Universidade Estadual Paulista

Campus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Corpos abelianos com aplicações

Oyran Silva Rayzaro

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Dissertação apresentada ao Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista, Câmpus São José do Rio Preto, como parte dos requisitos para a obtenção do título de Mestre em Matemática

São José do Rio Preto

Fevereiro - 2009

OYRAN SILVA RAYZARO

Corpos abelianos com aplicações

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

BANCA EXAMINADORA

Prof. Dr. Antonio Aparecido de Andrade
Professor Doutor
UNESP - São José do Rio Preto-SP

Prof. Dr. Andréia Cristina Ribeiro
Professor Doutor
UFMS - Paranaíba-MS

Prof. Dr. Jéfferson Luiz Rocha Bastos
Professor Doutor
UNESP - São José do Rio Preto-SP

São José do Rio Preto, 27 de fevereiro de 2009

Aos meus pais,
Carlos e Sônia
e aos meus queridos irmãos,
Moara e Ubirae
dedico.

Agradecimentos

Primeiramente agradeço a DEUS por todas as oportunidades maravilhosas que obtive em minha vida.

Agradeço aos meus pais, Carlos e Sônia, e meus irmãos Moara e Ubirae, pelo amor, paciência, respeito e confiança.

Agradeço aos meus avós maternos Jair e Rosa e aos meus avós paternos Orivaldo (in memoriam) e Arvelina pelo incentivo, apoio e pelos ensinamentos da vida.

Agradeço muito ao meu orientador, Antônio Aparecido de Andrade, pela orientação, amizade e paciência. Por dar-me a oportunidade de aprender com ele e pelos conselhos acadêmicos, profissionais e humanos.

Agradeço à banca examinadora: Prof. Dr. Andréia Cristina Ribeiro, pela disponibilidade, ao Prof. Jéfferson Luiz Rocha Bastos também pela disponibilidade.

Agradeço também à todos os professores do departamento de matemática do Ibilce, em especial aos professores Dr. Cláudio Aguinaldo Buzzi e Dr. Maria Gorete Carreira Andrade, pelo incentivo, simpatia e acolhida desde o início.

Agradeço também os professores e amigos da Unesp - Presidente Prudente, em particular aos professores José Roberto Nogueira e Marcelo Messias, e aos amigos Eder Ritiz e Rogério Galante.

Aos amigos da pós-graduação, pela agradável convivência, em especial aos amigos Ana Paula Tremura e Ruikson Sillas e aos amigos peruanos Rafael Asmat e Rodiak Nicolai.

À CAPES, pelo apoio financeiro.

A todos que de alguma forma contribuíram para a conclusão deste trabalho.

Resumo

Neste trabalho vemos que a imagem de um ideal do anel dos inteiros dos corpos de números, via o homomorfismo de Minkowski, é um reticulado, chamado de reticulado algébrico. Assim, o principal objetivo deste trabalho é a construção de reticulados algébricos de dimensão $2, 4, 6$ e 8, com densidade de centro ótimo.

Palavras chave: corpos ciclotômicos, reticulados algébricos, densidade de centro, forma quadrática.

Abstract

In this work, we see that the image of an ideal from the algebraic integer ring of the numbers fields by the Minkowski homomorphism is a lattice, named algebraic lattice. In this way, the main aim of this work is the construction of algebraic lattices of dimensions 2,4,6 and 8, with the center density excellent.

Key words: cyclotomic fields, algebraic lattices, center density, quadratic form.

Sumário

Introdução

No Congresso Internacional de Matemática, realizado em Paris em 1900, David Hilbert citou uma seleta lista de 23 problemas abertos, entre estes o 18° problema, cujo desafio era o de encontrar empacotamentos esféricos com alta densidade.

Entende-se por empacotamento esférico à distribuição de esferas de mesmo raio no $\mathbb{R}^n$, de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Assim, defini-se densidade de empacotamento esférico, como a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

O maior interesse nos empacotamentos esféricos são os conjuntos constituídos pelos centros das esferas formando um subgrupo discreto do $\mathbb{R}^n$ e o raio, chamado de empacotamentos reticulados.

O estudo de reticulados começou a despertar grande interesse entre os matemáticos por volta de 1950, quando o matemático Claude A. Shannon publicou um artigo mostrando a relação entre empacotamentos esféricos com alta densidade com códigos corretores de erros eficientes.

Na Teoria Algébrica dos Números, utilizando a técnica descrita por Minkowiski, podemos gerar reticulados através do anel de inteiros dos corpos numéricos, chamados de reticulados algébricos. Neste trabalho, o principal objetivo é a construção de reticulados algébricos. O trabalho está dividido em 5 capítulos.

No Capítulo 1, apresentamos alguns resultados básicos da teoria algébrica dos números, que servirá de base para os próximos capítulos. Assim, apresentamos o conceito de um A-módulo, e algumas de suas propriedades, os elementos inteiros, algébricos, anel de inteiros algébricos, e algumas de suas principais propriedades.

Também apresentamos os elementos algébricos e as extensões algébricas, em particular, os corpos de números que são extensões finitas dos racionais. Definimos também, a função traço, a função norma, o discriminante de uma n-upla, as formas quadráticas e também algumas propriedades destas funções. Em seguida, mostramos que o anel de inteiros do corpo de frações de um anel principal A é um A-módulo livre de posto finito. Por fim, apresentamos um estudo rápido sobre os anéis Noetherianos e de Dedekind, apresentando algumas de suas principais propriedades, e introduzimos o conceito de norma de um ideal do anel de inteiros algébricos, que será muito útil no cálculo da densidade de centro dos reticulados algébricos.

No capítulo 2, apresentamos o conceito de duas extensões algébricas abelianas, a saber, os corpos quadráticos e os corpos ciclotômicos, apresentando resultados de como determinar seus anéis de inteiros algébricos e seus discriminantes. Além disso, verificamos quando o grupo Z_n^* é cíclico e apresentamos métodos de como determinar anéis de inteiros algébricos dos subcorpos de $\mathbb{Q}(\zeta_p)$.

O capítulo 3 representa a parte central deste trabalho, pois nele apresentamos métodos que nos ajuda a decompor os ideais primos em uma determinada extensão, e apresentamos o conceito de reticulados e uma tabela de densidade de centro de reticulados conhecidos na literatura. Lembramos que até a dimensão 8 é provado que são os que possui densidade de centro ótima.

No Capítulo 4, apresentamos resultados sobre formas quadráticas via corpos ciclotômicos, que nos auxiliará na determinação da densidade de centro de um reticulado algébrico. Assim, apresentamos resultados sobre formas quadráticas via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$, $\mathbb{Q}(\zeta_{pq})$, com p, q primos distintos e r um inteiro maior ou igual a 1.

O Capítulo 5, tem como objetivo apresentar resultados que facilite o cálculo da densidade de centro dos reticulados algébricos. Além disso, apresentamos exemplos de reticulados algébricos obtidos via os corpos ciclotômicos, $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$ de dimensão 2, 4, 6 e 8, com densidade de centro ótima. Lembramos, que o uso do software MATHEMATICA foi indispensável nos cálculos apresentado neste capítulo.

Capítulo 1

Teoria Algébrica dos Números

1.1 Introdução

Neste capítulo, apresentamos alguns resultados básicos da teoria algébrica dos números, que servirá de base para os próximos capítulos. Na Seção 1.2, apresentamos o conceito de um A-módulo, e algumas de suas propriedades. Na Seção 1.3, apresentamos os elementos inteiros, anel de inteiros, e algumas de suas principais propriedades. Na Seção 1.4, apresentamos os elementos algébricos e as extensões algébricas, em particular, os corpos de números que são extensões finitas dos racionais. Na Seção 1.5, apresentamos a função traço, a função norma, o discriminante de uma n-upla, e também algumas propriedades destas funções. Em seguida, veremos que o anel de inteiros do corpo de frações de um anel principal A é um A-módulo livre de posto finito. Na Seção 1.6, apresentamos a definição de formas quadráticas, e algumas de suas principais propriedades, que serão muito úteis no estudo dos reticulados para determinar sua densidade de centro. Na Seção 1.7, apresentamos um estudo rápido sobre os anéis Noetherianos e de Dedekind, apresentando algumas de suas principais propriedades. Na Seção 1.8, introduzimos o conceito de norma de um ideal do anel dos inteiros algébricos, que será muito útil no cálculo da densidade de centro dos reticulados algébricos.

1.2 Módulos

Nesta seção, apresentamos o conceito de módulos e algumas de suas principais propriedades.

Definição 1.2.1 *Seja A um anel comutativo com unidade. Um A-***módulo** *M é um grupo abeliano aditivo, munido com uma aplicação $\alpha : A \times M \to M$, definida por $\alpha(a, m) = am\,(a \in A\, e\, m \in M)$, satisfazendo;*

(a) $(a + b)m = am + bm$,

(b) $a(m + n) = am + an$,

(c) $a(bm) = (ab)m$,

(d) $1m = m$,

para todo $a, b \in A$ e para todo $m, n \in M$.

Definição 1.2.2 *Sejam A um anel comutativo com unidade, M um A-módulo e $N \subset M$ um subconjunto não vazio. Dizemos que N é um A-***submódulo** *de M se é um subgrupo aditivo de M, e que se $n \in N$ e $a \in A$, então $an \in N$.*

Definição 1.2.3 *Um A-módulo M é* ***finitamente gerado*** *se existem elementos $x_1, \ldots, x_n \in M$ tal que $M = Ax_1 + \ldots + Ax_n$. Neste caso, dizemos que $\{x_1, \ldots, x_n\}$ é um sistema de geradores de M. Se o conjunto de elementos $\{x_1, \ldots, x_n\}$ forem linearmente independente sobre A, dizemos que $\{x_1, \ldots, x_n\}$ forma uma* ***base*** *para M. Todo A-módulo M que possui uma base é chamado de A-****módulo livre****, cujo o número de elementos da base é chamado* ***posto*** *de M.*

Observação 1.2.1 *Nem todo A-módulo finitamente gerado possui uma base, e nem todo A-submódulo N de um A-módulo livre também é livre.*

Teorema 1.2.1 *([1], p.21) Se A é um anel principal, M um A-módulo livre de posto n, e N um A-submódulo de M, então:*

(a) *N é livre de posto q, $0 \leq q \leq n$,*

(b) *Se $N \neq \emptyset$, então existe uma base $\{e_1, \ldots, e_n\}$ de M e elementos $a_1, \ldots, a_q \in A$ não todos nulos, tais que $\{e_1a_1, \ldots, e_qa_q\}$ é uma base de N e a_i divide a_{i+1}, com $1 \leq i \leq q - 1$.*

1.3 Elementos Inteiros

Nesta seção, apresentamos a definição de elementos inteiros, anel dos inteiros e algumas de suas principais propriedades.

Definição 1.3.1 *Sejam B um anel e $A \subset B$ um subanel. Dizemos que $\alpha \in B$ é um* ***elemento inteiro*** *sobre A se α for raiz de um polinômio mônico com coeficientes em A, ou seja, existem $a_1, \ldots, a_{n-1} \in A$ não todos nulos, tal que*

$$p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

onde esta equação é chamada de ***equação de dependência inteira*** *de α sobre A.*

Teorema 1.3.1 *([1], p.27) Sejam B um anel, A um subanel de B e α um elemento de B. As seguintes afirmações são equivalentes:*

(a) *α é um elemento inteiro sobre A;*

(b) *O anel $A[\alpha]$ é um A-módulo finitamente gerado;*

(c) *Existe um subanel R de B tal que R é um A-módulo finitamente gerado contendo A e α.*

Proposição 1.3.1 *([1], p.28) Sejam B um anel, A um subanel de B. Considere $\{\alpha_1, \alpha_2, , \ldots, \alpha_n\} \subset B$, se α_1 é um elemento inteiro sobre A e α_i é um elemento inteiro sobre $A[\alpha_1, \ldots, \alpha_{i-1}]$, para todo $i = 1, \ldots, n$, então $A[\alpha_1, \ldots, \alpha_n]$ é um A-módulo finitamente gerado.*

Corolário 1.3.1 *([1], p.29) Sejam B um anel, A um subanel de B. Considere $\mathbb{A}_{\mathbb{B}} = \{\alpha \in B, \alpha$ é um elemento inteiro sobre $A\}$. Se α e β são elementos de $\mathbb{A}_{\mathbb{B}}$, então $\alpha \pm \beta, \alpha\beta \in \mathbb{A}_B$, ou seja, $\mathbb{A}_B$ é um anel.*

Definição 1.3.2 *O anel $\mathbb{A}_{\mathbb{B}} = \{\alpha \in B : \alpha$ é um elemento inteiro sobre $A\}$ é chamado de* ***anel de elementos inteiros*** *de A em B, ou de B sobre A.*

Definição 1.3.3 *Sejam B um anel e A um subanel de B. Dizemos que B é* ***inteiro*** *sobre A, se todo elemento de B é um elemento inteiro sobre A, isto é, $\mathbb{A}_B = B$.*

Proposição 1.3.2 *([1], p.29) Sejam C um anel, B um subanel de C e A um subanel de B. Assim C é inteiro sobre A se, e somente se, B é inteiro sobre A e C é inteiro sobre B.*

Proposição 1.3.3 *([1], p.29) Se $A \subset B$ são anéis, onde B é inteiro sobre A, então A é um corpo se, e somente se, B é um corpo.*

Definição 1.3.4 *Sejam A um domínio e $\mathbb{K} = \left\{\frac{a}{s}; a, s \in A, s \neq 0\right\}$ o corpo de frações de A. Dizemos que A é **integralmente fechado** se $\mathbb{A}_{\mathbb{K}} = A$.*

Proposição 1.3.4 *([1], p.30) Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. O anel dos elementos inteiros $\mathbb{A}_{\mathbb{K}}$ é integralmente fechado.*

Proposição 1.3.5 *([1], p.30) Se A é um domínio principal, então A é integralmente fechado.*

Observação 1.3.1 *Todo domínio fatorial é integralmente fechado, pois é principal. Note que o anel $\mathbb{Z}$ é integralmente fechado, pois é um anel principal.*

1.4 Corpos de Números

Nesta seção, apresentamos os conceitos de elementos algébricos e extensões algébricas de um corpo. Em particular, apresentamos as extensões do corpo dos racionais, que são chamados de corpos de números, e também apresentamos alguns resultados principais destas extensões.

Definição 1.4.1 *Sejam A um anel e $\mathbb{K}$ um corpo onde $\mathbb{K} \subset A$. Dizemos que $\alpha \in A$ é um **elemento algébrico** sobre $\mathbb{K}$ se existe um polinômio não nulo $f(x) \in \mathbb{K}[x]$, tal que $f(\alpha) = 0$. Caso contrário, α é chamado elemento **transcendente** sobre $\mathbb{K}$. O polinômio mônico $f(x) \in \mathbb{K}[x]$ de menor grau tal que $f(\alpha) = 0$ é chamado de **polinômio minimal** de α sobre $\mathbb{K}$.*

Definição 1.4.2 *Sejam A um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subset A$. Se todo elemento de A é algébrico sobre $\mathbb{K}$ dizemos que A é* ***algébrico*** *sobre $\mathbb{K}$. Agora, no caso quando A for um corpo, A é chamado de* ***extensão algébrica*** *de $\mathbb{K}$.*

Definição 1.4.3 *Se $\mathbb{K} \subset \mathbb{L}$ são corpos, tal que $dim_{\mathbb{K}}\mathbb{L} = n$, então $\mathbb{L}$ é chamado uma* ***extensão*** *do corpo $\mathbb{K}$, e n é chamado o* ***grau*** *de $\mathbb{L}$ sobre $\mathbb{K}$.*

Definição 1.4.4 *Sejam $\mathbb{K}, \mathbb{L}$ corpos tal que $\mathbb{K} \subseteq \mathbb{L}$. Chamamos de* ***dimensão*** *de $\mathbb{L}$ sobre $\mathbb{K}$, visto como espaço vetorial, o grau da extensão de $\mathbb{L}$ sobre $\mathbb{K}$, denotada por $[\mathbb{L} : \mathbb{K}]$.*

Teorema 1.4.1 *([1], p.30) Sejam $\mathbb{K}, \mathbb{L}$ corpos tal que $\mathbb{K} \subseteq \mathbb{L}$ e α um elemento de $\mathbb{L}$. As seguintes afirmações são equivalentes:*
(a) *α é algébrico sobre $\mathbb{K}$,*
(b) *$[\mathbb{K}(\alpha) : \mathbb{K}]$ é finito.*

Corolário 1.4.1 *([1], p.31) Toda extensão finita é algébrica.*

Definição 1.4.5 *Um* ***corpo de números*** *$\mathbb{K}$ é uma extensão algébrica finita do corpo dos números racionais. Os elementos de $\mathbb{K}$ que são elementos inteiros sobre $\mathbb{Z}$ são chamados de* ***inteiros algébricos****, e o conjunto desses elementos é chamado* ***anel de inteiros algébricos*** *de $\mathbb{K}$.*

Teorema 1.4.2 *([2], p.47) Se α é raiz de um polinômio mônico, onde os coeficientes são inteiros algébricos, então α é inteiro algébrico.*

Teorema 1.4.3 *([2], p.40) Se $\mathbb{K}$ é um corpo de números, então existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. O elemento θ é chamado* ***elemento primitivo****.*

Teorema 1.4.4 *([1], p.31) Sejam $\mathbb{K}, \mathbb{L}$ e $\mathbb{M}$ corpos, com $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. Então $\mathbb{M}$ é uma extensão algébrica finita de $\mathbb{L}$ e $\mathbb{L}$ é uma extensão algébrica finita de $\mathbb{K}$, se e somente se, $\mathbb{M}$ é uma extensão algébrica finita de $\mathbb{K}$. Consequentemente, $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.*

Definição 1.4.6 *Sejam $\mathbb{L}$ e $\mathbb{M}$ extensões de um corpo $\mathbb{K}$. Dizemos que $\alpha \in \mathbb{L}$ e $\alpha' \in \mathbb{M}$ são **conjugados** sobre $\mathbb{K}$ se existe um $\mathbb{K}$-isomorfismo φ de $\mathbb{K}(\alpha)$ em $\mathbb{K}(\alpha')$ tal que $\varphi(\alpha) = \alpha'$. Assim, dizemos que $\mathbb{L}$ e $\mathbb{M}$ são **conjugados** sobre $\mathbb{K}$, se existe um $\mathbb{K}$-isomorfismo φ de $\mathbb{L}$ em $\mathbb{M}$ tal que $\varphi(a) = a$, para todo $a \in \mathbb{K}$.*

1.5 Norma, Traço e Discriminante

Nesta seção, apresentamos os conceitos de função traço, de função norma, do polinômio característico e do discriminante de uma n-upla, apresentamos também algumas de suas principais propriedades. Em seguida, veremos que o anel dos inteiros do corpo de frações de um anel principal A, é um A-módulo livre de posto finito.

Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto n e $\{e_1, e_2, \ldots, e_n\}$ uma base de B sobre A. Seja $\psi_\alpha : B \to B$ um homomorfismo de anéis definido por $\psi_\alpha(x) = \alpha x$, com $\alpha \in B$. Assim,

$$\begin{cases} \psi_\alpha(e_1) = a_{11}e_1 + a_{12}e_2 + \ldots + a_{1n}e_n \\ \quad \vdots \\ \psi_\alpha(e_n) = a_{n1}e_1 + a_{n2}e_2 + \ldots + a_{nn}e_n, \end{cases}$$

onde $a_{ij} \in A$, para $1 \leq i, j \leq n$, e deste modo

$$\begin{bmatrix} \psi_\alpha(e_1) \\ \vdots \\ \psi_\alpha(e_n) \end{bmatrix} = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}.$$

Definição 1.5.1 *Definimos o **traço** de um elemento $\alpha \in B$ por $Tr_{B/A}(\alpha) = \sum_{i=1}^{n} a_{ii}$, a **norma** de α por $N_{B/A}(\alpha) = det(a_{ij})$ e o **polinômio característico** de α por $m_{B/A}(x) = det(xI - [a_{ij}])$.*

Proposição 1.5.1 *([1], p.36) Se $\mathbb{K}$ é um corpo de característica zero ou um corpo finito, $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$ de grau n, α um elemento de $\mathbb{L}$ e $\alpha_1, \ldots, \alpha_n$*

as raízes do polinômio minimal de α sobre $\mathbb{K}$, então $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \ldots + \alpha_n$, $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1\alpha_2 \ldots \alpha_n$ e $m(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$.

Proposição 1.5.2 *([1], p.38) Se A é um domínio, $\mathbb{K}$ seu corpo de frações de característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$, e α um elemento de $\mathbb{L}$ inteiro sobre A, então os coeficientes do polinômio característico $m(x)$ de α são elementos inteiros sobre A. Em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos inteiros sobre A.*

Corolário 1.5.1 *([1], p.38) Se A é um anel integralmente fechado, então os coeficientes do polinômio característico $m(x)$ são elementos de A, em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de A.*

Agora, apresentamos algumas propriedades do traço e da norma, que serão muito úteis no decorrer de nosso trabalho.

Proposição 1.5.3 *Se $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ são corpos de números, α e $\alpha' \in \mathbb{M}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:*

(a) $Tr_{\mathbb{M}/\mathbb{K}}(\alpha+\alpha') = Tr_{\mathbb{M}/\mathbb{K}}(\alpha) + Tr_{\mathbb{M}/\mathbb{K}}(\alpha')$;

(b) $Tr_{\mathbb{M}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{M}/\mathbb{K}}(\alpha)$;

(c) $Tr_{\mathbb{M}/\mathbb{K}}(a) = [\mathbb{M}:\mathbb{K}]a$;

(d) $Tr_{\mathbb{M}/\mathbb{K}}(\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(\alpha))$;

(e) $N_{\mathbb{M}/\mathbb{K}}(\alpha\alpha') = N_{\mathbb{M}/\mathbb{K}}(\alpha)N_{\mathbb{M}/\mathbb{K}}(\alpha')$;

(f) $N_{\mathbb{M}/\mathbb{K}}(a) = a^{[\mathbb{M}:\mathbb{K}]}$;

(g) $N_{\mathbb{M}/\mathbb{K}}(a\alpha) = a^{[\mathbb{M}:\mathbb{K}]}N_{\mathbb{M}/\mathbb{K}}(\alpha)$;

(h) $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\alpha))$;

e em particular, se $\beta \in \mathbb{L}$, então:

(i) $Tr_{\mathbb{M}/\mathbb{K}}(\beta) = [\mathbb{M}:\mathbb{L}]Tr_{\mathbb{L}/\mathbb{K}}(\beta)$;

(j) $N_{\mathbb{M}/\mathbb{K}}(\beta) = N_{\mathbb{L}/\mathbb{K}}(\beta)^{[\mathbb{M}:\mathbb{L}]}$.

Definição 1.5.2 *Sejam $A \subset B$ anéis tal que B é um A-módulo livre de posto finito n e $(\alpha_1, \ldots, \alpha_n) \in B^n$. Definimos o* ***discriminante*** *de $(\alpha_1, \ldots, \alpha_n)$ por*

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

Exemplo 1.5.1 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *um corpo de números e* $\{1, \sqrt{5}\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$*, então*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{5}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{5}) \\ Tr(\sqrt{5}) & Tr(\sqrt{5})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 10 \end{vmatrix} = 20.$$

Observação 1.5.1 *Se* $\{\alpha_1, \ldots, \alpha_n\}$ *e* $\{\beta_1, \ldots, \beta_n\}$ *são duas bases de* B *sobre* A*, então a matriz* (a_{ij})*, que expressa uma base em termos da outra, admite matriz inversa com entradas em* A*. Assim, ambos os* $det(a_{ij})$ *e* $det(a_{ij})^{-1}$ *são inversíveis em* A*, e portanto os discriminantes dessas duas bases são associados.*

Proposição 1.5.4 *([1], p.38) Sejam* $A \subseteq B$ *anéis tal que* B *é um* A*-módulo livre de posto finito* n*, e* $(\alpha_1, \ldots, \alpha_n) \in B^n$*. Se* $(\beta_1, \ldots, \beta_n) \in B^n$ *é um outro conjunto de elementos de* B *tais que* $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$*, onde* $a_{ij} \in A$*, para* $i, j = 1, 2, \ldots, n$*, então*

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

Exemplo 1.5.2 *Vimos no Exemplo 1.5.1, que o discriminante da base* $\{1, \sqrt{5}\}$ *do corpo* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *é 20. Tomando outra base para* $\mathbb{K}$*, por exemplo* $\{1+\sqrt{5}, 3-\sqrt{5}\}$*, tem-se pela Proposição 1.5.4, que* $D_{\mathbb{K}/\mathbb{Q}}(1+\sqrt{5}, 3-\sqrt{5}) = 320$*.*

Definição 1.5.3 *Sejam* $A \subset B$ *anéis tal que* B *é um* A*-módulo livre de posto finito* n*. O* ***discriminante*** *de* B *sobre* A *é um ideal principal em* A*, definido por,*

$$D_{B/A} = \langle D_{B/A}(\alpha_1, \ldots, \alpha_n) \rangle,$$

onde $\{\alpha_1, \ldots, \alpha_n\}$ *é uma base de* B *sobre* A*.*

Lema 1.5.1 (Lema de Dedekind) *([1], p.39) Se* G *é um grupo,* $\mathbb{K}$ *um corpo e* $\{\sigma_1, \ldots, \sigma_n\}$ *homomorfismos distintos de* G *no grupo multiplicativo* $\mathbb{K}^*$*, então* $\{\sigma_1, \ldots, \sigma_n\}$ *são linearmente independente sobre* $\mathbb{K}$*.*

Proposição 1.5.5 *([1], p.39) Se* $\mathbb{K}$ *é um corpo finito ou de característica zero,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n*, e* $\{\sigma_1, \ldots, \sigma_n\}$ *os* $\mathbb{K}$*-isomorfismos distintos de* $\mathbb{L}$ *em um corpo algebricamente fechado* $\mathbb{M}$ *contendo* $\mathbb{K}$*, e se* $\{\alpha_1, \ldots, \alpha_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$*, então*

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2 \neq 0.$$

Exemplo 1.5.3 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *e* $\alpha = a + b\sqrt{5} \in \mathbb{K}$. *Como* $[\mathbb{K} : \mathbb{Q}] = 2$, *segue que existem dois* $\mathbb{Q}$*-isomorfismos,* σ_1 *e* σ_2 *onde* $\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ *e* $\sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$. *Como* $\{1, \sqrt{5}\}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$, *obtemos que*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{5}) = det(\sigma_i(\alpha_j))^2 = \begin{vmatrix} 1 & 1 \\ \sqrt{5} & -\sqrt{5} \end{vmatrix}^2 = (-2\sqrt{5})^2 = 20$$

Proposição 1.5.6 *([1], p.41) Se* $\mathbb{K}$ *é um corpo finito ou de característica zero,* $\mathbb{L} = \mathbb{K}(\alpha)$ *uma extensão finita de* $\mathbb{K}$ *de grau* n, *e* $m(x)$ *o polinômio minimal de* α *sobre* $\mathbb{K}$, *então*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(m'(\alpha)),$$

onde $m'(x)$ *é a derivada de* $m(x)$.

Exemplo 1.5.4 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *e* $m(x) = x^2 - 5$ *o polinômio minimal de* $\alpha = \sqrt{5}$ *sobre* $\mathbb{Q}$. *Como* $m'(\sqrt{5}) = 2\sqrt{5}$ *e* $N_{\mathbb{K}/\mathbb{Q}}(m'(\sqrt{5})) = N_{\mathbb{K}/\mathbb{Q}}(2\sqrt{5}) = -20$, *segue que* $D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{5}) = (-1)^{\frac{1}{2}2(2-1)} N_{\mathbb{K}/\mathbb{Q}}(m'(\sqrt{5})) = (-1)(-20) = 20$.

Teorema 1.5.1 *([1], p.40) Se* A *é um anel integralmente fechado,* $\mathbb{K}$ *seu corpo de frações e* $\mathbb{L}$ *uma extensão de* $\mathbb{K}$ *de grau* n, *então o anel de elementos inteiros* $\mathbb{A}_{\mathbb{L}}$ *de* A *em* $\mathbb{L}$ *é um submódulo de um* A*-módulo livre de posto* n. *Em particular, se* A *for um anel principal, então* $\mathbb{A}_{\mathbb{L}}$ *é um* A*-módulo livre de posto* n.

Sejam $\mathbb{L}$ um corpo de números de grau n e $A = \mathbb{Z}$. Como A é principal, pelo Teorema 1.5.1, segue que o anel $\mathbb{A}_{\mathbb{L}}$ de elementos inteiros de $\mathbb{L}$ é um $\mathbb{Z}$-módulo livre de posto n. Dessa forma, chamamos uma $\mathbb{Z}$-base de $\mathbb{A}_{\mathbb{L}}$ de **base integral** e o discriminante de uma base integral é chamado de **discriminante absoluto** do corpo $\mathbb{L}$ e denotado por $D_{\mathbb{L}}$.

1.6 Formas Quadráticas

Nesta seção, apresentamos as formas quadráticas sobre o $\mathbb{R}^n$, que serão indispensáveis no cálculo da densidade de centro dos reticulados.

Definição 1.6.1 *Seja n inteiro. Definimos a* ***forma quadrática*** *sobre $\mathbb{R}^n$ por*

$$Q_n(\underline{x}) = \sum_{i=1}^{n}(x_i)^2 + \sum_{1\leq i\leq j\leq n}(x_i - x_j)^2,$$

onde $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$.

Agora, como $\sum_{1\leq i\leq j\leq n}(x_i - x_j)^2 = (n-1)\sum_{i=1}^{n} {x_i}^2 - 2\sum_{1\leq i\leq j\leq n} x_i x_j$, segue que

$$Q_n(\underline{x}) = n\sum_{i=1}^{n} {x_i}^2 - 2\sum_{1\leq i\leq j\leq n} x_i x_j.$$

Para cada r, s inteiros, também podemos escrever

$$Q_{r,s}(x_1, \ldots, x_r) = \sum_{i=1}^{r} x_i^2 \; + \; s\sum_{1\leq i<j\leq r}(x_i - x_j)^2.$$

Observação 1.6.1 *A forma quadrática $Q_n(\underline{x})$ é uma função positiva, e totalmente simétrica pois $Q_n(x_1, \ldots, x_n) = Q_n(x_{\sigma 1}, \ldots, x_{\sigma n})$ para qualquer permutação σ do conjunto $[1, \ldots, n]$.*

Proposição 1.6.1 *([3], p.64) Se $Q_n(\underline{x})$ é uma forma quadrática, então:*

(a) *o menor valor que $Q_n(x_1, \ldots, x_n)$ assume com entradas inteiras não todas nulos é n.*

(b) *para $a \in \mathbb{Z}^n$, tem-se que $Q_n(\underline{a}) = n$ quando $\underline{a} = \pm(1, 1, \ldots, 1)$ ou $\underline{a} = \pm e_i$, para $i = 1, \ldots, n$, onde $\{e_1, \ldots, e_n\}$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$.*

Lema 1.6.1 *([3], p.76) A forma quadrática $Q_n(a_1, \ldots, a_n)$ não atinge o valor $n+1$, para $(a_1, \ldots, a_n) \in \mathbb{Z}^n$*

Lema 1.6.2 *([3], p.80) Se $Q_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2 + \sum_{1\leq i\leq j\leq n}(x_i - x_j)^2$, e $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{R}^n$, então*

$$Q_n(a_1, \ldots, a_n) = d^2(a, 0) + nd^2(a, \Delta),$$

onde $d^2(a, 0)$ e $d^2(a, \Delta)$ são os quadrados das distâncias euclidianas de $\underline{a}$ até a origem e de $\underline{a}$ até a diagonal do $\mathbb{R}^n$, respectivamente.

Teorema 1.6.1 *([3], p.81) Sejam $a_1, \ldots, a_t$ números inteiros com $t < n$. Se $F(x_{t+1}, \ldots, x_n) = Q_n(a_1, \ldots, a_t, x_{t+1}, \ldots, x_n)$, então F atinge seu valor mínimo com coordenadas inteiras no ponto*

$$(y, \ldots, y), \text{ onde } y = \left[\Big(\sum_{i=1}^{n} a_i \Big)/t + 1 \right],$$

e $[z]$ denota o inteiro mais próximo de z.

Teorema 1.6.2 *([3], p.84) Se $m \in \mathbb{N}$ e $Q'_n(m) = Q_n(m, t, \ldots, t)$, onde $t = [m/2]$, isto é, se $Q'(m)$ é o menor valor que $Q_n(m, x_2, \ldots, x_n)$ assume fazendo $x_2, \ldots, x_n$ variar no conjuntos dos números inteiros, então Q' é uma função crescente de m.*

1.7 Anéis Noetherianos e Anéis de Dedekind

O objetivo, desta seção, é definir os Anéis Noetherianos e os Anéis de Dedekind, e suas principais propriedades.

Definição 1.7.1 *Sejam A um anel e M um A-módulo. Dizemos que M é um A-**módulo Noetheriano**, se satisfaz uma das seguintes condições.*

(a) *Todo conjunto não vazio de submódulos de M contém um elemento maximal.*

(b) *Toda sequência crescente de submódulos de M é estacionária.*

(c) *Todo submódulo de M é finitamente gerado.*

Um anel A é chamado de **Noetheriano**, quando A considerado como um A-módulo for Noetheriano.

Exemplo 1.7.1 *Todo anel principal é Noetheriano, pois todos os seus ideais são submódulos finitamente gerado por um elemento.*

Proposição 1.7.1 *([1], p.46) Sejam A um anel, M um A-módulo e M' um submódulo de M. Então, M é Noetheriano se, e somente se, M' e $\dfrac{M}{M'}$ são Noetherianos.*

Corolário 1.7.1 *([1], p.27) Sejam A um anel. Se $M_1, \ldots, M_n$ são A-módulos Noetherianos, então $M_1 \times \ldots \times M_n$ é um A-módulo Noetheriano.*

Corolário 1.7.2 *([1], p.47) Se A é um anel Noetheriano e M um A-módulo finitamente gerado, então M é um A-módulo Noetheriano.*

Definição 1.7.2 *Um anel A é chamado um **anel de Dedekind**, se A for Noetheriano, integralmente fechado e todo ideal primo não nulo de A é maximal.*

Exemplo 1.7.2 *Se A é um domínio principal, então A é um anel de Dedekind. Por exemplo, $\mathbb{Z}$ é um anel de Dedekind.*

Proposição 1.7.2 *([1], p.47) Se A é um anel Noetheriano e integralmente fechado, $\mathbb{K}$ seu corpo de frações com característica zero, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau n e $\mathbb{A}_{\mathbb{L}}$ o anel de elementos inteiros de A em $\mathbb{L}$, então $A_{\mathbb{L}}$ é um A-módulo finitamente gerado e um anel Noetheriano.*

Proposição 1.7.3 *([1], p.49) Se A é um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau n e $\mathbb{A}_{\mathbb{L}}$ o anel de elementos inteiros de A em $\mathbb{L}$, então $\mathbb{A}_{\mathbb{L}}$ é um anel de Dedekind.*

Definição 1.7.3 *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Dizemos que um A-submódulo I de $\mathbb{K}$ é um **ideal fracionário**, se existe um $d \in A$, não nulo, tal que $dI \subset A$. Quando $d = 1$, dizemos que I é um ideal inteiro.*

Teorema 1.7.1 *([1], p.50) Sejam A um anel de Dedekind e $\mathbb{K}$ seu corpo de frações. Se $\mathfrak{p}$ é um ideal primo de A, então existe um ideal fracionário de A, denominado ideal fracionário inverso de $\mathfrak{p}$, e denotado por $\mathfrak{p}^{-1} = \{x \in \mathbb{K}; x\mathfrak{p} \subset A\}$, tal que $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

1.8 Norma de um Ideal

Nesta seção, definimos a norma de um ideal do anel de inteiros algébricos de um corpo de números e veremos algumas propriedades, dentre elas que a norma é multiplicativa. Para isto, consideramos $\mathbb{K}$ um corpo de números de grau finito n e $\mathbb{A}_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$.

