2.5.6, $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d)$, onde d é o máximo divisor comum entre m e n, em particular é um corpo ciclotômico, portanto não é totalmente real. Segue então que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)] = 1$, ou seja, $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$. Donde, n é o condutor de $\mathbb{K}$.

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{15})^+$ então m, o condutor de $\mathbb{K}$, é $15 = 3 \cdot 5$, logo

$$|Disc(\mathbb{K})| = \left(\frac{15}{3^{\frac{3^{1-1}-1+\frac{3-1}{u_1}}{3^{1-1}(3-1)}} \cdot 5^{\frac{5^{1-1}-1+\frac{5-1}{u_2}}{5^{1-1}(5-1)}}} \right)^4$$

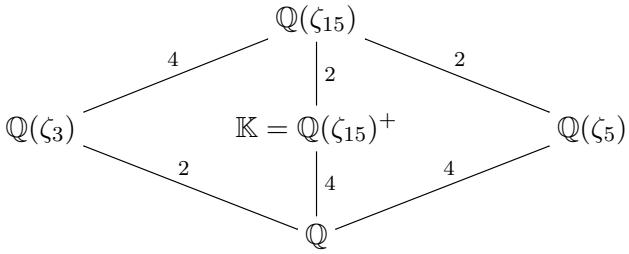
$$= \left(\frac{15}{3^{\frac{\frac{2}{u_1}}{2}} \cdot 5^{\frac{\frac{4}{u_2}}{4}}}\right)^4 = \left(\frac{15}{3^{\frac{1}{u_1}} \cdot 5^{\frac{1}{u_2}}}\right)^4$$

Precisamos calcular u_1 e u_2,

$$u_1 = [\mathbb{K} \cdot \mathbb{Q}(\zeta_{\frac{15}{3}}) : \mathbb{Q}(\zeta_{\frac{15}{3}})] = [\mathbb{K} \cdot \mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5)]$$

$$u_2 = [\mathbb{K} \cdot \mathbb{Q}(\zeta_{\frac{15}{5}}) : \mathbb{Q}(\zeta_{\frac{15}{5}})] = [\mathbb{K} \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}(\zeta_3)]$$

Temos portanto o seguinte diagrama:



Além disso, $\mathbb{K} \cdot \mathbb{Q}(\zeta_5)$ é o menor corpo que contem $\mathbb{K}$ e $\mathbb{Q}(\zeta_5)$. Sabemos que $\mathbb{Q}(\zeta_{15})$ contém ambos os corpos em questão, portanto o grau de $\mathbb{K} \cdot \mathbb{Q}(\zeta_5)$ sobre $\mathbb{Q}(\zeta_5)$ é menor ou igual a 2, isto é, pela multiplicidade de graus, temos duas hipóteses a considerar: $[\mathbb{K} \cdot \mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5)] = 1$ ou 2. Se a primeira opção for verdadeira, temos que $\mathbb{K} = \mathbb{Q}(\zeta_5)$ e isso é um absurdo, pois $\mathbb{K}$ é totalmente real e $\mathbb{Q}(\zeta_5)$ não. Donde, $u_1 = [\mathbb{K} \cdot \mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5)] = 2$.

Analogamente, $[\mathbb{K} \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}(\zeta_3)] = 1, 2$ ou 4. Suponha que $[\mathbb{K} \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}(\zeta_3)] = 1$ então, $\mathbb{K} \subset \mathbb{Q}(\zeta_3)$ absurdo, pois $[\mathbb{K} : \mathbb{Q}] = 4$ e $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. Agora, suponha que $[\mathbb{K} \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}(\zeta_3)] = 2$ então, $[\mathbb{Q}(\zeta_{15}) : \mathbb{K} \cdot \mathbb{Q}(\zeta_3)] = [\mathbb{Q}(\zeta_{15}) : \mathbb{K}] = 2$, e como $\mathbb{K} \subset \mathbb{K} \cdot \mathbb{Q}(\zeta_3)$, segue que $\mathbb{K} = \mathbb{K} \cdot \mathbb{Q}(\zeta_3)$, consequentemente, $\mathbb{Q}(\zeta_3) \subset \mathbb{K}$, o que é um absurdo pois $\mathbb{K}$ é totalmente real e $\mathbb{Q}(\zeta_3)$ não. Donde, $u_2 = [\mathbb{K} \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}(\zeta_3)] = 4$.

Portanto,

$$|Disc(\mathbb{K})| = \left(\frac{15}{3^{\frac{1}{2}} \cdot 5^{\frac{1}{4}}}\right)^4 = \frac{3^4 \cdot 5^4}{3^2 \cdot 5} = 3^2 \cdot 5^3.$$

Considere $\mathbb{K} = \mathbb{Q}(\zeta_{16})^+$ então m, o condutor de $\mathbb{K}$, é $16 = 2^4 = 2^{3+1}$, mas $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^4})$, portanto pelo Teorema 3.2.4, temos:

$$Disc(\mathbb{K}) = 2^{3\cdot 2^2-1} = 2^{11}$$

Suponha $\mathbb{K} = \mathbb{Q}(\zeta_{20})^+$ então m, o condutor de $\mathbb{K}$, é $20 = 2^2 \cdot 5$, pelo Teorema 3.2.4, temos:

$$\begin{aligned} |Disc(\mathbb{K})| &= \left(\frac{20}{2^{\frac{1+\frac{1}{u_1}}{2}} \cdot 5^{\frac{\frac{4}{u_2}}{4}}} \right)^4 \\ &= \left(\frac{20}{2^{\frac{1+\frac{1}{u_1}}{2}} \cdot 5^{\frac{1}{u_2}}} \right)^4, \end{aligned}$$

onde, procedendo de maneira analoga a feita no primeiro caso, $u_1 = \frac{[\mathbb{K}\cdot\mathbb{Q}(\zeta_5):\mathbb{Q}(\zeta_5)]}{2} = \frac{2}{2} = 1$ e $u_2 = \frac{[\mathbb{K}\cdot\mathbb{Q}(\zeta_4):\mathbb{Q}(\zeta_4)]}{1} = 4$. Consequentemente,

$$|Disc(\mathbb{K})| = \frac{(2^2)^4 \cdot 5^4}{2^4 \cdot 5} = 2^4 \cdot 5^3.$$

Escolha agora, $\mathbb{K} = \mathbb{Q}(\zeta_{24})^+$ então, o condutor de $\mathbb{K}$ é $24 = 2^3 \cdot 3$. Segue do Teorema 3.2.4 que:

$$\begin{aligned} |Disc(\mathbb{K})| &= \left(\frac{24}{2^{\frac{3+\frac{1}{u_1}}{4}} \cdot 3^{\frac{\frac{2}{u_2}}{2}}} \right)^4 \\ &= \left(\frac{24}{2^{\frac{3+\frac{1}{u_1}}{4}} \cdot 3^{\frac{1}{u_2}}} \right)^4, \end{aligned}$$

no qual, $u_1 = \frac{[\mathbb{K}\cdot\mathbb{Q}(\zeta_3):\mathbb{Q}(\zeta_3)]}{4} = \frac{4}{4} = 1$ e $u_2 = \frac{[\mathbb{K}\cdot\mathbb{Q}(\zeta_8):\mathbb{Q}(\zeta_8)]}{1} = 2$. Consequentemente,

$$|Disc(\mathbb{K})| = \frac{(2^3)^4 \cdot 3^4}{2^4 \cdot 3^2} = 2^8 \cdot 3^2.$$

Por fim, tome $\mathbb{K} = \mathbb{Q}(\zeta_{30})^+$. Devemos nos atentar para o fato de que 30 não é o condutor de $\mathbb{K}$. Isto se deve pois, $\mathbb{Q}(\zeta_{30}) = \mathbb{Q}(\zeta_{15})$ e portanto, $\mathbb{K} = \mathbb{Q}(\zeta_{30})^+ = \mathbb{Q}(\zeta_{15})^+$, o qual tem condutor igual

a 15, e assim:

$$|Disc(\mathbb{K})| = 3^2 \cdot 5^3.$$

Vamos mostrar o caso geral da afirmação feita anteriormente, $\mathbb{Q}(\zeta_{30}) = \mathbb{Q}(\zeta_{15})$. Isto é, dado n um número natural ímpar então, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$. Primeiramente, vamos verificar qual é o menor número natural k tal que, $(-\zeta_n)^k = 1$, isto é, $(-1)^k \cdot \zeta_n^k = 1$. Sabendo que, $\zeta_n^k = \cos\frac{2k\pi}{n} + i\,\mathrm{sen}\,\frac{2k\pi}{n}$, para que $\zeta_n^k = 1$ é necessário que k seja um múltiplo de n, pois neste caso, temos $i\,\mathrm{sen}\,\frac{2k\pi}{n} = i\,\mathrm{sen}\,k'\pi = 0$. Assim, $k = n \cdot t$, onde t é o menor número natural possível que cumpre $(-1)^k \cdot \zeta_n^k = 1$.

- Se $t = 1$ então, $k = n$ ímpar e assim, $(-1)^k \cdot \zeta_n^k = (-1)^n \cdot \zeta_n^n = -1 \cdot 1 = -1 \neq 1$.
- Se $t = 2$ então, $k = 2n$ e assim, $(-1)^k \cdot \zeta_n^k = (-1)^2 n \cdot (\zeta_n^n)^2 = 1$.

Sendo assim, $k = 2n$. Sabemos também que $k = 2n$ é o menor natural que cumpre $\zeta_{2n}^k = 1$, portanto ambos são raízes do polinômio $X^k - 1$, donde, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(-\zeta_n) = \mathbb{Q}(\zeta_{2n})$.

3.3 Corpos Abelianos de Condutor Primo

Nesta seção, com o objetivo de estudar os corpos abelianos de condutor primo, explicitaremos uma base integral normal para um p-ésimo corpo ciclotômico e seus subcorpos, apresentaremos uma forma de representar os referidos subcorpos, estudaremos quando estes são totalmente reais ou totalmente imaginários, além de apresentar e minimizar sua forma quadrática. Posteriormente, aplicaremos os resultados obtidos para os corpos $\mathbb{Q}(\zeta_7)$ e $\mathbb{Q}(\zeta_{17})$.

Iniciaremos determinando uma base integral normal para os p-ésimos corpos ciclotômicos e, em seguida, faremos o mesmo para seus subcorpos.

Considere p um número primo e $\mathbb{L} = \mathbb{Q}(\zeta_p)$, vimos que $Gal(\mathbb{L}/\mathbb{Q}) \approx (\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \cdots \overline{p-1}\}$ assim, aplicando o Teorema 3.2.2, temos que o gerador da base integral de $\mathbb{L}$ é dado por:

$$Tr_{\mathbb{L}/\mathbb{L}}(\zeta_p) = \zeta_p$$

Portanto, $\{\sigma_1(\zeta_p), \sigma_2(\zeta_p), \cdots, \sigma_{p-1}(\zeta_p)\} = \{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$ constitui uma base integral normal de $\mathbb{Q}(\zeta_p)$.