Definição 1.8.1 *Seja* $\mathfrak{a}$ *um ideal de* $\mathbb{A}_{\mathbb{K}}$. *A* ***norma*** *de* $\mathfrak{a}$ *é definida como,*

$$N(\mathfrak{a}) = \#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\right).$$

Observação 1.8.1 *Se* $\alpha \in \mathbb{A}_{\mathbb{K}}$ *e* $\alpha \neq 0$, *então, pelo Corolário 1.5.1, segue que* $N(\alpha) \in \mathbb{A}_{\mathbb{K}}$.

Proposição 1.8.1 *([1], p.52) Se* $\alpha \in \mathbb{A}_{\mathbb{K}}$, *então* $|N(\alpha)| = \#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathbb{A}_{\mathbb{K}}\alpha}\right)$, *onde* $\mathbb{A}_{\mathbb{K}}\alpha = \langle\alpha\rangle$.

Proposição 1.8.2 *([1], p.52) Se* $\mathfrak{a}$ *é um ideal não nulo de* $\mathbb{A}_{\mathbb{K}}$, *então* $N(\mathfrak{a})$ *é finita.*

Proposição 1.8.3 *([1], p.52) Se* $\mathfrak{a}$ *e* $\mathfrak{b}$ *são ideais não nulos de* $\mathbb{A}_{\mathbb{K}}$, *então* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Proposição 1.8.4 *([12], p.84) Se* $\mathfrak{a} \subseteq \mathbb{K}$ *é um ideal, então,*
(a) $N(\mathfrak{a}) \in \mathfrak{a}$
(b) $N(\mathfrak{a}) = 1$ *se, e somente se,* $\mathfrak{a} = \mathbb{A}_{\mathbb{K}}$.

1.9 Conclusão

Neste capítulo vimos alguns resultados da Teoria Algébrica dos Números, que nos auxiliará nos próximos capítulos. Por exemplo, introduzimos o conceito de anéis de inteiros algébricos e discriminante de um corpo $\mathbb{K}$, pois no segundo capítulo, apresentaremos alguns resultados, de como determinar os anéis de inteiros dos corpos quadráticos e dos corpos ciclotômicos. Vimos também algumas propriedades sobre as funções traço e norma, que será muito útil no cálculo da densidade de centro dos reticulados algébricos. Além disto, apresentamos alguns resultados sobre as formas quadráticas, pois veremos no quarto capítulo, a relação entre as formas quadráticas e a função traço aplicada em um elemento de um corpo $\mathbb{K}$ com o seu conjugado.

Capítulo 2

Corpos Abelianos

2.1 Introdução

O objetivo deste capítulo é apresentar o conceito de duas extensões algébricas abelianas, a saber, os corpos quadráticos e os corpos ciclotômicos. Assim, na Seção 2.2, apresentamos os corpos quadráticos, determinando seus correspondentes anéis de inteiros algébricos e discriminantes associados. Na Seção 2.3, apresentamos o grupo $\mathbb{Z}_n^*$, verificando quando este grupo é cíclico. Na Seção 2.4, definimos o polinômio ciclotômico e as extensões ciclotômicas, apresentando algumas de suas principais propriedades. Na Seção 2.5, determinamos os anéis de inteiros algébricos para as extensões ciclotômicas, e alguns resultados que facilitam o cálculo do discriminante destas extensões. Na Seção 2.6, apresentamos resultados sobre corpos abelianos, e como deteminar os anéis de inteiros algébricos dos subcorpos de $\mathbb{Q}(\zeta_p)$.

2.2 Corpos Quadráticos

Nesta seção, apresentamos o conceito de corpos quadráticos, determinando seus anéis de inteiros algébricos, e um método para encontrar seus discriminantes.

Definição 2.2.1 *Um* ***corpo quadrático*** *é um corpo de número* $\mathbb{K}$*, cujo grau da extensão sobre o corpo dos números racionais é* 2*.*

Proposição 2.2.1 *([2], p.67) Os corpos quadráticos são da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*

Demonstração: Seja $\mathbb{K}$ um corpo quadrático. Como $\mathbb{K}$ é um corpo de números, pelo Teorema 1.4.3, segue que existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Sendo $[\mathbb{K} : \mathbb{Q}] = 2$, tem-se que o polinômio minimal de θ sobre $\mathbb{K}$ é dado por $m(x) = x^2 + ax + b$, com $a, b \in \mathbb{Q}$. Assim $\theta^2 + a\theta + b = 0$, e deste modo $\theta = \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$ são as raízes de $m(x)$. Como $2\theta \pm a = \sqrt{a^2 - 4b}$ segue que $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b^2})$. Por outro lado, como $a, b \in \mathbb{Q}$, segue que $a^2 - 4b \in \mathbb{Q}$, e assim $a^2 - 4b = \dfrac{u}{v}$, com $u, v \in \mathbb{Z}$ e $mdc(u, v) = 1$, de modo que u e v não sejam quadrados perfeitos, pois caso contrário, teríamos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $a^2 - 4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, e $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv})$. Agora, supondo que $uv = m^2 d$, com $m, d \in \mathbb{Z}$, e d livre de quadrados, obtemos que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{m^2 d}) = \mathbb{Q}(\sqrt{d})$. □

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático. Se $d > 0$ dizemos que $\mathbb{K}$ é um **corpo quadrático real** e se $d < 0$ dizemos que $\mathbb{K}$ é um **corpo quadrático imaginário**. Note pela Proposição 2.2.1 que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados, tem-se desta forma que $\{1, \sqrt{d}\}$ é uma base de $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

Proposição 2.2.2 *([1], p.35) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com d um inteiro livre de quadrados. Se o elemento $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ é um inteiro algébrico, então $2a$ e $a^2 - db^2$ são números inteiros.*

Demonstração: Se $\alpha \in \mathbb{K}$ é um inteiro algébrico, então existem $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, não todos nulos tal que

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

Tomando σ um automorfismo de $\mathbb{K}$ tal que $\sigma(\sqrt{d}) = -\sqrt{d}$, segue que

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \ldots + a_1\sigma(\alpha) + a_0 = 0,$$

ou seja, $\sigma(\alpha)$ também é um inteiro algébrico de $\mathbb{K}$. Logo, pelo Corolário 1.3.1, tem-se que $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ são inteiros algéricos de $\mathbb{K}$. Além disso, se $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$, então $\alpha + \sigma(\alpha) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = a^2 - db^2 \in \mathbb{Q}$. Por outro lado, como $\mathbb{Z}$ é integralmente fechado, segue que $2a$ e $a^2 - db^2$ são números inteiros. □

Lema 2.2.1 *([2], p.67) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com d um inteiro livre de quadrados. Se o elemento $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ é um inteiro algébrico sobre $\mathbb{Z}$ com $b \neq 0$, então existem u e $v \in \mathbb{Z}$, tal que $u^2 - dv^2 \in 4\mathbb{Z}$, onde $u = 2a$ e $v = 2b$.*

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ um inteiro algébrico sobre $\mathbb{Z}$. O polinômio minimal de α sobre $\mathbb{Q}$ é dado por $m(x) = x^2 - 2ax + a^2 - db^2$. Pela Proposição 2.2.2, tem-se que $2a$ e $a^2 - db^2 \in \mathbb{Z}$, e assim $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Logo $d(2b)^2 \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Portanto $2b \in \mathbb{Z}$, pois caso contrário, no seu denominador existiria um fator primo p que apareceria na forma p^2 no denominador de $(2b)^2$ e como d é livre de quadrados teríamos que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Assim, tomando $a = \dfrac{u}{2}$ e $b = \dfrac{v}{2}$, com $u, v \in \mathbb{Z}$, obtemos que $u^2 - dv^2 \in 4\mathbb{Z}$. □

Teorema 2.2.1 *([2], p.35) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde d é um inteiro livre de quadrados. O anel dos inteiros algébricos $\mathbb{A}_{\mathbb{K}}$ de $\mathbb{K}$ é dada por:*

(a) $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$, *se* $d \equiv 2$ *ou* $d \equiv 3 (mod\, 4)$.

(b) $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$, *se* $d \equiv 1 (mod\, 4)$.

Demonstração: **(a)** Se $d \equiv 2$ ou $d \equiv 3 (mod\, 4)$, então u e v, dados como no Lema 2.2.1, são pares, pois caso contrário, se v fosse ímpar teríamos $v^2 \equiv 1 (mod\, 4)$. Deste modo, como $u^2 - dv^2 \in 4\mathbb{Z}$, segue que $u^2 - d \in 4\mathbb{Z}$, e assim $d \equiv 1 (mod\, 4)$ ou $d \equiv 0 (mod\, 4)$, o que é um absurdo. Portanto v é par. Logo $v^2 \equiv 0 (mod\, 4)$, e assim $u^2 \in 4\mathbb{Z}$, ou seja, u também é par. Agora, se $\alpha = a + b\sqrt{d} \in \mathbb{A}_{\mathbb{K}}$, então $\alpha \in \mathbb{Z}[\sqrt{d}]$, e assim $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, se $\alpha \in \mathbb{Z}[\sqrt{d}]$, então existe um polinômio $m(x) = x^2 - 2ax + a^2 - db^2$, tal que α é raiz de $m(x)$. Pela Proposição 2.2.2 tem-se que $2a$ e $a^2 - db^2 \in \mathbb{Z}$, e assim $m(x) \in \mathbb{Z}[x]$. Logo $\alpha \in \mathbb{A}_{\mathbb{K}}$, ou seja, $\mathbb{Z}[\sqrt{d}] \subset \mathbb{A}_{\mathbb{K}}$. Portanto concluímos que $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

(b) Se $d \equiv 1 (mod\, 4)$, e como $u^2 - dv^2 \in 4\mathbb{Z}$, tem-se que u e v são ambos pares ou ímpares. Se u e v são pares, então $a, b \in \mathbb{Z}$, logo $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então

$$\alpha = a + b\sqrt{d} = \frac{u}{2} + \frac{v\sqrt{d}}{2} = \frac{(u-v)}{2} + v\frac{(1+\sqrt{d})}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Portanto $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Por outro lado, se $\alpha = a+b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, com $a, b \in \mathbb{Z}$, então $2a-b \in \mathbb{Z}$ e $\left(a+\frac{b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = a^2+ab+\frac{(1-d)b^2}{4} \in \mathbb{Z}$, pois $d \equiv 1(mod\,4)$. Logo $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathbb{A}_{\mathbb{K}}$, pois os coeficientes do polinômio minimal de α, $m(x) = x^2-(2a+b)x+a^2+ab+(1-d)b^2/4$ estão em $\mathbb{Z}$. Portanto $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{A}_{\mathbb{K}}$. □

Teorema 2.2.2 *([2], p.68) Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático, com d um inteiro livre de quadrados, então o discriminante absoluto $D_{\mathbb{K}}$ é*

(a) *d, se $d \equiv 1(mod\,4)$,*

(b) *$4d$, se $d \equiv 2$ ou $3(mod\,4)$.*

2.3 O grupo $\mathbb{Z}_n^*$

O objetivo desta seção é verificar quando o grupo multiplicativo $\mathbb{Z}_n^*$ é cíclico, pois será muito útil para determinar os anéis de inteiros algébricos dos subcorpos de $\mathbb{Q}(\zeta_p)$.

Teorema 2.3.1 (Teorema de Lagrange) *([4], p.134] Se G é um grupo finito e H um subgrupo de G, então a ordem de H divide a ordem de G. Em particular, se $\alpha \in G$, então a ordem de α divide a ordem de G.*

Proposição 2.3.1 *([4], p.135] Seja G um grupo abeliano. Se $a, b \in G$ são dois elementos de ordem finita tal que $mdc(o(a), o(b)) = 1$, então $o(ab) = o(a)o(b)$.*

Demonstração: Suponhamos que $o(a) = n$ e $o(b) = m$ e $o(ab) = k$. Como G é um grupo abeliano, segue que a e b comutam. Assim $(ab)^{nm} = (a^n)^m(b^m)^n = e^m e^n = e$, e deste modo, $k|mn$. Por outro lado, como $o(ab) = k$, ou seja, $(ab)^k = e$, segue que,

$$\begin{cases} e = (ab)^k = [(ab)^k]^n = (ab)^{kn} = (a^n b^n)^k = b^{nk} \\ e = (ab)^k = [(ab)^k]^m = (ab)^{km} = (a^m b^m)^k = a^{mk}. \end{cases}$$

Como $o(a) = n$ e $o(b) = m$, segue que $n|mk$ e $m|nk$. Também, como $mdc(n, m) = 1$, segue que $n|k$ e $m|k$, e assim $nm|k$. Portanto $mn = k$, ou seja, $o(ab) = o(a)o(b)$. □

Lema 2.3.1 *([4], p.135) Seja G um grupo abeliano. Se $a, b \in G$ são elementos de ordem finita, então existe um elemento $c \in G$ tal que $o(c) = mmc(o(a), o(b))$.*

Demonstração: Supondo que $o(a) = n$ e $o(b) = m$, tem-se dois casos a considerar:

(a) Se $mdc(n, m) = 1$, então pela Proposição 2.3.1, é suficiente tomar $c = ab$.

(b) Se $mdc(n, m) \neq 1$, então podemos considerar as decomposições de n e m em elementos irredutíveis da seguinte forma;

$$\begin{aligned} n &= p_1^{\alpha_1} \dots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \dots p_t^{\alpha_t} \\ m &= p_1^{\beta_1} \dots p_k^{\beta_k} p_{k+1}^{\beta_{k+1}} \dots p_t^{\beta_t} \end{aligned},$$

com $\alpha_i, \beta_i \in \mathbb{N}$, tais que $0 \leq \alpha_i \leq \beta_i$, para $i = 1, \dots, k$, e $0 \leq \beta_j \leq \alpha_j$, para $j = 1, \dots, t$, com os $p_i's$ todos primos distintos. Agora, considere os elementos $a_1 = a^{p_1^{\alpha_1} \dots p_k^{\alpha_k}}$ e $b_1 = b^{p_{k+1}^{\beta_{k+1}} \dots p_t^{\beta_t}}$, com isso obtemos, $o(a_1) = \dfrac{n}{p_1^{\alpha_1} \dots p_k^{\alpha_k}} = p_{k+1}^{\alpha_{k+1}} \dots p_t^{\alpha_t}$ e $o(b_1) = \dfrac{m}{p_{k+1}^{\beta_{k+1}} \dots p_t^{\beta_t}} = p_1^{\beta_1} \dots p_k^{\beta_k}$. Logo as ordens de a_1 e b_1 são relativamente primas, e pela Proposição 2.3.1, tem-se que $o(a_1b_1) = o(a_1)o(b_1)$. Portanto, tomando $c = a_1b_1$, o lema está provado. □

Proposição 2.3.2 *([5], p.101) Seja G um grupo abeliano. Se considerarmos $r = max\{o(g); g \in G\}$ com r finito, então $o(x)$ divide r para todo $x \in G$.*

Demonstração: Por hipótese, existe $a \in G$ tal que $o(a) = r$. Suponha que exista um elemento $b \in G$, tal que $o(b) \nmid r$. Pelo Lema 2.3.1, existe $c \in G$ tal que $o(c) = mmc(o(a), o(b)) = mmc(r, o(b))$. Assim, $o(c) > r$, o que é absurdo, pois $r = max\{o(g); g \in G\}$. Portanto, $o(x)|r$, para todo $x \in G$. □

Proposição 2.3.3 *([5], p.102) Se G é um subgrupo finito do grupo abeliano multiplicativo $\mathbb{K}^*$ de um corpo $\mathbb{K}$, então G é cíclico.*

Demonstração: Sejam $o(G) = n$ e $a \in G$ um elemento de ordem igual a r, onde $r = max\{o(g); g \in G\}$. Pelo Teorema 2.3.1 tem-se que $r|n$, e assim $r \leq n$.

Pela Proposição 2.3.2, tem-se que para todo $x \in G$, $o(x)|r$, ou seja, existe $q \in \mathbb{N}$, tal que $r = qo(x)$. Logo, $x^r = x^{o(x)q} = (x^{o(x)})^q = 1$, para todo $x \in G$. Se $f(x) = x^r - 1 \in \mathbb{K}[x]$, então $f(\alpha) = 0$ para todo $\alpha \in G$. Como $o(G) = n$, segue que o polinômio $f(x)$ tem no máximo n raízes distintas. Logo, $n \leq \partial f = r$, assim $n = r$. Portanto a é um gerador do grupo G, ou seja, G é um grupo cíclico. □

Corolário 2.3.1 *([5], p.102) Se $\mathbb{K}$ é um corpo finito, então o grupo abeliano multiplicativo $\mathbb{K}^*$ do corpo $\mathbb{K}$ é cíclico.*

Demonstração: É suficiente tomar $G = \mathbb{K}^*$ na Proposição 2.2.3. □

Lema 2.3.2 *([5], p.119) Se r e s são dois números inteiros positivos não nulos, com $mdc(r, s) = 1$, então*

$$\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s.$$

Demonstração: Sejam $\sigma_r : \mathbb{Z} \to \mathbb{Z}_r$ e $\sigma_s : \mathbb{Z} \to \mathbb{Z}_s$ os homomorfismos canônicos de $\mathbb{Z}$ em $\mathbb{Z}_r$, e de $\mathbb{Z}$ em $\mathbb{Z}_s$ respectivamente, onde $\sigma_r(a) = \{x; x \equiv a(mod\, r)\} = a + r\mathbb{Z}$ e $\sigma_s(a) = \{x; x \equiv a(mod\, s)\} = a + s\mathbb{Z}$, para todo $a \in \mathbb{Z}$. Considerando a aplicação

$$\begin{array}{rccc} \rho & : & \mathbb{Z} & \to & \mathbb{Z}_r \times \mathbb{Z}_s \\ & & a & \to & (\sigma_r(a), \sigma_s(a)), \end{array}$$

para todo $a \in \mathbb{Z}$, temos os seguintes fatos:

(a) ρ é um homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_r \times \mathbb{Z}_s$. De fato, dados $a, b \in \mathbb{Z}$ temos

$$\begin{aligned} \rho(a+b) &= (\sigma_r(a+b), \sigma_s(a+b)) = (\sigma_r(a) + \sigma_r(b), \sigma_s(a) + \sigma_s(b)) = \\ &= (\sigma_r(a), \sigma_s(a)) + (\sigma_r(b), \sigma_s(b)) = \rho(a) + \rho(b), \end{aligned}$$

e

$$\begin{aligned} \rho(ab) &= (\sigma_r(ab), \sigma_s(ab)) = (\sigma_r(a)\sigma_r(b), \sigma_s(a)\sigma_s(b)) = \\ &= (\sigma_r(a), \sigma_s(a)(\sigma_r(b)\sigma_s(b)) = \rho(a)\rho(b). \end{aligned}$$

(b) $Ker(\rho) = rs\mathbb{Z}$. De fato, lembre-se que

$$Ker(\rho) = \{a \in \mathbb{Z}; \rho(a) = (\overline{0}, \overline{0}) = (r\mathbb{Z}, s\mathbb{Z})\}.$$

Assim, se $a \in Ker(\rho)$, então $\rho(a) = (\overline{0}, \overline{0}) = (r\mathbb{Z}, s\mathbb{Z}) = (\sigma_r(a), \sigma_s(a))$. Deste modo, $a \equiv 0(mod\, r)$ e $a \equiv 0(mod\, s)$, ou seja, $r|a$ e $s|a$. Como $mdc(r, s) = 1$, segue que

$rs|a$. Logo $a \in rs\mathbb{Z}$, ou seja, $Ker(\rho) \subseteq rs\mathbb{Z}$. Por outro lado, se $a \in rs\mathbb{Z}$, então $a = rsn$, onde $n \in \mathbb{N}$. Assim $a \equiv 0(mod\, r)$ e $a \equiv 0(mod\, s)$, ou seja, $\sigma_r(a) = r\mathbb{Z}$ e $\sigma_s(a) = s\mathbb{Z}$. Logo, $\rho(a) = (\sigma_r(a), \sigma_s(a)) = (r\mathbb{Z}, s\mathbb{Z}) = (\overline{0}, \overline{0})$, ou seja, $x \in Ker(\rho)$. Portanto $rs\mathbb{Z} \subseteq Ker(\rho)$, e deste modo, temos a igualdade.

(c) ρ é sobrejetora. De fato, se $\alpha \in \mathbb{Z}_r \times \mathbb{Z}_s$, pelo fato das aplicações σ_r e σ_s serem sobrejetoras, segue que existem $a, b \in \mathbb{Z}$, tal que $\alpha = (\sigma_r(a), \sigma_s(b))$. Como a, b, r e $s \in \mathbb{Z}$ e $mdc(r, s) = 1$, pelo Teorema do Resto Chinês, segue que existe $x \in \mathbb{Z}$ tal que

$$\begin{cases} x & \equiv & a & (mod\, r) \\ x & \equiv & b & (mod\, s), \end{cases}$$

isto é,

$$\begin{cases} \sigma_r(x) & = & \sigma_r(a) \\ \sigma_s(x) & = & \sigma_s(b). \end{cases}$$

Logo $\rho(x) = (\sigma_r(x), \sigma_s(x)) = (\sigma_r(a), \sigma_s(b)) = \alpha$, e portanto ρ é sobrejetora. Como ρ é um homomorfismo sobrejetor e $Ker\rho = rs\mathbb{Z}$, segue pelo Teorema do Homomorfismos de Grupos que

$$\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s,$$

o que prova o lema. □

Lema 2.3.3 *([5], p.120) Se $n > 1$ é um número natural e se $n = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$ é a decomposição de n em fatores primos, então*

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{s_1}} \times \mathbb{Z}_{p_2^{s_2}} \times \ldots \times \mathbb{Z}_{p_t^{s_t}}.$$

Demonstração: Segue por indução, usando o Lema 2.3.2. □

Lema 2.3.4 *([4], p.162) Um elemento $\sigma_n(a)$ de $\mathbb{Z}_n$ admite simétrico multiplicativo se, e somente se, $mdc(a, n) = 1$.*

Demonstração: Se $\sigma_n(a)$ admite simétrico multiplicativo, então existe $b \in \mathbb{Z}$, tal que $\sigma_n(a)\sigma_n(b) = \sigma_n(ab) = \sigma_n(1)$. Logo $ab \equiv 1(mod\, n)$, ou seja, existe $q \in \mathbb{Z}$ tal que $nq = ab - 1$. Assim, $ab - nq = 1$, o que mostra que o $mdc(a, n) = 1$. Por outro lado, se $mdc(a, n) = 1$, então existem $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + ny_0 = 1$. Assim, $ax_0 - 1 = -ny_0$, ou seja, $n|ax_0 - 1$, e deste modo $ax_0 \equiv 1(mod\, n)$. Portanto, $\sigma_n(a)\sigma_n(x_0) = \sigma_n(ax_0) = \sigma_n(1)$, ou seja, $\sigma_n(a)$ admite simétrico multiplicativo. □

Proposição 2.3.4 *([5], p.120) Se r e s são dois números naturais maiores do que 1 tal que $mdc(r,s)=1$, então*

$$\mathbb{Z}_{rs}^* \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*.$$

Demonstração: Sejam $\sigma_r : \mathbb{Z} \to \mathbb{Z}_r$, $\sigma_s : \mathbb{Z} \to \mathbb{Z}_s$ e $\sigma_{rs} : \mathbb{Z} \to \mathbb{Z}_{rs}$ os homomorfismo canônicos de $\mathbb{Z}$ em $\mathbb{Z}_r$, de $\mathbb{Z}$ em $\mathbb{Z}_s$ e de $\mathbb{Z}$ em $\mathbb{Z}_{rs}$, respectivamente. Considere a aplicação

$$\begin{array}{rccc} \rho & : & \mathbb{Z}_{rs}^* & \to & \mathbb{Z}_r^* \times \mathbb{Z}_s^* \\ & & \sigma_{rs}(a) & \to & (\sigma_r(a), \sigma_s(a)). \end{array}$$

Observe que, se $d_1 = mdc(a,r)$ e $d_2 = mdc(a,s)$ então $d_1|r$ e $d_2|s$. Logo $d_1|rs$ e $d_2|rs$. Como $d_1|a$ e $d_2|a$ segue que d_1 e d_2 são divisores comuns de a e rs. Sendo $mdc(a,rs)=1$, tem-se que $d_1 = d_2 = 1$, e portanto $\sigma_r(a) \in \mathbb{Z}_r^*$ e $\sigma_s(a) \in \mathbb{Z}_s^*$. A aplicação ρ é um isomorfismo, uma vez que,

(a) ρ está bem definida e é injetora. De fato, se $a, b \in \mathbb{Z}$, então:

$\rho(\sigma_{rs}(a)) = \rho(\sigma_{rs}(b))$ se, e somente se, $(\sigma_r(a), \sigma_s(a)) = (\sigma_r(b), \sigma_s(b))$ se, e somente se, $\sigma_r(a) = \sigma_r(b)$ e $\sigma_s(a) = \sigma_s(b)$ se, e somente se, $a \equiv b (mod\, r)$ e $a \equiv b (mod\, s)$ se, e somente se, $r|a-b$ e $s|a-b$ se, e somente se, $rs|a-b$ se, e somente se, $a \equiv b (mod\, rs)$ se, e somente se, $\sigma_{rs}(a) = \sigma_{rs}(b)$.

(b) ρ é sobrejetora. De fato, se $(\overline{m}, \overline{n}) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$, então devemos mostrar que existe $\sigma_{rs}(z) \in \mathbb{Z}_{rs}^*$ tal que $\rho(\sigma_{rs}(z)) = (m,n)$ onde $z \in \mathbb{Z}$. Como $(\overline{m}, \overline{n}) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$, segue que $\overline{m} = a + r\mathbb{Z}$ e $\overline{n} = b + s\mathbb{Z}$, onde $mdc(a,r) = mdc(b,s) = 1$. Sabendo que $\mathbb{Z}_r^* \times \mathbb{Z}_s^* \subset \mathbb{Z}_r \times \mathbb{Z}_s$, pelo Lema 2.3.2, tem-se que existe $z \in \mathbb{Z}$, tal que $(a + r\mathbb{Z}, b + s\mathbb{Z}) = (z + r\mathbb{Z}, z + s\mathbb{Z})$, ou seja, $z \equiv a (mod\, r)$ e $z \equiv b (mod\, s)$. Agora, se $d = mdc(z,r)$, então $d|z$ e $d|r$. Como $z \equiv a (mod\, r)$, segue que $r|(a-z)$, e assim $d|(a-z)$. Como $d|z$, segue que $d|a$. Logo $d|a$ e $d|r$, e como $mdc(a,r) = 1$, concluímos que $d = 1$. De modo análogo, obtemos que $mdc(z,s) = 1$. Também $mdc(z,rs) = 1$, uma vez que se existir um primo p tal que $p \mid z$ e $p \mid rs$, então $p \mid r$ ou $p \mid s$. Assim, $p \mid z$ e $p \mid r$ ou $p \mid z$ e $p \mid s$. Mas isso, contradiz o fato de $mdc(z,r) = mdc(z,s) = 1$. Portanto $mdc(z,rs) = 1$, e desse modo, $\sigma_{rs}(z) \in \mathbb{Z}_{rs}^*$. Assim, concluímos que se $(\overline{m}, \overline{n}) = (\sigma_r(a), \sigma_s(b)) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$ então existe $\sigma_{rs}(z) \in \mathbb{Z}_{rs}^*$ tal que $\rho(\sigma_{rs}(z)) = (\sigma_r(z), \sigma_s(z)) = (\sigma_r(a), \sigma_s(b)) = (\overline{m}, \overline{n})$.

(c) ρ é homomorfismo. De fato, se $\sigma_{rs}(a), \sigma_{rs}(b) \in \mathbb{Z}_{rs}^*$, então

$$\rho(\sigma_{rs}(a) + \sigma_{rs}(b)) = \rho(\sigma_{rs}(a+b)) = (\sigma_r(a+b), \sigma_s(a+b)) =$$
$$= (\sigma_r(a) + \sigma_r(b), \sigma_s(a) + \sigma_s(b)) = (\sigma_r(a), \sigma_s(a)) + (\sigma_r(b), \sigma_s(b)) =$$
$$= \rho(\sigma_{rs}(a)) + \rho(\sigma_{rs}(b)).$$
$$\rho(\sigma_{rs}(a)\sigma_{rs}(b)) = \rho(\sigma_{rs}(ab)) = (\sigma_r(ab), \sigma_s(ab)) = (\sigma_r(a)\sigma_r(b), \sigma_s(a)\sigma_s(b)) =$$
$$= (\sigma_r(a), \sigma_s(a))(\sigma_r(b)\sigma_s(b)) = \rho(\sigma_{rs}(a))\rho(\sigma_{rs}(b)).$$

Portanto por **(a)**, **(b)** e **(c)** concluímos que $\mathbb{Z}_{rs}^* \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*$. □

Proposição 2.3.5 *([5], p.120) Seja $n > 1$ um número natural. Se $n = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$ é a decomposição de n em fatores primos, então*

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{s_1}}^* \times \mathbb{Z}_{p_2^{s_2}}^* \times \dots \times \mathbb{Z}_{p_t^{s_t}}^*.$$

Demonstração: Segue, por indução, usando a Proposição 2.3.4. □

Definição 2.3.1 *Seja n um inteiro positivo. A função Φ de Euler do número n, denotada por $\Phi(n)$, é definida como sendo o número de inteiros positivos menores do que n ou iguais a n que são relativamente primos com n, ou seja,*

$$\Phi(n) = \#\{a \in \mathbb{N}; 1 \leq a \leq n, mdc(a, n) = 1\}.$$

Proposição 2.3.6 *([5], p.120) O número de elementos do grupo multiplicativo $\mathbb{Z}_n^*$ é igual $\Phi(n)$.*

Demonstração: Pelo Lema 2.3.4, os elementos de $\mathbb{Z}_n^*$ são da forma $\sigma_n(a)$, com $mdc(a, n) = 1$. Como consideramos apenas os $\sigma_n(a)$ com $mdc(a, n) = 1$, segue que o número de elementos de $\mathbb{Z}_n^*$ é igual a $\Phi(n)$. □

Proposição 2.3.7 *([5], p.120) Se r e s são dois números naturais não nulos com $mdc(r, s) = 1$, então $\Phi(rs) = \Phi(r)\Phi(s)$.*

Demonstração: Pela Proposição 2.3.4, vimos que $\mathbb{Z}_{rs}^* \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*$, e deste modo $o(\mathbb{Z}_{rs}^*) = o(\mathbb{Z}_r^*)o(\mathbb{Z}_s^*)$. Pela Proposição 2.3.6, tem-se que $o(\mathbb{Z}_n^*) = \Phi(n)$, e portanto $\Phi(rs) = \Phi(r)\Phi(s)$. □

Lema 2.3.5 *([5], p.121) Seja n um número natural maior que 1. Se $n = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$ é a decomposição de n em fatores primos positivos, então $\Phi(n) = \Phi(p_1^{s_1}) \dots \Phi(p_t^{s_t})$.*

Demonstração: Segue, por indução sobre n, aplicando a Proposição 2.3.4. □

Proposição 2.3.8 *([5], p.124) Os grupos $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$ são cíclicos.*

Demonstração: Como $\mathbb{Z}_2^* = \{\overline{1}\}$, segue que $\overline{1}$ é um gerador para $\mathbb{Z}_2^*$, e portanto, $\mathbb{Z}_2^*$ é cíclico. Agora, como $\mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}$, onde $\overline{3}$ é um gerador de $\mathbb{Z}_4^*$, segue que $\mathbb{Z}_4^*$ é cíclico. □

Lema 2.3.6 *([5], p.124) Para todo inteiro ímpar b e para todo natural t, vale a congruência*

$$b^{2^{t+1}} \equiv 1 (mod\, 2^{t+3}).$$

Demonstração: Se b é um inteiro ímpar, então existe $k \in \mathbb{Z}$, de modo que $b = 2k + 1$. A prova será feita por indução sobre t. De fato, para $t = 0$, tem-se que $b^2 = (2k+1)^2 = 4k^2 + 4 + 1 = 4k(k+1) + 1$, e assim $b^2 \equiv 1 (mod\, 2^3)$. Por hipótese de indução, suponhamos o resultado válido para t, ou seja, $b^{2^{t+1}} \equiv 1 (mod\, 2^{t+3})$. Assim existe $\alpha \in \mathbb{Z}$ tal que $b^{2^{t+1}} = 1 + \alpha 2^{t+3}$. Agora,

$$b^{2^{t+2}} = b^{2^{(t+1)}2} = (b^{2^{t+1}})^2 = (1 + \alpha 2^{t+3})^2 =$$

$$= 1 + \alpha 2^{t+4} + \alpha^2 2^{2t+6} = 1 + 2^{t+4}(\alpha + \alpha^2 2^{t+4}).$$

Tomando $(\alpha + \alpha^2 2^{t+2}) = \beta \in \mathbb{Z}$, obtemos $b^{2^{t+2}} \equiv 1 (mod\, 2^{t+4})$, assim o lema está provado. □

Lema 2.3.7 *([5], p.124) O grupo $\mathbb{Z}_{2^r}^*$ não é cíclico para $r \geq 3$.*

Demonstração: Pela Proposição 2.3.6 tem-se que $o(\mathbb{Z}_{2^r}^*) = \Phi(2^r) = 2^{r-1}$. Agora, mostraremos que a ordem de qualquer elemento de $\mathbb{Z}_{2^r}^*$ é no máximo 2^{r-2}. Se $\sigma_{2^r} : \mathbb{Z} \to \mathbb{Z}_{2^r}$ é o homomorfismo canônico e x um elemento de $\mathbb{Z}_{2^r}^*$, então existe $b \in \mathbb{Z}$ tal que $\sigma_{2^r}(b) = x$ se, e somente se, b é ímpar. Como r é um número natural maior ou igual a 3, e b é um inteiro ímpar, tomando $t = r - 3$, segue pelo Lema 2.3.6, que $b^{2^{t+1}} \equiv 1 (mod\, 2^{t+3})$, ou seja, $b^{2^{r-2}} \equiv 1 (mod\, 2^r)$. Logo $x^{2^{r-2}} = \sigma_{2^r}(1)$, e assim a ordem de x é no máximo 2^{r-2}. Portanto o grupo $\mathbb{Z}_{2^r}^*$ não é cíclico. □