Usando a notação já adotada, $G_p = Gal(\mathbb{L}/\mathbb{Q}) \approx (\mathbb{Z}/p\mathbb{Z})^*$, G_p é cíclico como visto no Teorema 3.1.2. Pelo Teorema 3.1.3, para cada divisor d de $p-1$, existe um único subgrupo H de G, de maneira que $[G : H] = d$, consequentemente, da Teoria de Galois, existe um único subcorpo $\mathbb{K}$ de $\mathbb{L}$, tal que $\mathbb{K} = \mathbb{L}^H$ de grau d sobre $\mathbb{Q}$. Em forma de diagrama temos:

$$\begin{array}{ccc} \mathbb{L}=\mathbb{Q}(\zeta_p) & \text{---} & \{Id\} \\ {\scriptstyle \frac{p-1}{d}}\big| & & \big| \\ \mathbb{K} & \text{---} & H \\ {\scriptstyle d}\big| & & \big|{\scriptstyle d} \\ \mathbb{Q} & \text{---} & G_p \end{array}$$

Uma vez que G_p é cíclico, podemos supor $G_p =< \sigma >$, para algum $\sigma \in G$, usando a Proposição 3.1.4, $H =< \sigma^d >$, assim

$$H = Gal(\mathbb{L}/\mathbb{K}) = \{\sigma^d, \sigma^{2d}, \cdots, \sigma^{\frac{p-1}{d}d}\} = \left\{\sigma^d, \left(\sigma^d\right)^2, \cdots, \left(\sigma^d\right)^{\frac{p-1}{d}} = Id\right\}.$$

Explicitaremos uma base integral normal de $\mathbb{K}$, para isto, observe que podemos reescrever G_p da seguinte maneira:

$$\begin{aligned} G_p &= H \cup \sigma H \cup \sigma^2 H \cup \cdots \cup \sigma^{d-1} H = \\ &= \{\sigma^d, \sigma^{2d}, \cdots, \sigma^{\frac{p-1}{d}d}, \sigma^{1+d}, \sigma^{1+2d}, \cdots, \sigma^{1+\frac{p-1}{d}d}, \cdots, \\ &\quad \sigma^{d-1+d}, \sigma^{d-1+2d}, \cdots, \sigma^{d-1+\frac{p-1}{d}d}\}. \end{aligned}$$

Seja $x \in \mathcal{O}_{\mathbb{K}}$, então, $x \in \mathcal{O}_{\mathbb{L}}$ e $x \in \mathbb{K}$. Consideremos a seguinte base integral normal de $\mathbb{L}$, $\mathcal{B} = \{\sigma^1(\zeta_p), \sigma^2(\zeta_p), \cdots, \sigma^{p-1}(\zeta_p)\}$, assim,

$$x = a_1\sigma^1(\zeta_p) + \cdots + a_{p-1}\sigma^{p-1}(\zeta_p),$$

reordenando as parcelas, tem-se:

$$\begin{aligned} x &= a_d\sigma^d(\zeta_p) + a_{2d}\sigma^{2d}(\zeta_p) + \cdots + a_{\frac{p-1}{d}}\sigma^{\frac{p-1}{d}}(\zeta_p) + a_{1+d}\sigma^{1+d}(\zeta_p) + a_{1+2d}\sigma^{1+2d}(\zeta_p) + \cdots + \\ &\quad + a_{1+\frac{p-1}{d}}\sigma^{1+\frac{p-1}{d}}(\zeta_p) + \cdots + a_{d-1+d}\sigma^{d-1+d}(\zeta_p) + \\ &\quad + a_{d-1+2d}\sigma^{d-1+2d}(\zeta_p) + \cdots + a_{d-1+\frac{p-1}{d}}\sigma^{d-1+\frac{p-1}{d}}(\zeta_p) \end{aligned}$$

Além disso, sabemos que $y \in \mathbb{K}$ se, e somente se, $\sigma(y) = y$, para todo $\sigma \in H$. Assim,

$$\begin{aligned} x &= \sigma^d(x) = a_{\frac{p-1}{d}}\sigma^d(\zeta_p) + a_d\sigma^{2d}(\zeta_p) + \cdots + a_{\frac{p-1}{d}-1}\sigma^{\frac{p-1}{d}}(\zeta_p) + a_{1+\frac{p-1}{d}}\sigma^{1+d}(\zeta_p) + \\ &\quad + a_{1+d}\sigma^{1+2d}(\zeta_p) + \cdots + a_{1+\frac{p-1}{d}-1}\sigma^{1+\frac{p-1}{d}}(\zeta_p) + \cdots + a_{d-1+\frac{p-1}{d}}\sigma^{d-1+d}(\zeta_p) + \\ &\quad + a_{d-1+d}\sigma^{d-1+2d}(\zeta_p) + \cdots + a_{d-1+\frac{p-1}{d}-1}\sigma^{d-1+\frac{p-1}{d}}(\zeta_p) \end{aligned}$$

Consequentemente, temos:

$$\begin{aligned}
a_d &= a_{2d} = \cdots = a_{\frac{p-1}{d}-1} = a_{\frac{p-1}{d}} \\
a_{1+d} &= a_{1+2d} = \cdots = a_{1+\frac{p-1}{d}-1} = a_{1+\frac{p-1}{d}} \\
\vdots &= \vdots \qquad\qquad \ddots \qquad\qquad \vdots \\
a_{d-1+d} &= a_{d-1+2d} = \cdots = a_{d-1+\frac{p-1}{d}-1} = a_{d-1+\frac{p-1}{d}}
\end{aligned}$$

Donde, colocando os termos comuns em evidência, temos:

$$x = a_d t_{\mathbb{K}} + a_{1+d}\sigma(t_{\mathbb{K}}) + \cdots + a_{d-1+d}\sigma^{d-1}(t_{\mathbb{K}}),$$

E assim, $\{t_{\mathbb{K}}, \sigma(t_{\mathbb{K}}), \cdots, \sigma^{d-1}(t_{\mathbb{K}})\}$ constitui uma base integral normal de $\mathbb{K}$.

Vale ressaltar que

$$t_{\mathbb{K}} = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p) = \sum_{i=1}^{\frac{p-1}{d}} \left(\sigma^d\right)^i (\zeta_p)$$

é o gerador da base integral normal de $\mathbb{K}$, conforme o Teorema 3.2.2.

Note que, determinamos a base integral normal de um corpo abeliano de condutor primo, sem explicitar tal corpo, isto será nosso próximo objetivo, mostrar que $\mathbb{K} = \mathbb{Q}(t_{\mathbb{K}})$.

Dado que $Tr_{\mathbb{L}/\mathbb{K}}(x) \in \mathbb{K}$, para todo $x \in \mathbb{L}$, então, $\mathbb{Q}(Tr_{\mathbb{L}/\mathbb{K}}(x)) \subset \mathbb{K}$, em particular, para $x = \zeta_p$, temos:

$$\begin{array}{c}
\mathbb{L} = \mathbb{Q}(\zeta_p) \\
| \\
\mathbb{K} \\
| \\
v \\
| \\
\mathbb{Q}(t_{\mathbb{K}}) \\
| \\
\mathbb{Q}
\end{array}$$

Além disso,

$$\begin{aligned}
-1 &= Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p) = Tr_{\mathbb{K}/\mathbb{Q}}\left(Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)\right) = \\
&= Tr_{\mathbb{Q}(t_{\mathbb{K}})/\mathbb{Q}}\left(Tr_{\mathbb{K}/\mathbb{Q}(t_{\mathbb{K}})}\left(Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)\right)\right) = \\
&= Tr_{\mathbb{Q}(t_{\mathbb{K}})/\mathbb{Q}}\left(Tr_{\mathbb{K}/\mathbb{Q}(t_{\mathbb{K}})}(t_{\mathbb{K}})\right) =
\end{aligned}$$

$$= \quad vTr_{\mathbb{Q}(t_{\mathbb{K}})/\mathbb{Q}}(t_{\mathbb{K}})$$

como o grau de uma extensão é sempre positivo e $Tr_{\mathbb{Q}(t_{\mathbb{K}})/\mathbb{Q}}(t_{\mathbb{K}}) \in \mathbb{Z}$, segue que $v = 1$ e $Tr_{\mathbb{Q}(t_{\mathbb{K}})/\mathbb{Q}}(t_{\mathbb{K}}) = -1$. Donde, $[\mathbb{K} : \mathbb{Q}(t_{\mathbb{K}})] = 1$ e, portanto, $\mathbb{K} = \mathbb{Q}(t_{\mathbb{K}})$.

Sabemos que, se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana então, $\mathbb{K}$ é totalmente real ou totalmente imaginário. Nosso objetivo portanto, será determinar em quais casos $\mathbb{K}$ é totalmente real ou totalmente imaginário.

Visto que $G_p = Gal(\mathbb{L}/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ é cíclico, para cada d_i, divisor de $o(G_p) = p-1$, existe um único subgrupo H_i de G_p tal que, $o(H_i) = d_i$. Além disso, pela Teoria de Galois, existe um subcorpo $\mathbb{K}_i$ de $\mathbb{L}$, $\mathbb{K}_i$ fixado por H_i, tal que $[\mathbb{L} : \mathbb{K}_i] = d_i$

Uma vez que, todo primo diferente de 2 é ímpar, temos $p-1$ par, assim, 2 é um divisor de $p-1$. Isto posto, existe um único subgrupo H_2 de G_p tal que, $o(H_2) = 2$. Além disso, o sugbrupo de G_p formado pela identidade e conjugação complexa, $\{\sigma_1, \sigma_{p-1}\}$, é um subgrupo de ordem 2, assim, pela unicidade da existência de um subgrupo de G_p de ordem 2, segue que, $H_2 = \{\sigma_1, \sigma_{p-1}\}$. Observe que, o subcorpo fixado por H_2 é constituido por todos os elementos reais de $\mathbb{L}$, à este subcorpo denominamos subcorpo real maximal de $\mathbb{L}$, o qual denotamos por $\mathbb{L}^+$, a partir de agora, denotaremos H_2 por H^+, em forma de diagrama temos:

$$\begin{array}{ccc} \mathbb{L} & \text{——} & \{Id\} \\ {\scriptstyle 2}\big| & & \big| \\ \mathbb{L}^+ & \text{——} & H^+ \\ {\scriptstyle \frac{p-1}{2}}\big| & & \big| \\ \mathbb{Q} & \text{——} & G \end{array}$$

Para os outros divisores d_i de $p-1$, existe um único subgrupo H_i de G_p de ordem d_i, denotemos por c_i o índice de H_i em G_p. Assim, se c_i divide $\frac{p-1}{2}$ então, H_i está contido em H^+, caso contrário, se c_i não divide $\frac{p-1}{2}$ temos que, H_i não está contido em H^+ e portanto, o subcorpo $\mathbb{K}_i$, fixado por H_i é totalmente imaginário. Donde, temos o seguinte:

Teorema 3.3.1. *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_p)$, p primo, $\mathbb{K}$ um subcorpo de $\mathbb{L}$ e $H = Gal(\mathbb{L}/\mathbb{K})$ então, $\mathbb{K}$ é totalmente real se, e somente se, o índice de H divide $\frac{p-1}{2}$.*

Todo corpo ciclotômico possui, pelo menos um subcorpo totalmente real, como o foco deste trabalho são os subcorpos reais, estaremos interessados em saber para quais números primos p, $\mathbb{L} = \mathbb{Q}(\zeta_p)$ possui apenas subcorpos próprios reais. Observe que, para isto ocorrer, $[\mathbb{L} : \mathbb{Q}] = p - 1$ deve ser uma potência de 2, isto é, $p = 2^{2^n} + 1$, $n \in \mathbb{N}$, tal número é conhecido como primo de Fermat, faremos uma breve explicação de tais números.

Um número de Fermat é um número inteiro positivo que assume a forma:

$$F_n = 2^{2^n} + 1$$

Pierre Fermat acreditou que os números que podiam ser escritos nessa forma eram primos e, apresentou tal conjectura à Marin Mersenne. No entanto, Leonard Euler, em 1732, provou que tal conjectura era falsa pois, considerando $n = 5$, temos:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$$

O problema de encontrar números primos de Fermat é um dos problemas matemáticos em aberto até os dias de hoje, são conhecidos cinco números primos de Fermat, e não se sabe se há mais ou não, tais números são:

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3 \\ F_1 &= 2^{2^1} + 1 = 5 \\ F_2 &= 2^{2^2} + 1 = 17 \\ F_3 &= 2^{2^3} + 1 = 257 \\ F_4 &= 2^{2^4} + 1 = 65537 \end{aligned}$$

Os números de Fermat de ordem 5 até 32 são comprovadamente compostos, além de outros casos que podem ser encontrados em: <http://www.prothsearch.net/fermat.html>.