Lema 2.3.8 *([5], p.121) Sejam $\sigma_p : \mathbb{Z} \to \mathbb{Z}_p$ e $\sigma_{p^r} : \mathbb{Z} \to \mathbb{Z}_{p^r}$ homomorfismos canônicos, onde a, b, p e r são inteiros positivos com p primo e $a = b^{p^{r-1}}$. Se a imagem de b pelo homomorfismo canônico de $\mathbb{Z}$ em $\mathbb{Z}_p$ possui ordem $p-1$ em $\mathbb{Z}_p$, isto é, $o(\sigma_p(b)) = p-1$, então a imagem de a pelo homomorfismo canônico de $\mathbb{Z}$ em $\mathbb{Z}_{p^r}$ possui ordem $p-1$ em $\mathbb{Z}_{p^r}$, ou seja, $o(\sigma_{p^r}(a)) = p-1$.*

Demonstração: Como $\mathbb{Z}_p$ é corpo, segue pelo Corolário 2.3.1, que $\mathbb{Z}_p^*$ é cíclico. Pela Proposição 2.3.6, tem-se $o(\mathbb{Z}_p^*) = \Phi(p) = p-1$. Logo, existe $b \in \mathbb{Z}$ tal que $o(\sigma_p(b)) = p-1$ e p não divide b. Agora, se $a = b^{p^{r-1}}$ e $d = mdc(a, p^r)$, então $d|p^r$ e $d|a = b^{p^{r-1}}$. Se $d|p^r$, então $d = 1, p, p^2, \ldots, p^r$, pois p é primo. Se $d \neq 1$, então $d = p^i$, para algum $i = 1, \ldots, r$. Como $p \nmid b$ segue que $p^i \nmid b$. Seja $b = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$, com $q_j \neq p$, para todo $j = 1, \ldots, s$. Assim $a = b^{p^{r-1}} = q_1^{\alpha_1 p^{r-1}} q_2^{\alpha_2 p^{r-1}} \ldots q_s^{\alpha_s p^{r-1}}$. Logo $p^i \nmid a$, para $i = 1, \ldots, r$, o que é absurdo, pois $d \neq 1$. Portanto $d = 1$, ou seja, $mdc(a, p^r) = 1$, e desse modo $\sigma_{p^r}(a) = x \in \mathbb{Z}_{p^r}^*$. Consequentemente, $x^{p-1} = (\sigma_{p^r}(a))^{p-1} = (b^{p^{r-1}})^{p-1} = b^{p^{r-1}(p-1)} = 1$, pois $o(\mathbb{Z}_{p^r}^*) = \Phi(p^r) = p^r - p^{r-1}$. Como $p^i \nmid b$, para todo $i = 1, \ldots, r$, segue que o $mdc(b, p^r) = 1$, e portanto $b \in \mathbb{Z}_{p^r}^*$, ou seja, $o(x) = p-1$. □

Lema 2.3.9 *([5], p.122) Se $p > 2$ é um número primo, então para todo número natural n, vale*

$$(1+p)^{p^n} \equiv 1 + p^{n+1} (mod\, p^{n+2}).$$

Demonstração: Faremos a prova por indução sobre n. De fato, para $n = 0$, tem-se $(1+p)^1 = 1+p$, e assim $(1+p)^1 \equiv 1 + p\,(mod\, p^2)$. Por hipótese de indução, suponhamos que o resultado seja válido para $n = k$, ou seja, que

$$(1+p)^{p^k} \equiv 1 + p^{k+1} (mod\, p^{k+2}).$$

Assim, existe um elemento $\alpha \in \mathbb{Z}$ tal que

$$(1+p)^{p^k} = 1 + p^{k+1} + \alpha p^{k+2} = 1 + p^{k+1}(1 + \alpha p).$$

Agora,

$$(1+p)^{p^{k+1}} = (1+p)^{pp^k} = ((1+p)^{p^k})^p = ((1 + p^{k+1}(1+\alpha p)))^p =$$

$$= 1+\begin{pmatrix} p \\ 1 \end{pmatrix} p^{k+1}(1+\alpha p)+\begin{pmatrix} p \\ 2 \end{pmatrix} p^{2(k+1)}(1+\alpha p)^2+\ldots+p^{p(k+1)}(1+\alpha p)^p =$$

$$= 1 + p^{k+2} + \alpha p^{k+3} + \tfrac{1}{2}(p-1)p^{2k+3}(1+\alpha p)^2 + \ldots + p^{p(k+1)}(1+\alpha p)^p =$$

$$= 1 + p^{k+2} + \beta p^{k+3},$$

com $\beta \in \mathbb{Z}$. Portanto, $(1+p)^{p^{k+1}} \equiv 1 + p^{k+2}(mod\, p^{k+3})$, o que prova o lema. □

Lema 2.3.10 *([5], p.123) Se $p > 2$ é um número primo, r um inteiro positivo maior do que 1 e $\sigma_{p^r} : \mathbb{Z} \to \mathbb{Z}_{p^r}$ o homomorfismo canônico, então o elemento $\beta = \sigma_{p^r}(1+p)$ tem ordem p^{r-1} em $\mathbb{Z}^*_{p^r}$.*

Demonstração: Pelo Lema 2.3.9, tomando $n = r-1$ tem-se que

$$(1+p)^{p^{r-1}} \equiv 1 + p^r(mod\, p^{r+1}).$$

Assim, existe $\alpha \in \mathbb{Z}$ tal que

$$(1+p)^{p^{r-1}} = 1 + p^r + \alpha p^{r+1} = 1 + p^r(1+\alpha p) = 1 + \beta p^r,$$

onde $\beta = (1+\alpha p) \in \mathbb{Z}$. Logo $(1+p)^{p^{r-1}} \equiv 1(mod\, p^r)$, o que mostra que $\beta^{p^{r-1}} = \sigma_{p^r}(1)$. Desse modo $o(\beta)|p^{r-1}$. Como p é primo, segue que $o(\beta) = p^j$, com $0 \leq j \leq r-1$. Se $j < r-1$, então $(\sigma_{p^r}(1+p))^{p^j} = \sigma_{p^r}(1)$, ou seja, $(1+p)^{p^j} \equiv 1(mod\, p^r)$. Novamente pelo Lema 2.3.9, tem-se que $(1+p)^{p^j} \equiv 1 + p^{j+1}(mod\, p^{j+2})$. Assim, existem $u, v \in \mathbb{Z}$ tais que $(1+p)^{p^j} = 1 + up^r$ e $(1+p)^{p^j} = 1 + p^{j+1} + vp^r$. Logo, $up^r = p^{j+1} + vp^{j+2}$ e $p^{j+1} = up^r - vp^{j+2} = up^{j+2}p^k - vp^{j+2} = p^{j+2}(up^k - v)$, pois $j+2 \leq r$. Assim, $p^{j+1} \equiv 0(mod p^{j+2})$, o que é um absurdo. Portanto, $j = r-1$, o que prova o lema. □

Proposição 2.3.9 *([5], p.121) Se $p > 2$ é um número primo e r um inteiro positivo, então o grupo $\mathbb{Z}^*_{p^r}$ é cíclico.*

Demonstração: Sejam $\sigma_p : \mathbb{Z} \to \mathbb{Z}_p$ e $\sigma_{p^r} : \mathbb{Z} \to \mathbb{Z}_{p^r}$ os homomorfismos canônicos. Como $\mathbb{Z}^*_p$ é cíclico, segue que existe $b \in \mathbb{Z}$ tal que $o(\sigma_p(b)) = p-1$. Pelo Lema 2.3.8 existe $a = b^{p^{r-1}}$, tal que $o(\sigma_{p^r}(a)) = p-1$ em $\mathbb{Z}_{p^r}$. Se $\beta = \sigma_{p^r}(1+p)$, então pelo

Lema 2.3.10, tem-se que $o(\beta) = p^{r-1}$ em $\mathbb{Z}_{p^r}$. Tomando $\alpha = \sigma_{p^r}(a)$ e $\beta = \sigma_{p^r}(1+p^r)$, e como $mdc(o(\alpha), o(\beta)) = mdc(p-1, p^{r-1}) = 1$, segue pela Proposição 2.3.1, que $o(\alpha\beta) = o(\alpha)o(\beta) = (p-1)p^{r-1} = o(\mathbb{Z}^*_{p^r})$. Portanto, $\alpha\beta$ é um gerador do grupo $\mathbb{Z}^*_{p^r}$, ou seja, o grupo $\mathbb{Z}^*_{p^r}$ é cíclico. □

Proposição 2.3.10 *([5], p.127) Se $p > 2$ é um número primo, então o grupo $\mathbb{Z}^*_{2p^r}$ é cíclico.*

Demonstração: Como $p > 2$ é um número primo, segue que $mdc(2, p^r) = 1$. Logo, pela Proposição 2.3.4, tem-se $\mathbb{Z}^*_{2p^r} \simeq \mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^r}$. Como $\mathbb{Z}^*_2 = \{\overline{1}\}$, segue que $\mathbb{Z}^*_{2p^r} \simeq \mathbb{Z}^*_{p^r}$. Agora, pela Proposição 2.3.9, segue que $\mathbb{Z}^*_{p^r}$ é cíclico, e portanto concluímos que $\mathbb{Z}^*_{2p^r}$ é cíclico. □

Lema 2.3.11 *([5], p.128) Se $G_1, G_2, \ldots, G_s$ são grupos finitos, então o grupo produto $G_1 \times G_2 \times \ldots \times G_s$ é cíclico se, e somente se, cada G_i é cíclico e as ordens de G_i e G_j são primos entre si, para $i, j = 1, 2, \ldots, n$, com $i \neq j$.*

Proposição 2.3.11 *([5], p.127) Se o grupo $\mathbb{Z}^*_n$, com n inteiro maior do que 1, é cíclico, então $n = 2, 4, p^r$ ou $2p^r$, onde $p > 2$ é um número primo e $r \geq 1$ é um número natural.*

Demonstração: Pela Proposição 2.3.10 tem-se que, se n é uma potência de 2 diferente de 2 e de 4, então o grupo $\mathbb{Z}^*_n$ não é cíclico. Agora, se n é um número par e não uma potência de 2, então n tem uma decomposição em fatores primos do tipo $n = 2^a p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, onde $a \geq 1$, $s \geq 1$, $\alpha_i > 0$ e p_i são primos distintos, com $p_i \neq 2$, para todo $i = 1, \ldots, s$. Pela Proposição 2.3.5, tem-se que $\mathbb{Z}^*_n \simeq \mathbb{Z}^*_{2^a} \times \mathbb{Z}^*_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}^*_{p_s^{\alpha_s}}$. Como, por hipótese, $\mathbb{Z}^*_n$ é cíclico, segue pelo Lema 2.3.11, que $\mathbb{Z}^*_{2^a}, \mathbb{Z}^*_{p_1^{\alpha_1}}, \ldots, \mathbb{Z}^*_{p_s^{\alpha_s}}$ são cíclicos. Desse modo, pelo Lema 2.3.7, concluímos que $a = 1$ ou $a = 2$. Se $a = 2$, então para $i, j = 1, 2, \ldots, s$, tem-se que $mdc(4, p_i^{\alpha_i} - p_i^{\alpha_i - 1}) \geq 2$, o que é um absurdo. Assim $a = 1$. Além disso, $s = 1$, uma vez que se $s > 1$, então, para $i, j = 1, 2, \ldots, s$ com $i \neq j$, tem-se que $mdc(p_i^{\alpha_i} - p_i^{\alpha_i - 1}, p_j^{\alpha_j} - p_j^{\alpha_j - 1}) \neq 1$, pois para $i, j = 1, 2, \ldots, s$, tem-se que, $p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ e $p_j^{\alpha_j} - p_j^{\alpha_j - 1}$ são números pares. Portanto $a = 1$ e $s = 1$, ou

seja, $n = 2p_1^{r_1}$. Finalmente, se n é um número ímpar, então n tem uma decomposição em fatores primos do tipo $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, onde $r_i \geq 1$, $s \geq 1$, $\beta_i \geq 0$, $p_i \neq 2$ e $p_i \neq p_j$ se $i \neq j$, para $i, j = 1, 2, \dots, n$. Agora, se $s > 1$, pela Proposição 2.3.5, tem-se que $\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{\beta_1}}^* \times \dots \times \mathbb{Z}_{p_s^{\beta_s}}^*$. Como, por hipótese, $\mathbb{Z}_n^*$ é cíclico, segue pelo Lema 2.3.11 que os $\mathbb{Z}_{p_i^{\beta_i}}^*$ são cíclicos, para $i = 1, \dots, s$, o que é um absurdo, pois $mdc(p_i^{\beta_i} - p_i^{\beta_i - 1}, p_j^{\beta_j} - p_j^{\beta_j - 1}) \neq 1$, para qualquer $i \neq j$, onde $i, j = 1, 2, \dots, s$. Logo $s = 1$, ou seja, $n = p_1^{\beta_1}$. □

Teorema 2.3.2 *([5], p.127) O grupo $\mathbb{Z}_n^*$ é cíclico se, e somente se, $n = 2, 4, p^r$ ou $2p^r$, onde $p > 2$ é um número primo e $r \geq 1$ é um número natural.*

Demonstração: Se $\mathbb{Z}_n^*$ é cíclico, segue pela Proposição 2.3.11, que $n = 2, 4, p^r$ ou $2p^r$, onde $p > 2$ é um número primo e $r \geq 1$ é um número natural. Reciprocamente, se $n = 2$ ou $n = 4$ então, pela Proposição 2.3.8, segue que o grupo $\mathbb{Z}_n^*$ é cíclico. Se $n = p^r$ com $p > 2$ um número primo e $r \geq 1$ um número natural, então pela Proposição 2.3.9, segue que $\mathbb{Z}_n^*$ é cíclico. Finalmente, se $n = 2p^r$, com $p > 2$ um número primo e $r \geq 1$ um número natural, segue pela Proposição 2.3.10, que $\mathbb{Z}_n^*$ é cíclico. □

2.4 Corpos Ciclotômicos

Nesta seção, apresentamos os conceitos de polinômio ciclotômico e da extensão ciclotômica, mostrando algumas propriedades, que serão muito úteis nos próximos capítulos. Mas antes faremos um breve estudo sobre o grupo multiplicativo U_n.

Definição 2.4.1 *Sejam ζ um elemento de $\mathbb{C}$ e n um inteiro positivo. Se $\zeta^n = 1$, dizemos que ζ é uma* ***raiz n-ésima da unidade****. Agora, se $\zeta^n = 1$ e $\zeta^m \neq 1$, para todo $1 \leq m < n$, dizemos que ζ é uma* ***raiz n-ésima primitiva da unidade****.*

Lema 2.4.1 *Seja $\zeta_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade e $k \in \mathbb{N}$. Assim, ζ_n^k é uma raiz n-ésima primitiva da unidade se, e somente se, $mdc(n, k) = 1$.*

Demonstração: Suponha que ζ_n^k é uma raiz n-ésima primitiva da unidade, e o $mdc(k,n) = d \neq 1$ e $d \neq n$. Agora, note que $n = dx$, com $x \in \mathbb{N}$, assim $(\zeta_n^k)^d = \zeta_n^{kd} = \zeta_n^{k\frac{n}{x}} = (\zeta_n^n)^{\frac{k}{x}} = 1^{\frac{k}{x}} = 1$, o que é um absurdo, pois $d < n$ e ζ_n^k é uma raiz n-ésima primitiva da unidade. Por outro lado, seja $m \in \mathbb{N}$, tal que $(\zeta_n^k)^m = 1$, ou seja, $\zeta_n^{km} = 1$, como ζ_n é uma n-ésima primitiva da unidade, tem-se que $n|km$, como por hipótese $mdc(n,k) = 1$, segue que $n|m$, logo ζ_n^k é uma raiz n-ésima primitiva da unidade. □

Seja $U_n = \{\zeta_n^{r_1}, \ldots, \zeta_n^{r_n}\} \subseteq \mathbb{C}$ o conjunto de todas as raízes distintas do polinômio $x^n - 1$. Como $(\zeta_n^i \zeta_n^j)^n = (\zeta_n^i)^n (\zeta_n^j)^n = (\zeta_n^n)^i (\zeta_n^n)^j = 1$ e $\left(\frac{\zeta_n^i}{\zeta_n^j}\right)^n = \frac{(\zeta_n^n)^i}{(\zeta_n^n)^j} = 1$, segue que U_n é um grupo multiplicativo finito. Assim, pelo Lema 2.3.1, tem-se que U_n é cíclico. Desse modo, podemos representar as raízes n-ésimas primitivas da unidade por $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$, onde ζ_n é um gerador do grupo U_n. Pelo Lema 2.4.1, tem-se que as raízes n-ésimas primitivas da unidade são os geradores do grupo U_n, ou seja, os elementos $\zeta_n^k \in \mathbb{C}$, com $mdc(k,n) = 1$, para $k = 1, \ldots, n$, geram U_n.

Lema 2.4.2 *([6], p.277) Se $m, n \in \mathbb{Z}$, e $mdc(m,n) = 1$, então*

$$U_{mn} \simeq U_m \times U_n.$$

Demonstração: Seja a aplicação,

$$\begin{array}{rccc} \psi & : & U_m \times U_n & \rightarrow & U_{mn} \\ & & (a,b) & \rightarrow & ab. \end{array}$$

A aplicação ψ está bem definida, pois $(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$. Também ψ é um homomorfismo, pois para todo $(a,b),(c,d) \in U_m \times U_n$, tem-se que $\psi((a,b)(c,d)) = \psi(ac,bd) = (acbd) = (abcd) = \psi(ab)\psi(cd)$. Além disso, ψ é injetora, uma vez que $Ker(\psi) = \{(a,b) \in U_m \times U_n \,;\, \psi(a,b) = 1\} = \{1,1\}$. De fato, se $(a,b) \in U_m \times U_n$ é tal que $\psi(a,b) = 1$, então $a = \zeta_m^k$ e ζ_n^l, para algum $k = 0,1,2,\ldots,m-1$, e para algum $l = 0,1,2,\ldots,n-1$. Assim, $\psi(a,b) = ab = 1$ se, e somente se, $\zeta_m^k \zeta_n^l = 1$ se, e somente se, $\zeta_m^k = \zeta_n^{-l}$ se, e somente se, $\zeta_m^{nk} = \zeta_n^{-nl}$ se, e somente se, $\zeta_m^{nk} = 1$. Como ζ_m é uma raiz m-ésima primitiva da unidade, segue

que $m|nk$ e como $mdc(m,n)=1$, tem-se que $m|k$, ou seja, $k=mx$, onde $x\in\mathbb{Z}$. De modo análogo, $n|l$, ou seja, $l=ny$, onde $y\in\mathbb{Z}$. Como $k<n$ e $l<n$ segue que $k=l=0$. Portanto $ab=1$ se, e somente se, $a=b=1$. Logo ψ é injetora. Finalmente, como $mdc(m,n)=1$, segue que $o(U_{mn})=o(U_m)o(U_n)$, e como ψ é injetora, segue que ψ é sobrejetora. Portanto, ψ é um isomorfismo, ou seja,

$$U_{mn}\simeq U_m\times U_n,$$

o que prova o lema. □

Proposição 2.4.1 *([6], p.277] Sejam $m,n\in\mathbb{N}$ e ζ_m, $\zeta_n\in\mathbb{C}$ raízes m-ésimas e n-ésimas da unidade, respectivamente. Se $mdc(m,n)=1$, então $\zeta_m^k\zeta_n^l$ é uma raiz mn-ésima primitiva da unidade, onde $0\leq k\leq m-1$ e $0\leq l\leq n-1$, se, e somente se, ζ_m^k é uma raiz m-ésima primitiva da unidade e ζ_n^l é uma raiz n-ésima primitiva da unidade.*

Demonstração: Se $\zeta_m^k\in\mathbb{C}$ não é uma raiz m-ésima primitiva da unidade, então pelo Lema 2.4.1, tem-se que $mdc(m,k)=d>1$. Assim,

$$(\zeta_m^k\zeta_n^l)^{\frac{mn}{d}}=(\zeta_m^{k\frac{mn}{d}})(\zeta_n^{l\frac{mn}{d}})=(\zeta_m^m)^{\frac{kn}{d}}(\zeta_n^n)^{\frac{lm}{d}}=(1)^{\frac{kn}{d}}(1)^{\frac{lm}{d}}=1,$$

o que é um absurdo pois $\frac{mn}{d}<mn$ e por hipótese, $\zeta_m^k\zeta_n^l$ é uma raiz mn-ésima primitiva da unidade. Portanto ζ_m^k é uma raiz m-ésima primitiva da unidade. De modo análogo, ζ_n^l é uma raiz n-ésima primitiva da unidade. Reciprocamente, se ζ_m^k e ζ_n^l são raízes m-ésimas e n-ésimas primitivas da unidade, respectivamente, então segue pelo Lema 2.4.1, que $mdc(k,m)=mdc(l,n)=1$. Assim, tem-se que $(\zeta_m^k\zeta_n^l)^a=1$ se, e somente se, $\zeta_m^{ka}\zeta_n^{la}=1$ se, e somente se, $\zeta_m^{ka}=\zeta_n^{-la}$ se, e somente se, $\zeta_m^{kan}=\zeta_n^{-lan}$ se, e somente se, $(\zeta_m^k)^{an}=1$ se, e somente se, $m|an$. Como $mdc(m,n)=1$, segue que $m|a$. De modo análogo, $n|a$. Assim, usando novamente o fato do $mdc(m,n)=1$, obtemos que $mn|a$. Agora, como $(\zeta_m^k\zeta_n^l)^{mn}=(\zeta_m^m)^{kn}(\zeta_n^n)^{lm}=1$, concluímos que mn é a menor potência tal que $(\zeta_m^k\zeta_n^l)^{mn}=1$. Portanto, $\zeta_m^k\zeta_n^l$ é uma raiz mn-ésima primitiva da unidade. □

Definição 2.4.2 *Sejam $n \in \mathbb{N}$ e $\zeta_n \in \mathbb{C}$ uma raiz n-ésima da unidade. O polinômio* $\phi_n(x) = \prod_{j=1\,,mdc(j,n)=1}^{n} (x - \zeta_n^j)$ *é chamado de* ***n-ésimo polinômio ciclotômico****.*

Proposição 2.4.2 *([6], pg 279) Se n é um inteiro positivo, então* $x^n - 1 = \prod_{d|n} \phi_d(x)$.

Demonstração: Sejam $f(x) = x^n - 1$ e $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} \subseteq \mathbb{C}$ as raízes de $f(x)$. Assim, $x^n - 1 = (x-1)(x-\zeta_n)\ldots(x-\zeta_n^{n-1})$. Analisando às ordens de cada raiz de $f(x)$ e escrevendo todas as raízes de mesma ordem como um polinômio da forma $\phi_d(x) = \prod_{d=\, o(\zeta_n)} (x - \zeta_n)$, obtemos que $x^n - 1 = \prod_{d|n} \phi_d(x)$. □

Observação 2.4.1 *Pela Proposição 2.4.2, segue que para todo inteiro positivo n podemos escrever* $\phi_n(x) = \dfrac{x^n - 1}{\prod_{d|n\,,d<n} \phi_d(x)}$.

Exemplo 2.4.1 *Sejam p um primo e* $f(x) = x^p - 1$. *Assim,*

$$x^p - 1 = \prod_{d|p} \phi_d(x) = \phi_1(x)\phi_p(x),$$

e deste modo,

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Em particular, se $n = p^r$, *com p primo e r um inteiro maior que* 1, *tem-se que*

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{\phi_1(x)\phi_2(x)\ldots\phi_{p^{r-1}}(x)} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + \ldots + x^{p^{r-1}} + 1.$$

Definição 2.4.3 *Seja $\zeta_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade, onde $n \in \mathbb{N}$. Dizemos que um corpo $\mathbb{K}$ é um* ***corpo ciclotômico****, se $\mathbb{K}$ for uma extensão de $\mathbb{Q}$ gerada por ζ_n, isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$.*

Teorema 2.4.1 *([6], p.278) Se $\zeta_n \in \mathbb{C}$ é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \Phi(n)$, onde Φ é a função de Euler.*

Demonstração: Seja $f(x)$ o polinômio minimal de ζ_n sobre $\mathbb{Q}$, dessa forma, tem-se que $x^n - 1 = f(x)g(x)$, com $g(x) \in \mathbb{Q}[x]$. Pelo, Lema de Gauss, segue que $f(x), g(x) \in \mathbb{Z}[x]$. Se p é um primo, tal que $p \nmid n$, então, segue pelo Lema 2.4.1, que ζ_n^p é uma raiz n-ésima primitiva da unidade. Como $x^n - 1 = f(x)g(x)$, segue que $(\zeta_n^p)^n - 1 = f(\zeta_n^p)g(\zeta_n^p)$, ou seja, $f(\zeta_n^p)g(\zeta_n^p) = 0$. Assim, se ζ_n^p não for raiz de $f(x)$, então ζ_n^p é raiz de $g(x)$ e ζ_n é raiz de $g(x^p)$. Como $f(x)$ é o polinômio minimal de ζ_n segue que $f(x)|g(x^p)$. Assim, pelo Lema de Gauss, tem-se $g(x^p) = f(x)h(x)$, com $h(x) \in \mathbb{Z}[x]$. Pelo Teorema de Fermat, tem-se que $a^p \equiv a(mod\, p)$, e deste modo $g(x^p) \equiv g(x)^p(mod\, p)$. Assim, $f(x)h(x) \equiv g(x)^p(mod\, p)$, ou seja, $g(x)^p \equiv f(x)h(x)(mod\, p)$. Como ζ_n é raiz de $f(x)$, segue que $\overline{g(\zeta_n)^p} = \overline{0}$, e deste modo $\overline{g}(\zeta_n) = 0$. Logo, $\overline{f}$ e $\overline{g}$ tem uma raiz em comum. Como, $x^n - \overline{1} = \overline{f}(x)\overline{g}(x)$, segue que $x^n - \overline{1}$ tem raízes múltiplas. Logo $nx^{n-1} = \overline{0}$, e deste modo, para qualquer $\alpha \in \mathbb{Z}_p$, obtemos que $n\alpha^{n-1} = \overline{0}$. Como a característica de $\mathbb{Z}_p$ é p, segue que $p|n$, o que é um absurdo, pois supomos que $p \nmid n$. Portanto, ζ_n^p é raiz de $f(x)$, para todo $p \nmid n$, onde $mdc(p, n) = 1$. Desse modo, $\partial(f(x)) \geq \partial(\phi(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$. Finalmente, como $f(x)|\phi_n(x)$, segue que $\partial(\phi_n(x)) \geq \partial(f(x))$, e portanto $\partial(f(x)) = \partial(\phi_n(x)) = \Phi(n)$. □

Corolário 2.4.1 *([7], p.44) Se ζ_n é uma raiz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \dfrac{\Phi(n)}{2}$.

Demonstração: Tem-se que $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal de $\mathbb{Q}(\zeta_n)$, onde $\mathbb{Q} \subset \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subset \mathbb{Q}(\zeta_n)$. Assim, pelo Teorema 1.4.4, segue que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})][\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}]$. Pelo Teorema 2.4.1, tem-se que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \Phi(n)$, e como o polinômio $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ tem ζ_n como raiz e é irredutível sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, segue que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Portanto $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \dfrac{\Phi(n)}{2}$. □

Corolário 2.4.2 *([6], p.278) Se m, n são números inteiros, tal que $mdc(m, n) = 1$, então $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.*

Demonstração: Segue do Teorema 2.4.1. □

Definição 2.4.4 *Seja* $\mathbb{L}$ *uma extensão de* $\mathbb{K}$. *O* ***grupo de Galois*** *de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *é dado por:*

$$Gal(\mathbb{L}/\mathbb{K}) = \{\sigma \in Aut(\mathbb{L});\ \sigma(x) = x,\ \forall x \in \mathbb{K}\}.$$

Definição 2.4.5 *Seja* $\mathbb{L}$ *uma extensão de um corpo* $\mathbb{K}$. *Dizemos que* $\mathbb{L}$ *é uma* ***extensão cíclica****, se o grupo de Galois* $G = Gal(\mathbb{L}/\mathbb{K})$ *é cíclico.*

Teorema 2.4.2 *Seja* n *um inteiro positivo, assim, uma extensão ciclotômica* $\mathbb{Q}(\zeta_n)$ *é cíclica se, e somente se,* $n = 2, 4, p^r$ *ou* $2p^r$*, com* p *primo e diferente de 2, e* r *um inteiro maior ou igual a* 1.

Demonstração: Sabendo que o grupo de Galois de $\mathbb{Q}(\zeta_n)$ é isomorfo a $\mathbb{Z}_n^*$, o resultado segue pelo Teorema 2.3.2. □

2.5 Anel de Inteiros Algébricos

O objetivo, desta seção, é determinar o anel de inteiros algébricos dos corpos ciclotômicos, e suas respectivas bases, e metódos que possam nos ajudar no cálculo do discriminante destes corpos ciclotômicos.

Lema 2.5.1 *([8], p.19) Se* $\zeta_p \in \mathbb{C}$ *é uma raiz* p*-ésima primitiva da unidade, onde* p *é primo, e* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *então:*

(a) $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = -1, \quad e \quad Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p^j) = p, \quad para \quad j = 1, \ldots, p-1.$

(b) $N_{\mathbb{K}/\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p \quad e \quad N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) = p.$

(c) $p = (1 - \zeta_p)(1 - \zeta_p^2)\ldots(1 - \zeta_p^{p-1}).$

Demonstração: **(a)** Sabemos que o p-ésimo polinômio ciclotômico é dado por $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ e que suas raízes são $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. Como $\phi_p(\zeta_p^j) = 0$, para $j = 1, \ldots, p-1$, obtemos que $\zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j + 1 = 0$, e deste modo $\zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j = -1$. Como $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = -1$, para $j = 1, 2, \ldots, p-1$. Agora, pela Proposição 1.5.3 no item (a)

tem-se $Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p^j) = Tr_{\mathbb{K}/\mathbb{Q}}(1) - Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j)$ e $Tr_{\mathbb{K}/\mathbb{Q}}(1) = 1+1+\ldots+1 = p-1$, pois $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, e como $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = -1$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p^j) = p-1+1 = p$.

(b) Como $\zeta_p - 1$ é uma raiz do polinômio $f(x) = x^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} x^{j-1}$, segue que $N_{\mathbb{K}/\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$ e $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{K}/\mathbb{Q}}((-1)(\zeta_p - 1)) = p$.

(c) Sendo $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ as raízes do p-ésimo polinômio ciclotômico $\phi_p(x)$, segue que $(x-\zeta_p)(x-\zeta_p^2)\ldots(x-\zeta_p^{p-1}) = x^{p-1} + x^{p-2} + \ldots + x + 1$. Deste modo, tomando $p = 1$, obtemos que $p = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$. □

Lema 2.5.2 *([8], p.20) Sejam $\zeta_p \in \mathbb{C}$ uma raiz p-ésima primitiva da unidade, onde p um número primo e $\mathbb{Q}(\zeta_p) = \mathbb{K}$. Se $\mathbb{A}_\mathbb{K}$ é o anel de inteiros algébricos de $\mathbb{K}$, então,*

(a) $(1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$.

(b) $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in p\mathbb{Z}$, *para todo* $\alpha \in \mathbb{A}_\mathbb{K}$.

Demonstração: **(a)** Pelo Lema 2.5.1, tem-se que $p = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$. Como $1-\zeta_p^j \in \mathbb{A}_\mathbb{K}$, para $j = 1, \ldots, p-1$, obtemos que $p \in (1-\zeta_p)\mathbb{A}_\mathbb{K}$. Portanto, $p\mathbb{Z} \subset (1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z}$. Agora, suponha que $p\mathbb{Z} \subsetneq (1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z} \subset \mathbb{Z}$. Como $\mathbb{Z}$ é um anel principal, segue que o ideal primo $p\mathbb{Z}$ é maximal e assim $p\mathbb{Z} = (1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z}$ ou $(1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z} = \mathbb{Z}$. Se $(1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z} = \mathbb{Z}$ e como $1 \in \mathbb{Z}$, segue que $1 = (1-\zeta_p)\alpha$, onde $\alpha \in \mathbb{A}_\mathbb{K}$. Assim $1-\zeta_p$ é inversível, e consequentemente $1-\zeta_p^j$ são inversíveis em $\mathbb{A}_\mathbb{K}$, para $j = 2, \ldots, p-1$. Visto que $p = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$, segue que p é inversível em $\mathbb{Z}$, o que é um absurdo. Portanto $(1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$.

(b) Pelo item (a) é suficiente mostrar que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in (1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z}$. Se $\alpha_i(1-\zeta_p^i)$ são os conjugados de $\alpha(1-\zeta_p)$, então cada conjugado é um múltiplo de $1-\zeta_p$ em $\mathbb{A}_\mathbb{K}$, onde $i = 1, \ldots, p-1$. Como $1-\zeta_p^i = (1-\zeta_p)(\zeta_p^{i-1} + \zeta_p^{i-2} + \ldots + \zeta_p + 1)$, para $i = 1, 2, \ldots, p-1$, segue que $1-\zeta_p^i$ é um múltiplo de $1-\zeta_p$ em $\mathbb{A}_\mathbb{K}$. Agora, usando este fato, obtemos $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) = \sum_{i=1}^{p-1} \alpha_i(1-\zeta_p^i) = \beta(1-\zeta_p)$, onde $\beta \in \mathbb{A}_\mathbb{K}$. Logo $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in (1-\zeta_p)\mathbb{A}_\mathbb{K}$. Agora, pela Observação 1.3.1, tem-se que $\mathbb{Z}$ é integralmente fechado, e pela Proposição 1.5.1, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in \mathbb{Z}$. Assim, $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in (1-\zeta_p)\mathbb{A}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$. □

Teorema 2.5.1 *([1], p.43) Se $\zeta_p \in \mathbb{C}$ é uma raiz p-ésima primitiva de unidade, onde p um número primo e $\mathbb{K} = \mathbb{Q}(\zeta_p)$, então o anel de inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_p]$ e $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Se $\mathbb{A}_\mathbb{K}$ é o anel de inteiros algébricos de $\mathbb{Q}(\zeta_p)$, então $\mathbb{Z}[\zeta_p] \subset \mathbb{A}_\mathbb{K}$. Se $\alpha \in \mathbb{A}_\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, então

$$\alpha = a_0 + a_1\zeta_p + a_2\zeta_p^2 + \ldots + a_{p-2}\zeta_p^{p-2} \tag{2.1}$$

onde $a_i \in \mathbb{Q}$, para $i = 1, \ldots, p-2$. Multiplicando ambos os lados da Equação (2.1), por $1 - \zeta_p$ obtemos

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p - \zeta_p^2) + \ldots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}). \tag{2.2}$$

Aplicando o traço na Equação (2.2), pelo Lema 2.5.2 e pela linearidade do traço, tem-se que

$$Tr(\alpha(1-\zeta_p)) = a_0Tr(1-\zeta_p)a_1Tr(\zeta_p - \zeta_p^2) + \ldots + a_{p-2}Tr(\zeta_p^{p-2} - \zeta_p^{p-1}) \in p\mathbb{Z}.$$

Agora, pelo Lema 2.5.1, obtemos que $Tr(\zeta_p^i - \zeta_p^{i+1}) = Tr(\zeta_p^i) - Tr(\zeta_p^{i+1}) = -1+1 = 0$, para todo $i = 1, \ldots, p-2$. Novamente, pelo Lema 2.5.1 parte (a), tem-se que $a_0Tr(1-\zeta_p) = a_0p \in p\mathbb{Z}$, e portanto $a_0 \in \mathbb{Z}$. Por outro lado, como $\zeta_p^{-1} = \zeta_p^{p-1}$, segue que $\zeta_p^{p-1} \in \mathbb{A}_\mathbb{K}$. Assim, pela Equação (2.1), segue que

$$(\alpha - a_0)\zeta_p^{-1} = a_1 + a_2(\zeta_p) + \ldots + a_{p-2}\zeta_p^{p-3}. \tag{2.3}$$