Mais adiante, abordaremos $\mathbb{Q}(\zeta_p)$, considerando $p = 17$, que é um dos primos de Fermat.

3.3.1 Forma Quadrática para Corpos Abelianos de Condutor Primo

Com o objetivo de determinarmos reticulados a partir de corpos abelianos de condutor primo, explicitaremos sua forma quadrática. Do mesmo modo que construimos a seção anterior, primeiro explicitando os resultados para $\mathbb{L} = \mathbb{Q}(\zeta_p)$ e posteriormente adapatando-os para seus subcorpos, o faremos nesta seção.

Conforme apresentado na seção 2.3, consideremos o homomorfismo de Minkowski $\sigma_{\mathbb{L}} : \mathbb{L} \longrightarrow \mathbb{R}^{p-1}$, que associa a cada $x \in \mathbb{L}$ à sua imagem $\sigma_{\mathbb{L}}(x)$, assim:

$$|\sigma_{\mathbb{L}}(x)|^2 = \frac{1}{2}\, Tr_{\mathbb{L}/\mathbb{Q}}\, x\overline{x},$$

Além disso, podemos escrever x e $\overline{x}$ como combinação linear dos elementos de

$\mathcal{B} = \{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$, base integral de $\mathbb{L}$, assim:

$$\begin{aligned} x &= x_0 + x_1\zeta_p + x_2\zeta_p^2 + \cdots + x_{p-2}\zeta_p^{p-2} \\ \overline{x} &= x_0 + x_1\zeta_p^{-1} + x_2\zeta_p^{-2} + \cdots + x_{p-2}\zeta_p^{-(p-2)} \end{aligned}$$

Assim,

$$\begin{aligned} x\overline{x} &= x_0^2 + x_1^2 + \cdots + x_{p-2}^2 + \left(\zeta_p + \zeta_p^{-1}\right)(x_0x_1 + x_1x_2 + \cdots + x_{p-3}x_{p-2}) + \\ &\quad + \left(\zeta_p^2 + \zeta_p^{-2}\right)(x_0x_2 + x_1x_3 + \cdots + x_{p-4}x_{p-2}) + \cdots + \left(\zeta_p^{p-2} + \zeta_p^{-(p-2)}\right)x_0x_{p-2}. \end{aligned}$$

Logo,

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}\ x\overline{x} &= (p-1)(x_0^2 + x_1^2 + \cdots + x_{p-2}^2) - 2\sum_{0\le i<j\le p-2} x_ix_j \\ &= p\sum_{i=0}^{p-2} x_i^2 - \left(\sum_{i=0}^{p-2} x_i^2 + 2\sum_{i<j} x_ix_j\right) \\ &= p\sum_{i=0}^{p-2} x_i^2 - \left(\sum_{i=0}^{p-2} x_i\right)^2. \end{aligned}$$

Donde,

$$Tr_{\mathbb{L}/\mathbb{Q}}\ x\overline{x} = p\sum_{i=0}^{p-2} x_i^2 - \left(\sum_{i=0}^{p-2} x_i\right)^2. \tag{3.1}$$

Nosso objetivo agora, será minimizar a forma quadrática acima. Para isto, faremos a seguinte identificação:

$$x = x_0 + x_1\zeta_p + x_2\zeta_p^2 + \cdots + x_{p-2}\zeta_p^{p-2} \sim (x_0, x_1, \cdots, x_{p-2}).$$

Observação 3.3.2. *Se subtrairmos uma unidade de algum elemento da $(p-1)$-upla e a adicionarmos em outro elemento, a parcela $\left(\sum_{i=0}^{p-2} x_i\right)^2$ não se altera.*

Analisaremos então, quando esta troca é conveniente, isto é, quando esta troca torna a parcela $\sum_{i=0}^{p-2} x_i^2$ menor, simbolicamente:

$$\sum_{i=0}^{p-2} x_i^2 \ge x_0^2 + \cdots + (x_i - 1)^2 + \cdots + (x_j + 1)^2 + \cdots x_{p-2}^2.$$

Equivalentemente,

$$x_i^2 + x_j^2 \ \ge\ (x_i - 1)^2 + (x_j + 1)^2 = x_i^2 - 2x_i + 1 + x_j^2 + 2x_j + 1$$

$$\begin{aligned} 2(x_i - x_j) &\geq 2 \\ x_i &\geq x_j + 1 \end{aligned}$$

Isto posto, tal mudança será conveniente se, e somente se, $x_i \geq x_j + 1$.

Agora, consideremos $\sum_{i=0}^{p-2} x_i = k$, $k > 0$, e façamos todas as trocas convenientes possíveis, conforme a Observação 3.3.2. Reordenando a $(p-1)$-upla, se necessário, temos:

$$(\underbrace{u+1, \cdots, u+1}_{r \text{ vezes}}, u, \cdots, u),$$

onde $k = (p-1)u + r$, $0 \leq r \leq p-2$. Donde,

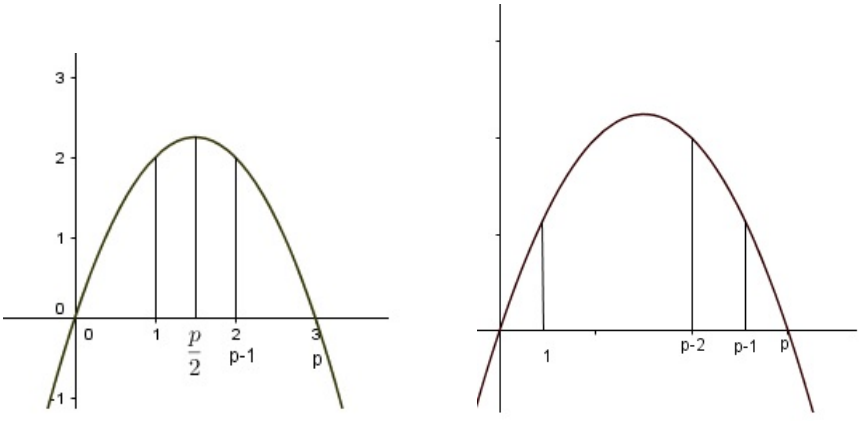
$$\begin{aligned} p\sum_{i=0}^{p-2} x_i^2 - \left(\sum_{i=0}^{p-2} x_i\right)^2 &= p\left(r(u+1)^2 + (p-1-r)u^2\right) - ((p-1)u + r)^2 \\ &= p\left(ru + 2ru + r + (p-1)u^2 - ru^2\right) - (p-1)^2u^2 - 2(p-1)ur - r^2 \\ &= (p-1)u^2 + r(p + 2u - r) \end{aligned}$$

Portanto, nosso objetivo é minimizar a função nas variáveis u e r:

$$\mathbf{Q} = (p-1)u^2 + r(p + 2u - r),$$

onde, $\sum x_i = (p-1)u + r$, $r = 0, 1, \cdots, p-2$.

Note que, se fixarmos o resto r, $\mathbf{Q}$ é uma função crescente na variável u. Portanto, para minimizá-la escolhemos o menor valor que u pode assumir, isto é, escolhemos $u = 0$, assim, $\mathbf{Q}_0 = rp - r^2$, e temos as seguintes possibilidades para r: $0, 1, \cdots, p-2$. Graficamente, temos a seguinte situação, primeiramente considerando $p = 3$ e posteriormente para p qualquer:



Note que, tal gráfico é simétrico, atinge sua imagem máxima em $\frac{p}{2}$ e sua imagem minima, diferente de zero, em 1 e $p-1$, como r é estritamente menor que $p-1$, segue que o menor valor da função é atingido quando $r=1$. Portanto, o menor valor que a forma quadrática 3.1 assume é atingido quando temos $\sum_{i=0}^{p-2} x_i = (p-1)u + r = 1$, isto é, temos uma $(p-1)$-upla que contém um elemento igual a 1 e os demais iguais a 0, e neste caso, a forma quadrática vale $p-1$. Sendo assim, $\min\{Tr_{\mathbb{L}/\mathbb{Q}}\ x\overline{x}\} = p-1$.

Observe que, se $\sum_{i=0}^{p-2} x_i = 0$, $Tr_{\mathbb{L}/\mathbb{Q}}\ x\overline{x} = p\sum_{i=0}^{p-2} x_i^2 - \left(\sum_{i=0}^{p-2} x_i\right)^2 = p\sum_{i=0}^{p-2} x_i^2$ e assim, o mínimo ocorre quando $x_i = 1$ e $x_j = -1$ para algum $i, j \in \{0, \cdots, p-2\}$, assim, $\min\{Tr_{\mathbb{L}/\mathbb{Q}}\ x\overline{x}\} = 2p$.

Procederemos de modo análogo aos subcorpos $\mathbb{K}$ de $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Seja $y \in \mathbb{K}$, escrevendo-o como combinação linear dos elementos da base integral normal de $\mathbb{K}$, temos:

$$y = y_1 t + y_2\sigma(t) + \cdots + y_{d-1}\sigma^{d-1}(t)$$

Além disso,

$$\begin{aligned}
Tr_{\mathbb{L}/\mathbb{Q}} y\overline{y} &= p\sum_{i=0}^{p-2} x_i^2 - \left(\sum_{i=0}^{p-2} x_i\right)^2 \\
&= p\left(\underbrace{x_0^2 + \cdots + x_{\frac{p-1}{d}-1}^2}_{=\frac{p-1}{d}y_1} + x_{\frac{p-1}{d}}^2 + \cdots + x_{p-2}^2\right) - \left(\left(\underbrace{x_0 + \cdots + x_{\frac{p-1}{d}-1}}_{=\frac{p-1}{d}y_1} + \cdots + x_{p-2}\right)\right)^2 \\
&= p\left(\frac{p-1}{d}\right)\sum_{i=1}^{d} y_i - \left(\frac{p-1}{d}\right)^2\left(\sum_{i=1}^{d} y_i\right)^2
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
Tr_{\mathbb{L}/\mathbb{Q}}\ y\overline{y} &= Tr_{\mathbb{K}/\mathbb{Q}}\left(Tr_{\mathbb{L}/\mathbb{K}}\ y\overline{y}\right) \\
&= Tr_{\mathbb{K}/\mathbb{Q}}\left(\frac{p-1}{d}\ y\overline{y}\right)
\end{aligned}$$

donde,

$$\frac{d}{p-1} Tr_{\mathbb{L}/\mathbb{Q}}\ y\overline{y} = Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y}$$

e portanto,

$$\frac{d}{p-1}\left(p\frac{(p-1)}{d}\sum_{i=1}^{d} y_i^2 - \left(\frac{p-1}{d}\right)^2\left(\sum_{i=1}^{d} y_i\right)^2\right) = Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y}$$

logo,

$$Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y} = p\sum_{i=1}^{d} y_i^2 - \frac{p-1}{d}\left(\sum_{i=1}^{d} y_i\right)^2 \tag{3.2}$$

Fixando $\sum_{i=1}^{d} y_i = m$, onde $m = dq+s$, e aplicando a troca sugerida na Observação 3.3.2, temos a seguinte d-upla:

$$(\underbrace{q+1,\cdots,q+1}_{s \text{ vezes}}, q+\cdots+q)$$

Assim,

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y} &= p\left(s(q+1)^2+(d-s)q^2\right) - \frac{p-1}{d}(dq+s)^2 \\ &= \frac{1}{d}\left\{(dq+s)^2 + ps(d-s)\right\} \end{aligned}$$

Se $\sum_{i=1}^{d} y_i = 0$, usando a Equação 3.2 temos que $Tr_{\mathbb{K}/\mathbb{Q}} y\overline{y} = p\sum_{i=1}^{d} y_i$ e o mínimo ocorre quando $y_i = 1$ e $y_j = -1$, para algum $i, j \in \{1,\cdots d\}$, neste caso, a forma quadrática vale $2p$.