Multiplicando ambos os lados da Equação (2.3) por $(1-\zeta_p)$ obtemos que

$$(\alpha - a_0)\zeta_p^{-1}(1-\zeta_p) = a_1(1-\zeta_p) + a_2(\zeta_p - \zeta_p^2) + \ldots + a_{p-2}(\zeta_p^{p-3} - \zeta_p^{p-2}). \tag{2.4}$$

Aplicando o traço na Equação (2.4), usando a linearidade do traço, concluímos que $Tr((\alpha - a_0)\zeta_p^{-1}(1-\zeta_p)) = a_1Tr(1-\zeta_p) + a_2Tr(\zeta_p - \zeta_p^2) + \ldots + a_{p-2}Tr(\zeta_p^{p-3} - \zeta_p^{p-2}) \in p\mathbb{Z}$, e de modo análogo, obtemos que $a_1 \in \mathbb{Z}$. Prosseguindo com o mesmo raciocínio, concluímos que $a_i \in \mathbb{Z}$, para todo $i = 1, \ldots, p-2$. Portanto $\alpha \in \mathbb{Z}[\zeta_p]$, ou seja, $\mathbb{A}_\mathbb{K} = \mathbb{Z}[\zeta_p]$. Finalmente, como $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ é linearmente independente sobre $\mathbb{Q}$ segue que $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ é linearmente independente sobre $\mathbb{Z}$, e usando o fato de $\mathbb{A}_\mathbb{K} = \mathbb{Z} + \mathbb{Z}\zeta_p + \ldots + \mathbb{Z}\zeta_p^{p-2}$, concluímos que $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$. □

Proposição 2.5.1 *([9], p.19) Se $\zeta_p \in \mathbb{C}$ é uma raiz p-ésima primitiva da unidade, onde p é um primo ímpar, então o dicriminante de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é dado por*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Demonstração: Pelo Teorema 2.5.1, $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$, e pela Proposição 1.5.6 o $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{K}/\mathbb{Q}}(\phi_p'(\zeta_p))$, onde $\phi_p'(x)$ é a derivada do p-ésimo polinômio ciclotômico. Assim

$$\phi_p'(\zeta_p) = \frac{p\zeta_p^{p-1}(\zeta_p - 1) - (\zeta_p^p - 1)}{(\zeta_p - 1)^2} = \frac{p\zeta_p^{p-1}}{\zeta_p - 1} = \frac{-p\zeta_p^{p-1}}{1 - \zeta_p}. \tag{2.5}$$

Aplicando a norma de $\mathbb{K}$ sobre $\mathbb{Q}$ em ambos os lados da Equação (2.5), usando sua linearidade e o Lema 2.5.1, obtemos que

$$N_{\mathbb{K}/\mathbb{Q}}\left(\frac{-p\zeta_p^{p-1}}{1 - \zeta_p}\right) = \frac{N_{\mathbb{K}/\mathbb{Q}}(-p)N_{\mathbb{K}/\mathbb{Q}}(\zeta_p^{p-1})}{N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p)} = \frac{(-p)^{p-1}1}{p} = p^{p-2}.$$

Finalmente, como p é ímpar, segue que $(-1)^{p-2} = -1$, e portanto

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2},$$

o que prova a proposição. □

Teorema 2.5.2 *([7], p.48) O anel de inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, com p primo, é $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ e $\{\zeta_p + \zeta_p^{p-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Pelo Teorema 2.5.1 tem-se que $\mathbb{Z}[\zeta_p]$ é o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_p)$. Como ζ_p e ζ_p^{-1} são inteiros algébricos, pelo Corolário 1.3.1, segue que $\zeta_p + \zeta_p^{-1}$ é um inteiro algébrico, e portanto $\mathbb{Z}[\zeta_p + \zeta_p^{p-1}] \subset \mathbb{A}_{\mathbb{K}}$. Agora, se $\alpha \in \mathbb{A}_{\mathbb{K}}$, então

$$\alpha = a_1(\zeta_p + \zeta_p^{-1}) + a_2(\zeta_p^2 + \zeta_p^{p-2}) + \ldots + a_{\frac{p-1}{2}}(\zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}) \tag{2.6}$$

onde $a_i \in \mathbb{Q}$, para $i = 1, \ldots, \frac{p-1}{2}$. Multiplicando ambos os lados da Equação (2.6) por $\zeta_p^{\frac{p-1}{2}}$, obtemos que $\zeta_p^{\frac{p-1}{2}}\alpha = a_1\zeta_p^{\frac{p+1}{2}} + a_1\zeta_p^{\frac{p-3}{2}} + \ldots + a_{\frac{p-1}{2}}\zeta_p^{p-1} + a_{\frac{p-1}{2}}$, e portanto é um inteiro algébrico de $\mathbb{Q}(\zeta_p)$, ou seja, pertence à $\mathbb{Z}[\zeta_p]$. Logo $a_i \in \mathbb{Z}$, para $i = 1, \ldots, \frac{p-1}{2}$, e assim $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Deste modo $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Agora, como $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ e pelo fato que $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\} \subset \mathbb{Z}[\zeta_p + \zeta_p^{-1}] = \mathbb{A}_{\mathbb{K}}$, é suficiente mostrar que $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ são linearmente independentes. Assim, se considerarmos $a_1(\zeta_p + \zeta_p^{-1}) + \ldots + a_{\frac{p-1}{2}}(\zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}) = 0$, com $a_1, \ldots, a_{\frac{p-1}{2}} \in \mathbb{Z}$, então, $a_1\zeta_p + a_1\zeta_p^{-1} + \ldots + a_{\frac{p-1}{2}}\zeta_p^{\frac{p-1}{2}} + a_{\frac{p-1}{2}}\zeta_p^{\frac{1-p}{2}} = 0$. Como $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$, segue que $a_1 = a_2 = \ldots = a_{\frac{p-1}{2}} = 0$, e assim $\{\zeta_p + \zeta_p^{p-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é linearmente independente. Portanto $\{\zeta_p + \zeta_p^{p-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ sobre $\mathbb{Z}$. □

Teorema 2.5.3 *([7], p.93) Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_p)$, onde p é um primo ímpar, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$|D_{\mathbb{K}/\mathbb{Q}}| = p^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Lema 2.5.3 *([8], p.20) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, com p primo e r um inteiro maior que 1. Se $\mathbb{A}_{\mathbb{K}}$ é o anel de inteiros algébricos de $\mathbb{K}$ então:*

(a) $(1 - \zeta_{p^r})\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

(b) $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_{p^r})) \in p\mathbb{Z}$, *para todo* $\alpha \in \mathbb{A}_{\mathbb{K}}$.

Demonstração: Análoga a do Lema 2.5.2. □

Lema 2.5.4 *([11], p.30) Se p é um primo ímpar e $r \geq 1$, então $\mathbb{Z}[1 - \zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$.*

Demonstração: Se $\alpha \in \mathbb{Z}[1 - \zeta_{p^r}]$, então

$$\alpha = a_0 + a_1(1 - \zeta_{p^r}) + a_2(1 - \zeta_{p^r})^2 + \ldots + a_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}} =$$
$$= (a_0 + a_1 + \ldots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2)\zeta_{p^r} + \ldots.$$

e assim $\alpha = b_0 + b_1\zeta_{p^r} + \ldots + b_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}} \in \mathbb{Z}[\zeta_{p^r}]$. Portanto, $\mathbb{Z}[1-\zeta_{p^r}] \subseteq \mathbb{Z}[\zeta_{p^r}]$. Por outro lado, se $\alpha \in Z[\zeta_{p^r}]$, então existem $a_i \in \mathbb{Z}$, para $i = 0, 1, \ldots, (p-1)p^{r-1}$, tal que

$$\alpha = a_0 + a_1\zeta_p^r + \ldots + a_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}. \tag{2.7}$$

Como $\zeta_{p^r} = 1 - (1 - \zeta_{p^r})$, segue que podemos escrever a Equação (2.7) como

$$\alpha = a_0 + a_1(1-(1-\zeta_{p^r})) + a_2(1-(1-\zeta_{p^r}))^2 + \ldots + a_{(p-1)p^{r-1}}(1-(1-\zeta_{p^r}))^{(p-1)p^{r-1}}$$
$$= (a_0 + a_1 + \ldots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2 - \ldots - ((p-1)p^{r-1}-1)a_{(p-1)p^{r-1}-1})$$
$$(1-\zeta_{p^r}) + (a_2 - 3a_3 + \ldots)(1-\zeta_{p^r})^2 + \ldots,$$

e assim $\alpha = b_0 + b_1(1-\zeta_{p^r}) + b_2(1-\zeta_{p^r})^2 + \ldots + b_{(p-1)p^{r-1}}(1-\zeta_{p^r})^{(p-1)p^{r-1}} \in \mathbb{Z}[1-\zeta_{p^r}]$, o que mostra que $\mathbb{Z}[\zeta_{p^r}] \subseteq \mathbb{Z}[1-\zeta_{p^r}]$. Portanto $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. □

Proposição 2.5.2 *([11], p.31) Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um primo e r é um inteiro maior que 1, então:*

(a) $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$, *para* $j = 1, 2, \ldots, p^{r-1}$, *onde* $mdc(j, p^r) = 1$.

(b) *Se* $\mathfrak{a}$ *é um ideal, então* $Tr_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a}) = (p-1)p^{r-1}\mathfrak{a}$ *e* $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a}) = \mathfrak{a}^{(p-1)p^{r-1}}$.

(c) *Se* $p \nmid k$, *onde* $1 \leq k \leq p^r$, *então* $\prod_k (1-\zeta_{p^r}^k) = p$, *assim,* $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = p$.

Demonstração: **(a)** Como $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = \zeta_{p^r}^j \zeta_{p^r}^{j+1} \ldots \zeta_{p^r}^{j+p^{r-1}}$, para $j = 1, \ldots, p^{r-1}$, onde $mdc(j,p) = 1$, e como $\zeta_{p^r}^j$ e $\zeta_{p^r}^{j+p^{r-1}}$ são conjugados, obtemos que $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$, para $j = 1, \ldots, p^{r-1}$, onde $mdc(j, p^r) = 1$.

(b) Como $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1)p^{r-1}$, o resultado segue dos itens (c) e (f) da Proposição 1.5.3.

(c) O p^r-ésimo polinômio ciclotômico é dado por

$$\phi_{p^r}(x) = \frac{x^{p^r}-1}{\phi_1(x)\phi_2(x)\ldots\phi_{p^{r-1}}(x)} = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = x^{(p-1)p^{r-1}} + \ldots + x^{p^{r-1}} + 1.$$

Assim, para todo k, tal que $p \nmid k$ e $1 \leq k \leq p^r$, tem-se que os elementos $\zeta_{p^r}^k$ são raízes de $\phi_{p^r}(x)$, uma vez que são raízes de $x^{p^r}-1$, mas não são raízes de $x^{p^{r-1}}-1$. Deste modo, $\phi_{p^r}(x) = \prod_k (x-\zeta_{p^r}^k)$, e existem $\Phi(p^r) = (p-1)p^{r-1}$ valores de k, pois $\partial(\phi_{p^r}(x)) = (p-1)p^{r-1}$. Agora, tomando $x = 1$, obtemos que

$$\phi_{p^r}(1) = \prod_{k\,;p\nmid k}^{p^r} (1-\zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + \ldots + 1^{(p-1)p^{r-1}} = p = N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = p.$$

□

Teorema 2.5.4 *([11], p.31) Sejam $\mathbb{K}$ uma extensão finita de grau n de $\mathbb{Q}$ e $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, com $\alpha_i \in \mathbb{A}_{\mathbb{K}}$, para $i = 1, \ldots, n$. Se $D_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) = d$ e $\alpha \in \mathbb{A}_{\mathbb{K}}$, então α pode ser escrito da forma*

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

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

Demonstração: Como $\alpha \in \mathbb{A}_{\mathbb{K}}$, e como $\mathbb{A}_{\mathbb{K}} \subset \mathbb{K}$, segue que $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$, onde $a_i \in \mathbb{Q}$, para $i = 1, \ldots, n$. Sejam σ_i, para $i = 1, 2, \ldots, n$, os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Aplicando todos os $\sigma_i's$ em α, obtemos um sistema de n equações dado por

$$\begin{cases} \sigma_1(\alpha) &= a_1\sigma_1(\alpha_1) + \ldots + a_n\sigma_1(\alpha_n) \\ \quad\vdots & \\ \sigma_n(\alpha) &= a_1\sigma_n(\alpha_1) + \ldots + a_n\sigma_n(\alpha_n). \end{cases}$$

Resolvendo este sistema por Cramer, obtemos as n raízes, que são dadas por $a_j = \dfrac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_i))$ e γ_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$, para $i, j = 1, 2, \ldots, n$. Note que δ e γ_j, para $j = 1, \ldots, n$, são inteiros algébricos, uma vez que são obtidos via $\alpha_i's$, que são inteiros algébricos. Assim pela Proposição 1.5.5, obtemos que $\delta^2 = d$, e deste modo $da_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j$, para $j = 1, 2, \ldots, n$, e portanto da_j é um inteiro algébrico, para $j = 1, 2, \ldots, n$. Como $\mathbb{Z}$ é integralmente fechado, segue que $da_j \in \mathbb{Z}$, para $j = 1, 2, \ldots, n$. Tomando $m_j = da_j$, para $j = 1, 2, \ldots, n$, é suficiente mostrar que $\dfrac{m_j^2}{d} \in \mathbb{Z}$, pois assim m_j^2 será divisível por d. Agora, como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$ e $\dfrac{m_j^2}{d} \in \mathbb{Q}$, para $j = 1, 2, \ldots, n$, é suficiente mostrar que $\dfrac{m_j^2}{d}$ é um inteiro algébrico. Deste modo, se $m_j = da_j = \delta\gamma_j$, para $j = 1, 2, \ldots, n$, então $m_j^2 = \delta^2\gamma_l^2 = d\gamma_j^2$, ou seja, $\dfrac{m_j^2}{d} = \gamma_j^2$. Assim, m_j^2 é um inteiro algébrico, pois γ_j é um inteiro algébrico, para $j = 1, 2 \ldots, n$. Portanto, $\dfrac{m_j^2}{d} \in \mathbb{Z}$, ou seja, m_j^2 é divisível por d, para $j = 1, 2, \ldots, n$. Assim, $\alpha = \dfrac{m_1\alpha_1 + \ldots + m_n\alpha_n}{d}$, onde $m_j \in \mathbb{Z}$ e m_j^2 é divisível por d para $j = 1, \ldots, n$. □

Lema 2.5.5 *([11], p.31] Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, com p primo e r um inteiro maior que 1. Se $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p^r, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$, então $d = p^t$, para algum $t \in \mathbb{N}$.*

Demonstração: Sabemos que o p^r-ésimo polinômio ciclotômico é dado por $\phi_{p^r}(x) = \dfrac{x^{p^r}-1}{x^{p^{r-1}}-1}$, logo, $x^{p^r} - 1 = \phi_{p^r}(x)g(x)$, onde $g(x) = x^{p^{r-1}} - 1$. Agora, derivando ambos os lados, obtemos $p^r x^{p^r-1} = \phi'_{p^r}(x)g(x) + \phi_{p^r}(x)g'(x)$, e substituindo x por ζ_{p^r}, obtemos que $p^r(\zeta_{p^r})^{p^r-1} = \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r})$, pois $\phi_{p^r}(\zeta_{p^r}) = 0$. Assim, $p^r(\zeta_{p^r})^{p^r}(\zeta_{p^r})^{-1} = \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r})$, ou seja,

$$p^r = \zeta_{p^r}\phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}). \tag{2.8}$$

Aplicando a função norma na Equação (2.8), obtemos

$$p^{r(p-1)p^{r-1}} = N(\phi'_{p^r}(\zeta_{p^r}))N(\zeta_{p^r}g(\zeta_{p^r})).$$

Pela Proposição 1.5.5, tem-se que $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = (\pm 1)N(\phi'_{p^r}(\zeta_{p^r}))$ e por hipótese, $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p^r, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$. Assim, $p^{r(p-1)p^{r-1}} = dN(\zeta_{p^r}g(\zeta_{p^r}))$, e portanto $d = p^t$, para algum $t \in \mathbb{Z}$. □

Teorema 2.5.5 *([11], p.30) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, com p primo e r um inteiro maior que 1. Se $\mathbb{A}_{\mathbb{K}}$ é o anel de inteiros algébricos de $\mathbb{K}$, então $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$.*

Demonstração: Pelo Lema 2.5.4, tem-se que $\mathbb{Z}[1 - \zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. Suponhamos que $\mathbb{A}_{\mathbb{K}} \neq \mathbb{Z}[1 - \zeta_{p^r}]$. Sejam $\alpha \in \mathbb{A}_{\mathbb{K}}$ e $n = [\mathbb{K} : \mathbb{Q}] = \Phi(p^r)$. Pelo Teorema 2.5.4 e pelo Lema 2.5.5 podemos escrever

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

onde $m_i \in \mathbb{Z}$ e m_i^2 divisível por $p^s = d$, para todo $i = 1, \ldots, n$. Assim, existe $\alpha \in \mathbb{A}_{\mathbb{K}}$ de modo que nem todos os m_i são divisíveis por p^s. Seja $i \leq n$ tal que os m_i não sejam divisíveis por p^s. Deste modo, existem $q, r \in Z$ tal que $m_i = p^s q + r$, com $r < p^s$. Dessa forma podemos escrever α da seguinte forma,