Nosso objetivo agora será minimizar a função $\mathbf{Q} = \frac{1}{d}\left\{(dq+s)^2 + ps(d-s)\right\}$, onde d e p são constantes e s assume um dos valores: $0, 1, \cdots, d-1$.

Se $s = 0$, temos $\mathbf{Q} = \frac{1}{d}(dq)^2 = dq^2$, portanto, $\min\{\mathbf{Q}\}$ ocorre quando q assume seu menor valor possível diferente de zero, pois do contrário, $\sum y_i = 0$ que já analisamos. Assim, $q = 1$ e $\sum y_1 = d$, neste caso, $\min\{\mathbf{Q}\} = d$.

Além disso,

$$Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y} = \frac{1}{d}\left\{(dq+s)^2 + ps(d-s)\right\} \geq dq^2 \geq d$$

ou seja, o mínimo que a função assume é d.

Neste momento, deixaremos os anéis dos inteiros e estudaremos seus sub-módulos que podem ser caracterizados por:

$$\mathcal{M}_m = \left\{ x = \sum_{i=0}^{d-1} a_i\ \theta^i(t);\ \sum_{i=0}^{d-1} a_i \equiv 0 \mod (m) \right\}$$

Um dos objetivos da próxima seção, será determinar reticulados e calcular sua densidade de centro. Para isto, precisamos determinar o índice de $\mathcal{M}_m$ sobre $\mathcal{O}_{\mathbb{K}}$, o qual denotaremos por $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$, e tal índice é exatamente a quantidade de classes laterais de $\mathcal{M}_m$ em $\mathcal{O}_{\mathbb{K}}$.

É claro que $0, t, 2t, \cdots, (m-1)t \in \mathcal{O}_{\mathbb{K}}$, assim, $\overline{0}, \overline{t}, \overline{2t}, \cdots, \overline{(m-1)t} \in \mathcal{O}_{\mathbb{K}}/\mathcal{M}_m$, o nosso primeiro

objetivo será mostrar que essas classes são todas distintas. Vale ressaltar que as classes $\overline{x}$ e $\overline{y}$ são iguais se, e somente se, $x - y \in \mathcal{M}_m$. Com isto, $\overline{it} = \overline{jt}$ se, e somente se, $(i-j)t \in \mathcal{M}_m$, isto é, se e somente se, $i - j \equiv 0 \mod (m)$ ou seja, se $i = j$. Donde, as classes laterais listadas anteriormente são duas a duas distintas e assim, temos pelo menos m classes de laterais. Nosso próximo objetivo será mostrar que não há mais nenhuma classe lateral.

Consideremos x um elemento arbitrário de $\mathcal{M}_m$,

$$x = a_0 t + a_1\theta(t) + \cdots + a_{d-1}\theta^{d-1}(t)$$

assim, $\sum_{i=0}^{d-1} a_i = mq + r$, $q \in \mathbb{Z}$ e r assume um dos valores: $0, 1, \cdots, m-1$. Seja $y = rt$, fazendo $x - y$ temos

$$x - y = (a_0 - r)t + a_1\theta(t) + \cdots + a_{d-1}\theta^{d-1}(t) = \sum_{i=0}^{d-1} a_i - r = mq + r - r = mq$$

donde, $x \in \overline{rt}$ e portanto, existem apenas m classes laterais. Consequentemente, $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}_m] = m$.

Isto posto, para calcularmos a densidade de centro, precisamos ainda, minimizar a função:

$$\mathbf{Q} = \frac{1}{d}\left\{\left(\sum_{i=1}^{d} y_i\right)^2 + ps(d-s)\right\}.$$

Além disso, como $\sum_{i=1}^{d} y_i \equiv 0 \mod (m)$ então existe $b \in \mathbb{N}$ tal que $\sum_{i=1}^{d} y_i = bm$, assim:

$$\sum_{i=1}^{d} y_i = bm \equiv s \mod (d), \quad 0 \leq s \leq d-1,$$

logo, para todo $c \in \mathbb{N}$ tal que $bm \neq cm$ mas $bm \equiv s \mod (d)$ e $cm \equiv s \mod (d)$, o minimo de $\mathbf{Q}$ ocorrerá no menor valor de $\sum_{i=1}^{d} y_i$ portanto, temos $d+1$ casos à analisar, os d casos considerando $s = 0, s = 1, \cdots, s = d-1$ e o caso $\sum_{i=1}^{d} y_i = 0$.

Exemplo. *Exemplificaremos o que foi escrito anteriormente, para isto, considere* $\mathbb{K} = \mathbb{Q}(\zeta_5)$ *e consideremos a seguinte restrição:*

$$\mathcal{M}_3 = \left\{x = \sum_{i=1}^{4} y_i\ \theta^i(t_{\mathbb{K}});\ \sum_{i=1}^{4} y_i \equiv 0 \mod (3)\right\}.$$

Nosso objetivo, como já dito, é minimizar a seguinte função:

$$\mathbf{Q} = \frac{1}{d}\left\{\left(\sum_{i=1}^{d} y_i\right)^2 + ps(d-s)\right\},$$

neste exemplo, $d = 4$, $p = 5$ e s assume um dos valores: $0, 1, 2, 3$. Isto é,

$$\mathbf{Q} = \frac{1}{4}\left\{\left(\sum_{i=1}^{4} y_i\right)^2 + 5s(4-s)\right\}; \quad s \in \{0,1,2,3\}.$$

Considerando a restrição para $\sum_{i=1}^{4} \equiv 0 \mod (3)$, temos que $\sum_{i=1}^{4} = 3 \cdot k$, $k \in \mathbb{N}$. Observe que, se tivermos $\sum_{i=1}^{4} = 9$ e $\sum_{i=1}^{4} = 21$, ambos são côngruos a $1 \mod (4)$, isto é, $s = 1$. Assim:

$$\mathbf{Q_9} = \frac{1}{4}\left\{(9)^2 + 5 \cdot 1(4-1)\right\} = \frac{4}{81+15} = 24,$$

$$\mathbf{Q_{21}} = \frac{1}{4}\left\{(21)^2 + 5 \cdot 1(4-1)\right\} = \frac{4}{441+15} = 114.$$

Logo, como nosso objetivo é minimizar $\mathbf{Q}$, basta considerarmos os valores para $\sum_{i=1}^{4} = r \equiv s \mod (4)$, onde r é o primeiro número natural côngruo a $s \mod (4)$, para $s = 0, 1, 2, 3$. Isto é, além do caso $\sum_{i=1}^{4} = 0$ temos os seguintes casos à analisar:

$$3 \equiv 3 \mod (4) \quad 6 \equiv 2 \mod (4)$$
$$9 \equiv 1 \mod (4) \quad 12 \equiv 0 \mod (4)$$

Nestes casos, a função $\mathbf{Q}$ assume os seguintes valores:

$\sum y_i$	$\mathbf{Q}$
0	$2p = 10$
3	$\left(3^2 + 5 \cdot 3 \cdot (4-3)\right)/4 = 6$
6	$\left(6^2 + 5 \cdot 2 \cdot 2\right)/4 = 14$
9	$(81 + 5 \cdot 1 \cdot 3)/4 = 24$
12	$(144 + 5 \cdot 0 \cdot 4)/4 = 36$

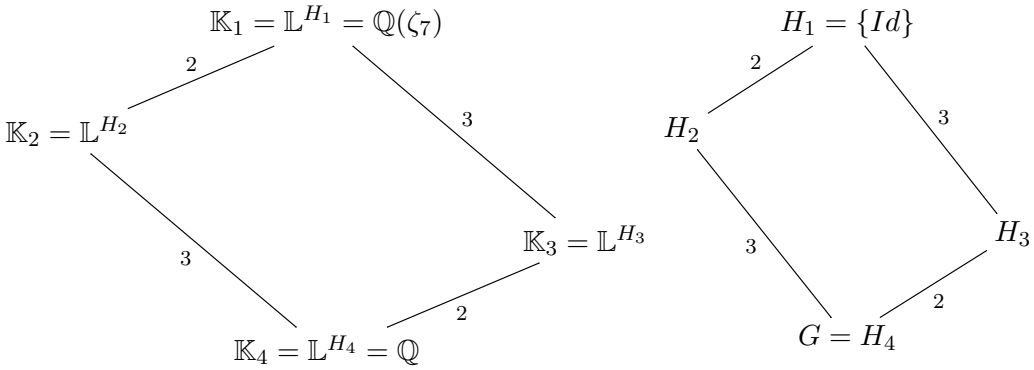
Donde, $\min \mathbf{Q} = 6$, e este valor é atingido quando $\sum_{i=1}^{4} = 3$.

3.3.2 Aplicações

Nesta seção, aplicaremos os conceitos desenvolvidos para corpos abelianos de condutor primo, aos corpos $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{17})$ e seus respectivos subcorpos. Em outras palavras, apresentaremos os subcorpos dos referidos corpos, bem como, seu grupo de Galois, base integral normal, discriminante, e por fim, calcularemos a densidade de centro de algumas realizações geométricas.

▶ $p = 7$.

Seja $\mathbb{L} = \mathbb{Q}(\zeta_7)$ então, $G = Gal(\mathbb{L}/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^*$ e portanto, cíclico. Assim, pelo Teorema 3.1.3 existem, e são únicos, os subgrupos H_1, H_2, H_3 e H_4 de G, onde, $o(H_1) = 1$, $o(H_2) = 2$ $o(H_3) = 3$ e $o(H_4) = 6$. Logo, $H_1 =< \sigma_1 >$, $H_2 =< \sigma_6 >$, $H_3 =< \sigma_2 >$ e $H_4 =< \sigma_3 >$. Além disso, pela teoria de Galois, temos a seguinte correspondência:



Para determinarmos $\mathbb{K}_2$ e $\mathbb{K}_3$ usaremos o resultado que provamos, $\mathbb{K} = \mathbb{Q}(t_{\mathbb{K}})$, onde $t_{\mathbb{K}} = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_7)$.

$$t_{\mathbb{K}_2} = Tr_{\mathbb{L}/\mathbb{K}_2}(\zeta_7) = \sigma_1(\zeta_7) + \sigma_6(\zeta_7) = \zeta_7 + \zeta_7^6 = \zeta_7 + \zeta_7^{-1}$$

$$t_{\mathbb{K}_3} = Tr_{\mathbb{L}/\mathbb{K}_3}(\zeta_7) = \sigma_1(\zeta_7) + \sigma_2(\zeta_7) + \sigma_4(\zeta_7) = \zeta_7 + \zeta_7^2 + \zeta_7^4$$

Donde, $\mathbb{K}_1 = \mathbb{L}$, $\mathbb{K}_2 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $\mathbb{K}_3 = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$ e $\mathbb{K}_4 = \mathbb{Q}$.

A seguir, em cada subcorpo $\mathbb{K}$ de $\mathbb{L}$, determinaremos seu discriminante conforme o Teorema 3.2.4, exibiremos uma base integral normal, minimizaremos a forma quadrática e por fim, calcularemos a densidade de centro da realização geométrica de $\mathcal{O}_{\mathbb{K}}$.

•$\mathbb{K}_1 = \mathbb{L} = \mathbb{Q}(\zeta_7)$

Neste caso, $\mathbb{K}_1$ é totalmente imaginário, $G_1 = Gal(\mathbb{L}/\mathbb{K}_1) =< \sigma_1 >$, uma base integral normal

é composta por $\{\zeta_7, \zeta_7^2, \zeta_7^3, \cdots, \zeta_7^6\}$ e seu discriminante absoluto é dado por:

$$|Disc(\mathbb{K}_1)| = \left(\frac{7}{7^{\frac{1}{6}}}\right)^6 = 7^5$$

Vimos que $\min\{Tr_{\mathbb{K}_1/\mathbb{Q}}(x\overline{x}); x \in \mathcal{O}_{\mathbb{K}}; x \neq 0\} = p - 1 = 6$, assim,

$$\delta(\sigma_{\mathbb{K}_1}(\mathcal{O}_{\mathbb{K}_1})) = \frac{6^{\frac{6}{2}}}{2^6 \cdot (7^5)^{\frac{1}{2}}} = \frac{6^3}{2^6 \cdot 7^{\frac{5}{2}}} = \frac{27}{8 \cdot 7^{\frac{7}{2}}} \approx 0,0037.$$

•$\mathbb{K}_2 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$

Neste caso, $\mathbb{K}_2$ é totalmente real, $G_2 = Gal(\mathbb{L}/\mathbb{K}_2) =< \sigma_6 >$, uma base integral normal é dada por $\{(\zeta_7 + \zeta_7^{-1}), (\zeta_7^2 + \zeta_7^{-2}), (\zeta_7^3 + \zeta_7^{-3})\}$ e seu discriminante absoluto é dado por:

$$|Disc(\mathbb{K}_2)| = \left(\frac{7}{7^{\frac{1}{3}}}\right)^3 = \frac{7^3}{7} = 7^2$$

Vimos que $Tr_{\mathbb{K}_2/\mathbb{Q}}(y\overline{y}) = \frac{1}{3}\left((3q+s)^2 + 7s(3-s)\right) = 3q^2 + 2qs - 2s^2 + 7s$, assim, o menor valor é obtido tomando $q = 1$ e $s = 0$, neste caso, $Tr_{\mathbb{K}_2/\mathbb{Q}}(y\overline{y}) = 3$, portanto, temos:

$$\delta(\sigma_{\mathbb{K}_2}(\mathcal{O}_{\mathbb{K}_2})) = \frac{3^{\frac{3}{2}}}{2^3 \cdot (7^2)^{\frac{1}{2}}} = \frac{3^{\frac{3}{2}}}{8 \cdot 7} = \frac{3^{\frac{3}{2}}}{56} \approx 0,0927.$$

•$\mathbb{K}_3 = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$

Temos que $[\mathbb{K}_3 : \mathbb{Q}] = 2$ e $2 \nmid 3 = [\mathbb{L}^+ : \mathbb{Q}]$, portanto, $\mathbb{K}_3$ é totalmente imaginário, uma base integral normal é $\{(\zeta_7 + \zeta_7^2 + \zeta_7^4), (\zeta_7^3 + \zeta_7^5 + \zeta_7^6)\}$, seu grupo de Galois, $G_3 = Gal(\mathbb{L}/\mathbb{K}_3) =< \sigma_2 >$ e seu discriminante absoluto é:

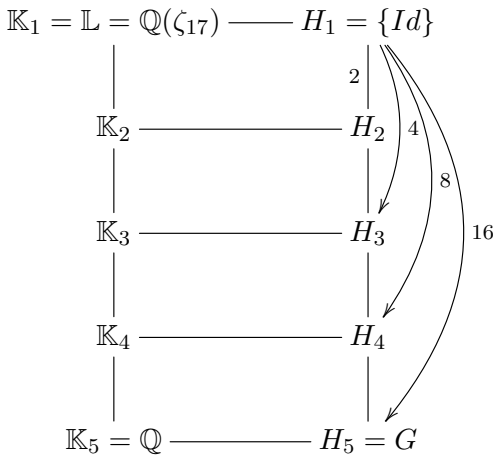
$$|Disc(\mathbb{K}_3)| = \left(\frac{7}{7^{\frac{1}{2}}}\right)^2 = \frac{7^2}{7} = 7$$

Visto que $Tr_{\mathbb{K}_3/\mathbb{Q}}(y\overline{y}) = \frac{1}{2}\left((2q+s)^2 + 7s(2-s)\right) = 2q^2 + 2qs - 3s^2 + 7s$, assim, o menor valor é obtido tomando $q = 1$ e $s = 0$, neste caso, $Tr_{\mathbb{K}_3/\mathbb{Q}}(y\overline{y}) = 2$, portanto, temos:

$$\delta(\sigma_{\mathbb{K}_3}(\mathcal{O}_{\mathbb{K}_3})) = \frac{2^{\frac{2}{2}}}{2^2 \cdot 7^{\frac{1}{2}}} = \frac{1}{2\sqrt{7}} \approx 0,1889.$$

► $p = 17$.

Uma vez que, $[\mathbb{L} = \mathbb{Q}(\zeta_{17}) : \mathbb{Q}] = 16$ e $G = Gal(\mathbb{L}/\mathbb{Q}) \simeq (\mathbb{Z}/17\mathbb{Z})^*$ que é cíclico, temos para divisor de 16, um único subgrupo de G cuja ordem é igual ao divisor. Além disso, como o subgrupo de um grupo cíclico é ainda um grupo cíclico, a propriedade anterior se repete, donde, temos:



Ou seja, como a ordem do grupo G é a quarta potência de 2, e este é cíclico, ele possui um único subgrupo de ordem $2^3, 2^2, 2$ e 1, pelo mesmo argumento, o subgrupo de ordem 2^3 possui um único subgrupo de ordem $2^2, 2$ e 1 que, pela unicidade, coincide com o subgrupo com ordem correspondente de G, isto é, os subgrupos de ordem menor estão contidos nos subgrupos de ordem maior. Assim, pela Teoria de Galois, temos uma torre de corpos. Donde, como $\mathbb{K}_2$ é subcorpo real maximal, os demais subcorpos são totalmente reais.

Os subgrupos de G são: $H_1 =< \sigma_1 = Id >$, $H_2 =< \sigma_{16} >$, $H_3 =< \sigma_4 >$, $H_4 =< \sigma_2 >$ e $H_5 = G =< \sigma_3 >$. Vamos determinar agora os subcorpos de $\mathbb{L}$, para cada caso determinaremos uma base integral normal, calcularemos o discriminante do referido corpo bem como, a densidade de centro da realização geométrica de $\mathcal{O}_{\mathbb{K}}$ e de um módulo de $\mathcal{O}_{\mathbb{K}}$, para cada $\mathbb{K}$ subcorpo de $\mathbb{L}$. Em relação ao discriminante, vale ressaltar que, do Teorema 3.2.4, temos:

$$|Disc(\mathbb{K}_i)| = \left(\frac{17}{17^{u_i}}\right)^{[\mathbb{K}_i:\mathbb{Q}]} = \left(17^{(1-u_i)}\right)^{[\mathbb{K}_i:\mathbb{Q}]},$$

onde $u_i = [\mathbb{K} \cdot \mathbb{Q} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}]$

•$\mathbb{K}_1 = \mathbb{L}$

Neste caso, uma base integral normal para $\mathbb{K}_1$ é dada por $\{\zeta_{17}, \zeta_{17}^2, \zeta_{17}^3, \cdots, \zeta_{17}^{16}\}$. Além disso, seu discriminante é

$$|Disc(\mathbb{K}_1)| = \left(\frac{17}{17^{16}}\right)^{16} = 17^{15}$$

Neste caso, vimos que $\min\{Tr_{\mathbb{L}/\mathbb{Q}}\ x\overline{x}\} = p - 1$, portanto, 16. Donde,

$$\delta(\sigma_{\mathbb{K}_1}(\mathcal{O}_{\mathbb{K}_1})) = \frac{16^{\frac{16}{2}}}{2^{16}17^{\frac{15}{2}}} = \frac{4^8}{17^{\frac{15}{2}}} \approx 0,00003.$$

•$\mathbb{K}_2 = \mathbb{Q}(t_{\mathbb{K}_2})$

$$t_{\mathbb{K}_2} = Tr_{\mathbb{L}/\mathbb{K}_2}\zeta_{17} = \zeta_{17} + \zeta_{17}^{-1}$$

Donde, $\mathbb{K}_2 = \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$. Além disso, uma base integral para $\mathbb{K}_2$ é constituida por $\{\sigma_3^i(\zeta_{17}+\zeta_{17}^{-1}), 1 \leq i \leq 8 = [\mathbb{K}_2 : \mathbb{Q}]\} = \{\left(\zeta_{17} + \zeta_{17}^{-1}\right),\ \left(\zeta_{17}^2 + \zeta_{17}^{-2}\right),\ \left(\zeta_{17}^3 + \zeta_{17}^{-3}\right),\ \left(\zeta_{17}^4 + \zeta_{17}^{-4}\right), \left(\zeta_{17}^5 + \zeta_{17}^{-5}\right), \left(\zeta_{17}^6 + \zeta_{17}^{-6}\right), \left(\zeta_{17}^7 + \zeta_{17}^{-7}\right),\ \left(\zeta_{17}^8 + \zeta_{17}^{-8}\right)\}$. Além disso,

$$|Disc(\mathbb{K}_2)| = \left(\frac{17}{17^8}\right)^8 = 17^7$$

Vimos que, $\min\{Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y}\} = d$, portanto, 8. Donde,

$$\delta(\sigma_{\mathbb{K}_2}(\mathcal{O}_{\mathbb{K}_2})) = \frac{8^{\frac{8}{2}}}{2^8 17^{\frac{7}{2}}} = \frac{8^4}{2^8 17^{\frac{7}{2}}} = \frac{16}{17^{\frac{7}{2}}} \approx 0,0007.$$

•$\mathbb{K}_3 = \mathbb{Q}(t_{\mathbb{K}_3})$

$$t_{\mathbb{K}_3} = Tr_{\mathbb{L}/\mathbb{K}_3}\zeta_{17} = \zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^4 + \zeta_{17}^{-4}$$

Donde, $\mathbb{K}_3 = \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^4 + \zeta_{17}^{-4})$. Neste caso, uma base integral para $\mathbb{K}_3$ é formada por $\{\left(\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^4 + \zeta_{17}^{-4}\right),\ \left(\zeta_{17}^3 + \zeta_{17}^{-3} + \zeta_{17}^5 + \zeta_{17}^{-5}\right),\ \left(\zeta_{17}^2 + \zeta_{17}^{-2} + \zeta_{17}^8 + \zeta_{17}^{-8}\right),\ \left(\zeta_{17}^6 + \zeta_{17}^{-6} + \zeta_{17}^7 + \zeta_{17}^{-7}\right)\}$. Também,

$$|Disc(\mathbb{K}_3)| = \left(\frac{17}{17^4}\right)^4 = 17^3$$

Neste caso, $\min\{Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y}\} = 4$, portanto,

$$\delta(\sigma_{\mathbb{K}_3}(\mathcal{O}_{\mathbb{K}_3})) = \frac{4^{\frac{4}{2}}}{2^4 17^{\frac{3}{2}}} = \frac{1}{2 \cdot 17^{\frac{3}{2}}} \approx 0,0071.$$

•$\mathbb{K}_4 = \mathbb{Q}(t_{\mathbb{K}_4})$

$$t_{\mathbb{K}_4} = Tr_{\mathbb{L}/\mathbb{K}_4}\zeta_{17} = \zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^2 + \zeta_{17}^{-2} + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^8 + \zeta_{17}^{-8}$$

Donde, $\mathbb{K}_2 = \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^2 + \zeta_{17}^{-2} + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^8 + \zeta_{17}^{-8})$. E uma base integral normal para $\mathbb{K}_2$ é $\{\left(\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^2 + \zeta_{17}^{-2} + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^8 + \zeta_{17}^{-8}\right), \left(\zeta_{17}^3 + \zeta_{17}^{-3} + \zeta_{17}^6 + \zeta_{17}^{-6} + \zeta_{17}^5 + \zeta_{17}^{-5} + \zeta_{17}^7 + \zeta_{17}^{-7}\right)\}$. Além disso,

$$|Disc(\mathbb{K}_4)| = \left(\frac{17}{17^2}\right)^2 = 17$$

Assim, $\min\{Tr_{\mathbb{K}/\mathbb{Q}}\ y\overline{y}\} = 2$, donde,

$$\delta(\sigma_{\mathbb{K}_4}(\mathcal{O}_{\mathbb{K}_4})) = \frac{2^{\frac{2}{2}}}{2^2 17^{\frac{1}{2}}} = \frac{1}{2 \cdot 17^{\frac{1}{2}}} \approx 0,1212.$$

Agora, consideremos a seguinte restrição de $\mathcal{O}_{\mathbb{K}}$, o módulo

$$\mathcal{M}_3 = \left\{ \sum_{i=0}^{d-1} a_i \theta^i(t_{\mathbb{K}}); \quad \sum_{i=0}^{d-1} a_i \equiv 0 \mod (3) \right\}.$$

Nosso objetivo será determinar a densidade de centro, do reticulado obtido através do homomorfismo de Minkowski aplicado em $\mathcal{M}$, sabemos que:

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M}_m)) = \frac{t^{\frac{n}{2}}}{2^n |D|^{\frac{1}{2}} [\mathcal{O}_{\mathbb{K}} : \mathcal{M}_m]}$$

onde, $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}\ x\overline{x};\ x \in \mathcal{M}_m, x \neq 0\}$, $n = [\mathbb{K} : \mathbb{Q}]$, D é o discriminante de $\mathbb{K}$ e $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}_m] = m$, que neste caso é 3. Portanto, para determinar a referida densidade de centro, precisamos determinar t, faremos isto para cada subcorpo de $\mathbb{Q}(\zeta_{17})$ e, por fim, apresentaremos uma tabela com as respectivas densidades.

Seja $\sum_{i=1}^{d} y_i = qd + s$, onde $q \in \mathbb{N}$, $d = [\mathbb{K}_i : \mathbb{Q}]$ e s assume um dos valores: $\{0, 1, 2, \cdots, d-1\}$. Nosso objetivo é minimizar a função:

$$\mathbf{Q} = \frac{1}{d} \left\{ \left(\sum_{i=1}^{d} y_i \right)^2 + ps(d-s) \right\},$$

com a restrição, $\sum_{i=1}^{d} y_i \equiv 0 \mod (3)$.

- $\mathbb{K}_1 = \mathbb{Q}(\zeta_{17})$

Note que, se $\sum_{i=1}^{d} y_i = qd + s$ ou $\sum_{i=1}^{d} y_i = rd + s$ então, quando aplicarmos a função $\mathbf{Q}$ em ambos valores, o menor $\sum_{i=1}^{d} y_i$ é o que assume o menor valor de $\mathbf{Q}$. Como nosso objetivo é minimizar a função $\mathbf{Q}$, temos d casos à analisar, além do caso $\sum_{i=1}^{d} y_i = 0$.

Exemplificando o que foi escrito anteriormente, considere $\sum_{i=1}^{16} y_i = 0 \cdot 16 + 3 = 3$ e $\sum_{i=1}^{16} y_i = 1 \cdot 16 + 3 = 19$, ambos possuem o mesmo $d = 16$, o mesmo $s = 3$, e o mesmo $p = 17$, sendo assim, o que determinará qual deles tem a menor imagem será o valor de $\sum_{i=1}^{16} y_i$, isto é, o menor valor tem também a menor imagem. Em outras palavars, o primeiro número positivo côngruo a 3 mod (16) é o que corresponde a menor imagem de $\mathbf{Q}$, considerando $s = 3$. Isto posto, temos os seguintes casos a considerar:

$$\begin{array}{llll} 3 \equiv 3 \mod 16 & 6 \equiv 6 \mod 16 & 9 \equiv 9 \mod 16 & 12 \equiv 12 \mod 16 \\ 15 \equiv 15 \mod 16 & 18 \equiv 2 \mod 16 & 21 \equiv 5 \mod 16 & 24 \equiv 8 \mod 16 \\ 27 \equiv 11 \mod 16 & 30 \equiv 14 \mod 16 & 33 \equiv 1 \mod 16 & 36 \equiv 4 \mod 16 \\ 39 \equiv 7 \mod 16 & 42 \equiv 10 \mod 16 & 45 \equiv 13 \mod 16 & 48 \equiv 0 \mod 16 \end{array}$$

Nestes casos, a função $\mathbf{Q}$ assume os seguintes valores:

$\sum y_i$	$\min \mathbf{Q}$
0	$2p = 34$
3	$\left(3^2 + 17 \cdot 3 \cdot (16-3)\right)/16 = 42$
6	$(36 + 17 \cdot 6 \cdot 10)/16 = 66$
9	$(81 + 17 \cdot 9 \cdot 7)/16 = 72$
12	$(144 + 17 \cdot 12 \cdot 4)/16 = 60$
15	$(225 + 17 \cdot 15)/16 = 30$
18	50
21	86
24	106
27	104
30	86
33	84
36	132
39	162
42	174
45	168
48	144

Donde, $t = 30$ e este mínimo é atingido em $\sum_{i=1}^{16} y_i = 15$.

•$\mathbb{K}_2$ Agora, procedendo de modo análogo ao feito no caso anterior, precisamos analisar os $\sum_{i=1}^{8} y_i$ iguais aos primeiros números positivos côngruos a $r \mod (8)$, onde $r = \{0,1,2,3,4,5,6,7\}$, considerando a restrição $\sum_{i=1}^{8} y_i \equiv 0 \mod (3)$. Ou seja, temos os seguintes casos a considerar:

$$\begin{array}{llll} 3 \equiv 3 \mod 8 & 6 \equiv 6 \mod 8 & 9 \equiv 1 \mod 8 & 12 \equiv 4 \mod 8 \\ 15 \equiv 7 \mod 8 & 18 \equiv 2 \mod 8 & 21 \equiv 5 \mod 8 & 24 \equiv 0 \mod 8 \end{array}$$

Para estes valores, a função $\mathbf{Q}$ assume:

$\sum y_i$	$\min \mathbf{Q}$
0	$2p = 34$
3	$\left(3^2 + 17 \cdot 3 \cdot (8-3)\right)/8 = 33$
6	$(36 + 17 \cdot 6 \cdot 2)/8 = 30$
9	$(81 + 17 \cdot 7)/8 = 25$
12	$(144 + 17 \cdot 4 \cdot 4)/8 = 52$
15	$(225 + 17 \cdot 7)/8 = 43$
18	$(324 + 17 \cdot 2 \cdot 6)/8 = 66$
21	$(441 + 17 \cdot 5 \cdot 3)/8 = 87$
24	$(576)/8 = 72$

Assim, $t = 25$ e este valor é atingido quando $\sum_{i=1}^{8} y_i = 9$.

•$\mathbb{K}_3$ Agora, analisaremos os primeiros valores de $\sum_{i=1}^{4} y_i$ tal que, $\sum_{i=1}^{4} y_i \equiv r \mod 4$, $r = \{0, 1, 2, 3\}$, além do caso $\sum_{i=1}^{4} y_i = 0$. Isto é, temos seguintes casos a considerar:

$$3 \equiv 3 \mod 4 \quad 6 \equiv 2 \mod 4$$
$$9 \equiv 1 \mod 4 \quad 12 \equiv 0 \mod 4$$

Nestes casos, a função $\mathbf{Q}$ corresponde:

$\sum y_i$	$\min \mathbf{Q}$
0	$2p = 34$
3	$\left(3^2 + 17 \cdot 3 \cdot (4-3)\right)/4 = 15$
6	$(36 + 17 \cdot 2 \cdot 2)/4 = 26$
9	$(81 + 17 \cdot 3)/4 = 33$
12	$(144)/4 = 36$

Consequentemente, $t = 15$ e este valor é atingido quando $\sum_{i=1}^{4} y_i = 3$.

•$\mathbb{K}_4$ Finalmente, analisaremos $\sum_{i=1}^{2} y_i \equiv r \mod (2)$, $r = 0, 1$. Assim, temos os seguintes casos a considerar: $\sum_{i=1}^{2} y_i$ igual a 0, $3 \equiv 1 \mod 2$ e $6 \equiv 0 \mod 2$.

Nos quais a função $\mathbf{Q}$ assume os seguintes valores:

$\sum y_i$	$\min \mathbf{Q}$
0	$2p = 34$
3	$(9+17)/2 = 13$
6	$(36)/2 = 18$

Donde, $t = 13$ e este valor ocorre quando $\sum_{i=1}^{2} y_i = 3$.

Assim, temos a seguinte tabela:

$\mathbb{K}_i$	$\delta(\sigma_{\mathbb{K}_i}(\mathcal{M}))$
$\mathbb{K}_1$	$\frac{30^8}{2^{16}\cdot 17^{\frac{15}{2}}\cdot 3} = \frac{15^8}{2^8\cdot 17^{\frac{15}{2}}\cdot 3} \approx 0,0019$
$\mathbb{K}_2$	$\frac{25^4}{2^8\cdot 17^{\frac{7}{2}}\cdot 3} \approx 0,0251$
$\mathbb{K}_3$	$\frac{15^2}{2^4\cdot 17^{\frac{3}{2}}\cdot 3} \approx 0,0668$
$\mathbb{K}_4$	$\frac{13}{2^2\cdot 17^{\frac{1}{2}}\cdot 3} \approx 0,2627$

3.4 Subcorpos Reais Maximais de Corpos Ciclotômicos de grau 8

De agora em diante, restringimos nossos estudos aos subcorpos reais maximais dos corpos ciclotômicos de grau 8. Em conformidade com $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, n assume um dos seguintes valores: $15, 16, 20, 24$ ou 30.

Observação 3.4.1. *Resulta da Proposição 2.1.14 que, para nossos casos particulares,* $\mathbf{B} = \{1, (\zeta_n + \zeta_n^{-1}), (\zeta_n + \zeta_n^{-1})^2, (\zeta_n + \zeta_n^{-1})^3\}$ *é uma base integral de* $\mathbb{Q}(\zeta_n)^+$. *Mais ainda, temos que* $(\zeta_n + \zeta_n^{-1})^2 = \zeta_n^2 + \zeta_n^{-2} + 2$ *e* $(\zeta_n + \zeta_n^{-1})^3 = \zeta_n^3 + \zeta_n^{-3} + 3\zeta_n + 3\zeta_n^{-1}$. *Logo, os elementos de* $\mathcal{B} = \{1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \zeta_n^3 + \zeta_n^{-3}\}$ *podem ser escritos como combinação linear dos elementos de* $\mathbf{B}$ *e reciprocamente, os elementos de* $\mathbf{B}$ *podem ser escritos como combinação linear dos elementos de* $\mathcal{B}$. *Donde,* $\mathcal{B}$ *é também uma base integral para* $\mathbb{Q}(\zeta_n)^+$, *e será esta que usaremos daqui em diante.*

Em seguida, determinaremos o grupo de Galois de cada extensão $\mathbb{Q}(\zeta_n)^+$.

•$\mathbb{Q}(\zeta_{15})^+$

Primeiramente, vamos escrever os elementos de $\mathbb{Q}(\zeta_{15})$ como combinação linear dos elementos da base integral de $\mathbb{Q}(\zeta_{15})$, ou seja, como combinação linear de $\{1, \zeta_{15}, \zeta_{15}^2, \cdots, \zeta_{15}^7\}$. Para isto, precisaremos do polinômio ciclotômico que é dado por:

$$\Phi_{15}(X) = \frac{X^{15} - 1}{\Phi_5(X)\Phi_3(X)\Phi_1(X)} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Assim, denotanto ζ_{15} por ζ, temos que ζ é raiz de $\Phi_{15}(X)$, logo, $\zeta^8 - \zeta^7 + \zeta^5 - \zeta^4 + \zeta^3 - \zeta + 1 = 0$ e

portanto,

$$\begin{aligned}
\zeta^8 &= \zeta^7-\zeta^5+\zeta^4-\zeta^3+\zeta-1\\
\zeta^9 &= \zeta^8\cdot\zeta=(\zeta^7-\zeta^5+\zeta^4-\zeta^3+\zeta-1)\cdot\zeta=\zeta^7-\zeta^5+\zeta^4-\zeta^3+\zeta-1-\zeta^6+\zeta^5-\zeta^4+\zeta^2-\zeta\\
&= \zeta^7-\zeta^6-\zeta^3+\zeta^2-1\\
\zeta^{10} &= -\zeta^5-1\\
\zeta^{11} &= -\zeta^6-\zeta\\
\zeta^{12} &= -\zeta^7-\zeta^2\\
\zeta^{13} &= -\zeta^7+\zeta^5-\zeta^4-\zeta+1\\
\zeta^{14} &= -\zeta^7+\zeta^6-\zeta^4+\zeta^3-\zeta^2+1\\
\zeta^{15} &= 1
\end{aligned}$$

Agora, vamos determinar como é a ação do grupo de Galois neste corpo. Temos que $Gal(\mathbb{Q}(\zeta)^+|\mathbb{Q})=<\sigma_2>$, além disso, para determinarmos a ação deste grupo no corpo, é suficiente determinarmos, sua ação em um elemento arbitrário, faremos isto para $a_0+a_1(\zeta+\zeta^{-1})+a_2(\zeta^2+\zeta^{-2})+a_3(\zeta^3+\zeta^{-3})$.

Observemos que, $\sigma_2(1)=1$, $\sigma_2(\zeta+\zeta^{-1})=\sigma_2(\zeta)+\sigma_2(\zeta^{-1})=\zeta^2+\zeta^{-2}$, $\sigma_2(\zeta^2+\zeta^{-2})=\zeta^4+\zeta^{-4}$ e $\sigma_2(\zeta^3+\zeta^{-3})=\zeta^6+\zeta^{-6}$. Portanto precisamos escrever $\zeta^4+\zeta^{-4}$ e $\zeta^6+\zeta^{-6}$ como combinação linear dos elementos da base. Temos que:

$$\begin{aligned}
\zeta^4+\zeta^{-4} &= a_0+a_1(\zeta+\zeta^{-1}+a_2(\zeta^2+\zeta^{-2})+a_3(\zeta^3+\zeta^{-3})\\
\zeta^4+\zeta^{11} &= a_0+a_1(\zeta+\zeta^{14}+a_2(\zeta^2+\zeta^{13})+a_3(\zeta^3+\zeta^{12})\\
-\zeta^6+\zeta^4-\zeta &= a_0+a_1(-\zeta^7+\zeta^6-\zeta^4+\zeta^3-\zeta^2+\zeta+1)+a_2(-\zeta^7+\zeta^5-\zeta^4+\zeta^2-\zeta+1)+\\
&\quad +a_3(-\zeta^7+\zeta^3-\zeta^2)\\
-\zeta^6+\zeta^4-\zeta &= \zeta^7(-a_1+a_2-a_3)+a_1\zeta^6+a_2\zeta^5+\zeta^4(-a_1-a_2)+\zeta^3(a_1+a_3)+\\
&\quad +\zeta^2(-a_1+a_2-a_3)+\zeta(a_1-a_2)+a_0+a_1+a_2
\end{aligned}$$

Donde, $a_1=-1$, $a_2=0$, $a_3=1$ e $a_0=1$. E portanto, $\zeta^4+\zeta^{-4}=1-(\zeta+\zeta^{-1})+(\zeta^3+\zeta^{-3})$. Analogamente,

$$\begin{aligned}
\zeta^6+\zeta^{-6} &= a_0+a_1(\zeta+\zeta^{-1}+a_2(\zeta^2+\zeta^{-2})+a_3(\zeta^3+\zeta^{-3})\\
\zeta^4+\zeta^9 &= a_0+a_1(\zeta+\zeta^{14}+a_2(\zeta^2+\zeta^{13})+a_3(\zeta^3+\zeta^{12})
\end{aligned}$$

$$\begin{aligned}\zeta^6+\zeta^7-\zeta^6-\zeta^3+\zeta^2-1 &= a_0+a_1(-\zeta^7+\zeta^6-\zeta^4+\zeta^3-\zeta^2+\zeta+1)+a_2(-\zeta^7+\zeta^5-\zeta^4+\zeta^2-\zeta+1)+\\ &\quad +a_3(-\zeta^7+\zeta^3-\zeta^2)\\ \zeta^7-\zeta^3+\zeta^2-1 &= \zeta^7(-a_1+a_2-a_3)+a_1\zeta^6+a_2\zeta^5+\zeta^4(-a_1-a_2)+\zeta^3(a_1+a_3)+\\ &\quad +\zeta^2(-a_1+a_2-a_3)+\zeta(a_1-a_2)+a_0+a_1+a_2\end{aligned}$$

Donde, $a_1=0$, $a_2=0$, $a_3=-1$ e $a_0=-1$. E portanto, $\zeta^6+\zeta^{-6}=-1-(\zeta^3+\zeta^{-3})$.

Aplicando σ_2 e suas potências em um elemento arbitrário de $\mathbb{Q}(\zeta_{15})^+$, e denotando $\zeta^i+\zeta^{-i}$ por α_i temos:

$$\begin{aligned}\sigma_2(a_0+a_1\alpha_1+a_2\alpha_2+a_3\alpha_3) &= \sigma_2(a_0)+\sigma_2(a_1\alpha_1)+\sigma_2(a_2\alpha_2)+\sigma_2(a_3\alpha_3)\\ &= a_0\sigma_2(1)+a_1\sigma_2(\alpha_1)+a_2\sigma_2(\alpha_2)+a_3\sigma_2(\alpha_3)\\ &= a_0+a_1\alpha_2+a_2(1-\alpha_1+\alpha_3)+a_3(-1-\alpha_3)\\ &= a_0+a_1\alpha_2+a_2-a_2\alpha_1+a_2\alpha_3-a_3-a_3\alpha_3\\ &= (a_0+a_2-a_3)-a_2\alpha_1+a_1\alpha_2+(a_2-a_3)\alpha_3\end{aligned}$$

$$\begin{aligned}\sigma_2^2(a_0+a_1\alpha_1+a_2\alpha_2+a_3\alpha_3) &= \sigma_2\left((a_0+a_2-a_3)-a_2\alpha_1+a_1\alpha_2+(a_2-a_3)\alpha_3\right)\\ &= (a_0+a_2-a_3)-a_2\sigma_2(\alpha_1)+a_1\sigma_2(\alpha_2)+(a_2-a_3)\sigma_2(\alpha_3)\\ &= (a_0+a_2-a_3)-a_2\alpha_2+a_1(1-\alpha_1+\alpha_3)+(a_2-a_3)(-1-\alpha_3)\\ &= (a_0+a_2-a_3)-a_2\alpha_2+a_1-a_1\alpha_1+a_1\alpha_3-a_2+a_3+(-a_2+a_3)\alpha_3\\ &= (a_0+a_1)-a_1\alpha_1-a_2\alpha_2+(a_1-a_2+a_3)\alpha_3\end{aligned}$$

$$\begin{aligned}\sigma_2^3(a_0+a_1\alpha_1+a_2\alpha_2+a_3\alpha_3) &= \sigma_2\left((a_0+a_1)-a_1\alpha_1-a_2\alpha_2+(a_1-a_2+a_3)\alpha_3\right)\\ &= (a_0+a_1)-a_1\sigma_2(\alpha_1)-a_2\sigma_2(\alpha_2)+(a_1-a_2+a_3)\sigma_2(\alpha_3)\\ &= (a_0+a_1)-a_1\alpha_2-a_2(1-\alpha_1+\alpha_3)+(a_1-a_2+a_3)(-1-\alpha_3)\\ &= (a_0-a_3)+a_2\alpha_1-a_1\alpha_2+(-a_1-a_3)\alpha_3\end{aligned}$$

Os demais casos são similares a este, portanto, os descreveremos sem tantos detalhes.

•$\mathbb{Q}(\zeta_{16})^+$

Neste caso, temos $\Phi_{16}(X) = X^8 + 1$, portanto, denotando ζ_{16} por ζ, temos $\zeta^8 = -1$. Além disso, $Gal(\mathbb{Q}(\zeta_{16})^+|\mathbb{Q}) =< \sigma_3 >$ e, sua ação na base integral é dada por:

$$\sigma_3(1) = 1 \quad \sigma_3(\alpha_1) = \alpha_3 \quad \sigma_3(\alpha_2) = -\alpha_2 \quad \sigma_3(\alpha_3) = -\alpha_1$$

Donde, para um elemento arbitrário de $\mathbb{Q}(\zeta_{16})^+$, $a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3$, a ação do grupo de Galois, e de suas potências é dado por:

$$\sigma_3(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 - a_3\alpha_1 - a_2\alpha_2 + a_1\alpha_3$$

$$\sigma_3^2(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 - a_1\alpha_1 + a_2\alpha_2 - a_3\alpha_3$$

$$\sigma_3^3(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 + a_3\alpha_1 - a_2\alpha_2 - a_1\alpha_3$$

•$\mathbb{Q}(\zeta_{20})^+$

Já que $\Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$, denotando ζ_{20} por ζ, temos $\zeta^8 = \zeta_6 - \zeta^4 + \zeta^2 - 1$. Além disso, $Gal(\mathbb{Q}(\zeta_{20})^+|\mathbb{Q}) =< \sigma_3 >$ e, sua ação na base integral é:

$$\sigma_3(1) = 1 \quad \sigma_3(\alpha_1) = \alpha_3 \quad \sigma_3(\alpha_2) = 1 - \alpha_2 \quad \sigma_3(\alpha_3) = -\alpha_1$$

Assim, para um elemento arbitrário de $\mathbb{Q}(\zeta_{20})^+$, $a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3$, a ação do grupo de Galois, e de suas potências é dado por:

$$\sigma_3(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 + a_2 - a_3\alpha_1 - a_2\alpha_2 + a_1\alpha_3$$

$$\sigma_3^2(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 - a_1\alpha_1 + a_2\alpha_2 - a_3\alpha_3$$

$$\sigma_3^3(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 + a_2 + a_3\alpha_1 - a_2\alpha_2 - a_1\alpha_3$$

•$\mathbb{Q}(\zeta_{24})^+$

Temos que $\Phi_{24}(X) = X^8 - X^4 + 1$, portanto, denotando ζ_{24} por ζ, temos $\zeta^8 = \zeta^4 - 1$. Além disso, $Gal(\mathbb{Q}(\zeta_{24})^+|\mathbb{Q}) =< (\sigma_5, \sigma_7) >$. A ação do grupo de Galois para um elemento arbitrário de $\mathbb{Q}(\zeta_{24})^+$ é dada por:

$$\sigma_5(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 + a_1\alpha_1 - a_2\alpha_2 + (-a_1 - a_3)\alpha_3$$

$$\sigma_7(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 - a_1\alpha_1 - a_2\alpha_2 + (a_1 + a_3)\alpha_3$$

$$(\sigma_5 \circ \sigma_7)(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = a_0 - a_1\alpha_1 + a_2\alpha_2 - a_3\alpha_3$$

•$\mathbb{Q}(\zeta_{30})^+$

Agora, $\Phi_{30}(X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$, portanto, denotando ζ_{30} por ζ, temos $\zeta^8 = -\zeta^7 + \zeta^5 + \zeta^4 + \zeta^3 - \zeta - 1$. Além disso, $Gal(\mathbb{Q}(\zeta_{30})^+|\mathbb{Q}) =< \sigma_7 >$ e, sua ação, e de suas potências, em um elemento qualquer do corpo $\mathbb{Q}(\zeta_{30})^+$ são dadas por:

$$\sigma_7(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = (a_0 + a_3) - a_2\alpha_1 + a_1\alpha_2 + (-a_1 - a_3)\alpha_3$$

$$\sigma_7^2(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = (a_0 - a_1) - a_1\alpha_1 - a_2\alpha_2 + (a_1 + a_2 + a_3)\alpha_3$$

$$\sigma_7^3(a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = (a_0 + a_2 + a_3) + a_2\alpha_1 - a_1\alpha_2 + (-a_2 - a_3)\alpha_3$$

3.4.1 Aplicações

Nesta seção, explicitaremos alguns reticulados obtidos via homomorfismo de Minkowski, para subcorpos reais maximais de corpos ciclotômicos de grau 8, bem como seu volume, raio de empacotamento e densidade de centro.

Iniciamos escolhendo dois elementos arbitrários de $\mathcal{O}_{\mathbb{K}}$, α e β, supondo que $Gal(\mathbb{K}|\mathbb{Q}) =< \sigma >$, escolhemos também $\sigma(\alpha)$ e $\sigma(\beta)$, de maneira que estes elementos constituam uma base para um $\mathbb{Z}$-módulo. Assim, como já vimos, aplicando o homomorfismo de Minkowski temos um reticulado. Neste trabalho, explicitaremos as estapas deste método para $\mathbb{K} = \mathbb{Q}(\zeta_{15})^+$ e para $\mathbb{K} = \mathbb{Q}(\zeta_{24})^+$, os demais casos são análogos ao primeiro.

- $\mathbb{K} = \mathbb{Q}(\zeta_{15})^+$

Uma vez que $Gal(\mathbb{K}|\mathbb{Q}) =< \sigma_2 >$, escolha o $\mathbb{Z}$-módulo $\mathcal{M}$ de $\mathbb{K}$, cuja base é formada por $3\alpha_1$, α_3, $\sigma_2(3\alpha_1)$ e $\sigma_2(\alpha_3)$, isto é, $\mathcal{B} = \{3\alpha_1, 3\sigma_2(\alpha_1), \alpha_3, \sigma_2(\alpha_3)\} = \{3\alpha_1, 3\alpha_2, \alpha_3, -1 - \alpha_3\}$ forma uma $\mathbb{Z}$-base para $\mathcal{M}$. Além disso, pela Proposição 2.3.2, a imagem de um $\mathbb{Z}$-módulo pelo homomorfismo de Minkowski é um reticulado, cujo volume é o determinante da matriz M dada por: a primeira coluna são os elementos da base, a segunda é a imagem de σ_2 da primeira, a terceira coluna é a imagem de σ_2^2 da primeira, ou equivalentemente, a imagem de σ_2 da segunda, e por fim, a quarta é a imagem de

σ_2^3 da primeira, ou a imagem de σ_2 da terceira. Isto é:

$$M = \begin{pmatrix} 3\alpha_1 & 3\alpha_2 & 3-3\alpha_1+3\alpha_3 & -3\alpha_2-3\alpha_3 \\ 3\alpha_2 & 3-3\alpha_1+3\alpha_3 & -3\alpha_2-3\alpha_3 & 3\alpha_1 \\ \alpha_3 & -1-\alpha_3 & \alpha_3 & -1-\alpha_3 \\ -1-\alpha_3 & \alpha_3 & -1-\alpha_3 & \alpha_3 \end{pmatrix}$$

Donde, $\det M = 135(2+\sqrt{5})$. Usando a Equação 2.5, dado $v \in \mathcal{M}$, tem-se:

$$\begin{aligned} |\sigma_{\mathbb{K}}(v)|^2 &= 81X_1^2 + 81X_2^2 + 6X_3^2 + 6X_4^2 - 18X_1X_2 + 12X_1X_3 - 18X_1X_4 - 18X_2X_3 + 12X_2X_4 - 8X_3X_4 \\ &= (3X_1 - 3X_2)^2 + (6X_1 + X_3)^2 + (6X_1 - X_4)^2 + (6X_2 + X_4)^2 + (6X_2 - X_3)^2 + (2X_3 - 2X_4)^2 \\ &\quad -6(X_1X_4 + X_2X_3) \end{aligned}$$

Donde, $|\sigma_{\mathbb{K}}(v)|^2$ assume valor mínimo quando $X_1 = 0$, $X_2 = 0$, $X_3 = 1$ e $X_4 = 1$. Neste caso, temos $|\sigma_{\mathbb{K}}(v)|^2 = 4$ consequentemente, $|\sigma_{\mathbb{K}}(v)| = 2$ e portanto, $\rho = 1$. Logo,

$$\delta = \frac{1}{135(2+\sqrt{5})} \approx 0,001$$

- $\mathbb{K} = \mathbb{Q}(\zeta_{24})^+$

Neste caso, o grupo de Galois não é cíclico, já que, $Gal(\mathbb{K}|\mathbb{Q}) =< (\sigma_5, \sigma_7) >$. Escolhemos o $\mathbb{Z}$-módulo $\mathcal{M}$ de $\mathbb{K}$, cuja base é formada por $1+2\alpha_1$, $-2+\alpha_2$, $\sigma_5(1+2\alpha_1)$ e $\sigma_5(-2+\alpha_2)$. Assim, temos que $\mathcal{B} = \{1+2\alpha_1, 1+2\alpha_1-2\alpha_3, -2+\alpha_2, -2-\alpha_2\}$ forma uma $\mathbb{Z}$-base para $\mathcal{M}$. Também, pela Proposição 2.3.2, a imagem de um $\mathbb{Z}$-módulo pelo homomorfismo de Minkowski é um reticulado, cujo volume é o valor absoluto do determinante da matriz $M = (\sigma_i(x_j))$. No caso anterior, estávamos considerando σ_1 como sendo a função identidade, σ_2 o gerador do grupo de Galois que naquele caso era σ_2, $\sigma_3 = \sigma_2^2$ e $\sigma_4 = \sigma_2^3$, no entanto, neste caso não há um único gerador do grupo de Galois, portanto, consideramos σ_1 como sendo a função identidade, $\sigma_2 = \sigma_5$, $\sigma_3 = \sigma_7$ e $\sigma_4 = \sigma_5 \circ \sigma_7$, donde temos:

$$M = \begin{pmatrix} 1+2\alpha_1 & 1+2\alpha_1-2\alpha_3 & 1-2\alpha_1+2\alpha_3 & 1-2\alpha_1 \\ 1+2\alpha_1-2\alpha_3 & 1+2\alpha_1 & 1-2\alpha_1 & 1-2\alpha_1+2\alpha_3 \\ -2+\alpha_2 & -2-\alpha_2 & -2-\alpha_2 & -2+\alpha_2 \\ -2-\alpha_2 & -2+\alpha_2 & -2+\alpha_2 & -2-\alpha_2 \end{pmatrix}$$

Donde, $\det M = 768$.

Usando a Equação 2.5, dado $v \in \mathcal{M}$, tem-se:

$$\begin{aligned}|\sigma_{\mathbb{K}}(v)|^2 &= 36X_1^2 + 36X_2^2 + 28X_3^2 + 28X_4^2 + 40X_1X_2 - 16X_1X_3 - 16X_1X_4 - 16X_2X_3 - 16X_2X_4 + 8X_3X_4 \\ &= (5X_1 + 4X_2)^2 + (2X_1 - 4X_3)^2 + (2X_1 - 4X_4)^2 + (4X_2 - 2X_3)^2 + (2X_2 - 2X_4)^2 + (2X_3 + 2X_4)^2 \\ &\quad +3X_1^2 + 4X_3^2 + 4X_4^2 - 8X_2X_4\end{aligned}$$

Donde, $|\sigma_{\mathbb{K}}(v)|^2$ assume valor mínimo quando $X_1 = 0$, $X_2 = 0$, $X_3 = 1$ e $X_4 = 0$, ou, $X_1 = 0$, $X_2 = 0$, $X_3 = 0$ e $X_4 = 1$. Assim, temos $|\sigma_{\mathbb{K}}(v)|^2 = 28$ consequentemente, $|\sigma_{\mathbb{K}}(v)| = 2\sqrt{7}$ e portanto, $\rho = \sqrt{7}$. Logo,

$$\delta = \frac{\sqrt{7}^4}{768} = \frac{49}{768} \approx 0,0638$$

A Proposição 2.3.3, nos garante que aplicando o homomorfismo de Minkowski no anel de elementos inteiros obtemos um reticulado, cujo o volume correspondente é dado pela raiz quadrada do módulo do discriminante do corpo. Além disso, pela Observação 2.4.1, o raio de empacotamento é igual a 1. Portanto,

$$\begin{aligned}\delta(\sigma_{\mathbb{Q}(\zeta_{15})^+})(\mathcal{O}_{\mathbb{Q}(\zeta_{15})^+}) &= \frac{1}{15\sqrt{5}} \approx 0,0298 \\ \delta(\sigma_{\mathbb{Q}(\zeta_{16})^+})(\mathcal{O}_{\mathbb{Q}(\zeta_{16})^+}) &= \frac{1}{2^5\sqrt{2}} \approx 0,0220 \\ \delta(\sigma_{\mathbb{Q}(\zeta_{20})^+})(\mathcal{O}_{\mathbb{Q}(\zeta_{20})^+}) &= \frac{1}{20\sqrt{5}} \approx 0,0223 \\ \delta(\sigma_{\mathbb{Q}(\zeta_{24})^+})(\mathcal{O}_{\mathbb{Q}(\zeta_{24})^+}) &= \frac{1}{2^4 \cdot 3} \approx 0,0208 \\ \delta(\sigma_{\mathbb{Q}(\zeta_{30})^+})(\mathcal{O}_{\mathbb{Q}(\zeta_{30})^+}) &= \frac{1}{15\sqrt{5}} \approx 0,0298\end{aligned}$$

Referências Bibliográficas

[1] CONWAY, J. H.; SLOANE, N. J. A. Sphere Packings, Lattices and Groups. New York: Springer Verlang,3rd ed, 1999.

[2] INTERLANDO, J. C.; LOPES,J. O. D.; NETO, T. P. da N. The Discriminant of Abelian Number Fields. Journal of Algebra and its Applications. Vol. 5, No. 1. págs: 35-41, 2006.

[3] LANG, S. Algebraic Number Theory. New York: Springer-Verlag, 1986.

[4] MARCUS, D. A. Number Fields. New York: Springer-Verlag, 1977.

[5] MONTEIRO, L. H. J. Teoria de Galois Impa, 1969.

[6] MORANDI, P. Field and Galois Theory Graduate Texts in Mathematics - Springer-Verlag, 1996.

[7] MOREIRA, C. G.; SALDANHA, N. Primos de Mersenne (e outros primos muito grandes) Publicações Matemáticas - Impa, 3º ed, 2008.

[8] RIBENBOIM, P. Classical Theory of Algebraic Numbers Springer-Verlag, New York, 2001.

[9] ROTMAN, J. J. An Introduction to the Theory of Groups Springer-Verlag, 1934, 4th ed.

[10] SAMUEL, P. Algebraic Theory of Numbers. Hermann, 1970.

[11] STEWART, I. N. and Tall; D. O. Algebraic Number Theory. Champman and Hall, 1986.

[12] WASHINGTON, L. C. Introduction to Cyclotomic Fields. Springer-Verlag, New York, 1982.

Índice Remissivo