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

Com isso, $\mathbb{A}_{\mathbb{K}}$ possui um elemento da forma

$$\beta = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^i + \ldots + m_n(1-\zeta_{p^r})^{n-1}}{p^s}. \tag{2.9}$$

Multiplicando ambos os lados da Equação (2.9) por p^{s-1}, obtemos

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

ou seja,

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

onde $a_i \in \mathbb{Z}$ e a_i não divisível por p. Agora, pela Proposição 2.5.2, tem-se que $\prod_{k=1, p\nmid k}^{p^r} (1-\zeta_{p^r}^k) = p$. Como $1-\zeta_{p^r}^k$ é divisível por $1-\zeta_{p^r}$ em $\mathbb{Z}[1-\zeta_{p^r}]$, segue que $\frac{p}{(1-\zeta_{p^r})^n} \in \mathbb{Z}[1-\zeta_{p^r}]$. Agora, como $\frac{p}{(1-\zeta_{p^r})^n} \in \mathbb{Z}[1-\zeta_{p^r}]$ e $\lambda \in \mathbb{A}_{\mathbb{K}}$, segue que

$$\frac{\lambda p}{(1-\zeta_{p^r})^n} \in \mathbb{Z}[1-\zeta_{p^r}].$$

Subtraindo termos que estão em $\mathbb{A}_{\mathbb{K}}$ obtemos $\frac{a_i}{(1-\zeta_{p^r})} \in \mathbb{A}_{\mathbb{K}}$, e assim $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r})$ divide $N_{\mathbb{K}/\mathbb{Q}}(a_i)$. Agora, como $N_{\mathbb{K}/\mathbb{Q}}(a_i) = a_i^n$ e $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = p$, segue que $p|a_i^n$, o que é um absurdo pois $p \nmid a_i$. Portanto $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. □

Corolário 2.5.1 *([7], p.52) Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, com p primo e r um inteiro maior que 1, então o anel dos inteiros de $\mathbb{K}$ é $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$.*

Proposição 2.5.3 *([10], p.9) Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, com p um primo ímpar e r um inteiro maior que 1, então o dicriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm p^{p^{r-1}(r(p-1)-1)}.$$

Demonstração: Pela Proposição 1.5.6, tem-se que

$$D(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm N_{\mathbb{K}/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r}),$$

onde $\phi'_{p^r}(x)$ é a derivada do p^r-ésimo polinômio ciclotômico. Assim,

$$\phi'_{p^r}(\zeta_{p^r}) = \frac{p^r\zeta_{p^r}^{p^r-1}(\zeta_{p^r}^{p^r-1}-1) - (\zeta_{p^r}^{p^r}-1)p^{r-1}\zeta_{p^r}^{p^{r-1}-1}}{(\zeta_{p^r}^{p^{r-1}}-1)^2} = \frac{-p^r}{(1-\zeta_{p^r}^{p^{r-1}})\zeta_{p^r}}, \qquad (2.10)$$

uma vez que $\zeta_{p^r}^{p^r} = 1$. Aplicando a norma em ambos os lados da Equação (2.10), usando sua linearidade e a Proposição 2.5.2, obtemos que

$$N_{\mathbb{K}/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})) = \frac{N_{\mathbb{K}/\mathbb{Q}}(-p^r)}{N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p)N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r})} = \frac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)},$$

e portanto, $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm p^{p^{r-1}(r(p-1)-1)}$. □

Teorema 2.5.6 *([7], p.92) Seja p um primo ímpar e r um inteiro positivo. Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, com $[\mathbb{K} : \mathbb{Q}] = up^j$, onde u é um divisor de $p-1$ e $0 < j \leq r-1$, então o discriminante do corpo $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por:*

$$|D_{\mathbb{K}/\mathbb{Q}}| = p^{\beta_{(u,j)}},$$

onde $\beta_{(u,j)} = u\left[(j+2)p^j - \dfrac{p^{j+1}-1}{p-1}\right] - 1.$

Teorema 2.5.7 *([10], p.11) O anel de inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \ldots, \zeta_n^{\Phi(n)-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ como um $\mathbb{Z}$-módulo.*

Teorema 2.5.8 *([10], p.12) Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde n é um inteiro maior que 1, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_n, \ldots, \zeta_{p^r}^{\Phi(n)-1}) = \frac{n^{\Phi(n)}}{\prod_{p|n} p^{\Phi(n)/(p-1)}}.$$

Definição 2.5.1 *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números, $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_m\}$ bases de $\mathbb{K}$ sobre $\mathbb{Q}$ e $\mathbb{L}$ sobre $\mathbb{Q}$, respectivamente. Dizemos que $\mathbb{K}$ e $\mathbb{L}$ são* ***linearmente disjuntos*** *se $\{\alpha_1\beta_1, \ldots, \alpha_n\beta_m\}$ é uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$.*

Teorema 2.5.9 *([7], p.110) Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números de graus n e m, respectivamente. Se os discriminantes $D_{\mathbb{K}/\mathbb{Q}}$ e $D_{\mathbb{L}/\mathbb{Q}}$ são relativamente primos e os corpos são linearmente disjuntos, então*

$$D_{\mathbb{KL}/\mathbb{Q}} = (D_{\mathbb{K}/\mathbb{Q}})^m (D_{\mathbb{L}/\mathbb{Q}})^n.$$

2.6 Corpos Abelianos

Nesta seção, apresentamos alguns resultados de corpos abelianos e também sobre seus subcorpos. Assim, através destes resultados, determinamos o anel de inteiros algébricos de subcorpos de $\mathbb{Q}(\zeta_p)$, que será muito útil no decorrer do nosso trabalho, principalmente na construção de reticulados via subcorpos de corpos ciclotômicos.

Teorema 2.6.1 *([10], p.401) (Kronecker-Weber) Se $\mathbb{L}$ é uma extensão abeliana de $\mathbb{Q}$ então $\mathbb{L} \subseteq \mathbb{Q}(\zeta_n)$, para algum n.*

Com base no Teorema 2.6.1, concluímos que o estudo de corpos de números abelianos é equivalente ao estudo de subcorpos de corpos ciclotômicos.

Definição 2.6.1 *Seja $\mathbb{L}$ uma extensão finita e abeliana de $\mathbb{Q}$. O menor n tal que $\mathbb{L} \subseteq \mathbb{Q}(\xi_n)$ é chamado de* ***condutor*** *de $\mathbb{L}$.*

Sejam $\zeta_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade, $\mathbb{L} = \mathbb{Q}(\zeta_n)$, $\mathbb{K} \subset \mathbb{L}$, onde $[\mathbb{L} : \mathbb{K}] = m$, $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_n)$ e $g \in \mathbb{Z}$ tal que σ_g gera o grupo de Galois $G = Gal(\mathbb{L}/\mathbb{Q})$. Como G é um grupo cíclico (logo abeliano) segue que os subgrupos de G são normais. Assim, pelo Teorema Fundamental de Galois, temos que os subcorpos correspondentes a esses subgrupos são **extensões Galoisianas**. Portanto $\mathbb{Q} \subseteq \mathbb{Q}(\theta)$ é uma extensão Galoisiana.

Se $H = Gal(\mathbb{L}/\mathbb{K})$ então H tem ordem m. Como $G = \langle \sigma_g \rangle$, segue pelo Teorema 2.4.1, que a ordem de σ_g é $\Phi(n)$. Assim, $\sigma_{g^{\frac{\Phi(n)}{m}}}$ gera um subgrupo de ordem m, e portanto $H = \{\sigma_{g^{\frac{\Phi(n)}{m}}}, \sigma_{g^{2\frac{\Phi(n)}{m}}}, \cdots, \sigma_{g^{m\frac{\Phi(n)}{m}}}\}$. Além disso, tem-se que

$$\theta = \zeta^{g^{\frac{\Phi(n)}{m}}} + \zeta^{g^{2\frac{\phi(n)}{m}}} + \cdots + \zeta^{g^{m\frac{\Phi(n)}{m}}}$$

e

$$\sigma_{g^i}(\theta) = \sigma_{g^i}(\zeta^{g^{\frac{\Phi(n)}{m}}} + \zeta^{g^{2\frac{\Phi(n)}{m}}} + \cdots + \zeta^{g^{m\frac{\Phi(n)}{m}}}) = \zeta^{g^{\frac{\Phi(n)}{m}+i}} + \zeta^{g^{2\frac{\Phi(n)}{m}+i}} + \cdots + \zeta^{g^{m\frac{\Phi(n)}{m}+i}},$$

para $i = 1, 2, \cdots, \frac{\Phi(n)}{m}$.

Sejam $s = \frac{\Phi(n)}{m}$, $n = p_1^{a_1} \cdots p_s^{a_s}$ a decomposição de n em fatores primos distintos, e t_1, t_2, i_1, i_2 números inteiros tais que $1 \leq t_1, t_2 \leq m, 1 \leq i_1, i_2 \leq s$.

Proposição 2.6.1 *([13], p.69) Se $t_1 = t_2$ e $i_1 \neq i_2$ (ou $t_1 \neq t_2$ e $i_1 = i_2$) então $\zeta^{g^{t_1 s+i_1}} \neq \zeta^{g^{t_2 s i_2}}$.*

Demonstração: Suponha que $\zeta^{g^{t_1 s+i_1}} = \zeta^{g^{t_2 s+i_2}}$ com $t_1 = t_2$ e $i_1 \neq i_2$, assim $g^{t_1 s+i_1} \equiv g^{t_2 s+i_2}(mod\ n)$, ou seja, n divide $g^{t_1 s+i_1} - g^{t_2 s+i_2} = g^{t_1 s}(g^{i_1} - g^{i_2})$. Como $t_1 = t_2$ e $p_i^{a_i}$ divide n, segue que $p_i^{a_i}$ divide $g^{t_1 s}(g^{i_1} - g^{i_2})$, para $i = 1, 2, \cdots, s$. Além disso, como $mdc(g, n) = 1$ segue que $mdc(g^{t_1 s}, p_i^{a_i}) = 1$ e portanto $p_i^{a_i}$ divide $g^{i_1} - g^{i_2}$ para $i = 1, 2, \cdots, s$. Assim, n divide $g^{i_1} - g^{i_2}$. Deste modo, se $i_1 > i_2$ então $i_1 = i_2 + t$ com t um inteiro positivo. Assim, n divide $g^{i_2}(g^t - 1)$ e portanto n divide $g^t - 1$, uma vez que $mdc(n, g^{i_2}) = 1$. Logo, $g^t \equiv 1(mod\ n)$. Agora, como $t = i_1 - i_2 \leq s - 1 \leq \frac{\Phi(n)}{m} < \Phi(n)$, segue que a ordem do subgrupo gerado por g é menor que $\Phi(n)$, o que é um absurdo. Portanto $\zeta^{g^{t_1 s+i_1}} \neq \zeta^{g^{t_2 s+i_2}}$. Para o caso em que $t_1 \neq t_2$ e $i_1 = i_2$ a demonstração é análoga. □

Proposição 2.6.2 *([13], p.69) Se $t_1 \neq t_2$ e $i_1 \neq i_2$ então $\zeta^{g^{t_1 s+i_1}} \neq \zeta^{g^{t_2 s+i_2}}$.*

Demonstração: Se $\zeta^{g^{t_1 s+i_1}} = \zeta^{g^{t_2 s+i_2}}$, então $g^{t_1 s+i_1} \equiv g^{t_2 s+i_2}(mod\ n)$, ou seja, n divide $g^{t_1 s+i_1} - g^{t_2 s+i_2}$. Agora, se $t_1 > t_2$ e $i_1 > i_2$, então existem $k_1, k_2 \in \mathbb{N}$ tais que $t_1 = t_2 + k_1$ e $i_1 = i_2 + k_2$, e portanto n divide $g^{t_2 s+i_2}(g^{k_1 s+k_2} - 1)$. Agora, como $mdc(n, g^{t_2 s+i_2}) = 1$, segue que n divide $g^{k_1 s+k_2} - 1$, ou seja, $g^{k_1 s+k_2} \equiv 1(mod\ n)$. Como $k_1 \leq m - 1$ e $k_2 \leq s - 1$, segue que $k_1 s \leq (m-1)s$ e que $k_1 s + k_2 \leq (m-1)s + s_1 = ms - 1 < ms = \phi(n)$. Logo, a ordem de g é menor que $\Phi(n)$, o que é um absurdo. Portanto $\zeta^{g^{t_1 s+i_1}} \neq \zeta^{g^{t_2 s+i_2}}$. □

Corolário 2.6.1 *([13], p.69) Os elementos $\zeta^{g^{t\frac{\Phi(n)}{m}+i}}$, com $t = 1, 2, \cdots, m$ e $i = 1, 2, \cdots, \frac{\Phi(n)}{m}$, são dois a dois distintos.*

Demonstração: Segue diretamente das Proposições 2.6.1 e 2.6.2. □

Lema 2.6.1 *([13], p.69) Se $\mathbb{K}$ é um subcorpo $\mathbb{Q}(\zeta_p)$, com p primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, e $g \in G$ é tal que σ_g gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, então o conjunto*

$$\{\zeta_p^{g^{s+1}}, \ldots, \zeta_p^{g^{rs+1}}, \zeta_p^{g^{s+2}}, \ldots, \zeta_p^{g^{rs+2}}, \ldots, \zeta_p^{g^{s+s}}, \ldots, \zeta_p^{g^{rs+s}}\},$$

é linearmente independente.

Demonstração: Considere a seguinte combinação linear,

$$\sum_{j=1}^{s}\sum_{i=1}^{r} a_{ji}\zeta_p^{g^{is+j}} = 0. \tag{2.11}$$

Pelo Corolário 2.6.1, segue que os elementos $\zeta_p^{g^{is+j}}$ são dois a dois distintos, num total de $p-1$ elementos. Assim, a Equação (2.11) pode ser escrita da seguinte forma, $\sum_{k=1}^{p-1} b_k\zeta_p^k = 0$, com $b_k \in \mathbb{Q}$, para $k = 1, \ldots, p-1$. Mas, pelo Teorema 2.5.1, tem-se que o conjunto $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ é uma base de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$, e assim $b_k = 0$, para $k = 1, \ldots, p-1$. Deste modo, segue que $a_{ji} = 0$, para todo $j = 1, \ldots, s$ e $i = 1, \ldots, t$. Com isto, concluímos que o conjunto

$$\{\zeta_p^{g^{s+1}}, \ldots, \zeta_p^{g^{rs+1}}, \zeta_p^{g^{s+2}}, \ldots, \zeta_p^{g^{rs+2}}, \ldots, \zeta_p^{g^{s+s}}, \ldots, \zeta_p^{g^{rs+s}}\}$$

é linearmente independente. □

Teorema 2.6.2 *([13], p.70) Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_p)$, com p primo, de modo que $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p) = \theta$ e $g \in G$ é tal que σ_g gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, então $\mathbb{K} = \mathbb{Q}(\theta)$.*

Demonstração: Por hipótese, como $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p) = \theta$, segue que $\theta \in \mathbb{K}$, e portanto $\mathbb{Q}(\theta) \subset \mathbb{K}$. Por outro lado, pelo Teorema 2.4.2, tem-se que o grupo $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ é cíclico, ou seja, $G =< \sigma_g >$. Agora, seja $G' = Gal(\mathbb{Q}(\zeta_p)/\mathbb{K})$. Como $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, segue que o subgrupo cíclico que fixa o corpo $\mathbb{K}$ tem ordem r. Sendo $\{\overline{g^s}, \overline{g^{2s}}, \ldots, \overline{g^{rs}} = \overline{1}\}$ o único subgrupo de $\mathbb{Z}_p^*$ de ordem r, e como ordem de G' é r, segue que $G' =< \sigma_{g^s} >= \{\sigma_{g^s}, \sigma_{g^{2s}}, \ldots, \sigma_{g^{rs}}\}$. Do fato que $\mathbb{Q} \subset \mathbb{Q}(\theta) \subset \mathbb{K} \subset \mathbb{Q}(\zeta_p)$, e que G é um subgrupo cíclico, segue que $\mathbb{Q}(\theta)$ é fixado por um subgrupo cíclico, ou seja, logo um subgrupo normal. Assim, $\mathbb{Q}(\theta)/\mathbb{Q}$ é uma extensão galoisiana. Agora, se $f(x) \in \mathbb{Q}(\theta)$ é o polinômio irredutível de θ, então

$$f(\theta) = \theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 = 0, \tag{2.12}$$

onde $a_i \in \mathbb{Q}$, para $i = 1, \ldots, n-1$. Aplicando σ_{g^i} na Equação (2.12), para $i = 1, \ldots, s$, vemos que $\sigma_{g^i}(\theta)$ é raiz de $f(x)$. Como $\mathbb{Q}(\theta)/\mathbb{Q}$ é uma extensão ga-

loisiana, concluímos que $\sigma_{g^i}(\theta) \in \mathbb{Q}(\theta)$, para $i = 1, \ldots, s$. Agora, se $\sum_{i=1}^{s} a_i \sigma_{g^i}(\theta) = 0$, onde $a_i \in \mathbb{Q}$, para $i = 1, \ldots, s$, então,

$$a_1\zeta_p^{g^{s+1}} + \ldots + a_1\zeta_p^{g^{rs+1}} + a_2\zeta_p^{g^{s+2}} + \ldots + a_2\zeta_p^{g^{rs+2}} + \ldots + a_s\zeta_p^{g^{s+s}} + \ldots + a_s\zeta_p^{g^{rs+s}} = 0.$$

Dessa forma, pelo Lema 2.6.1, tem-se que o conjunto

$$\{\zeta_p^{g^{s+1}}, \ldots, \zeta_p^{g^{rs+1}}, \zeta_p^{g^{s+2}}, \ldots, \zeta_p^{g^{rs+2}}, \ldots, \zeta_p^{g^{s+s}}, \ldots, \zeta_p^{g^{rs+s}}\}$$

é linearmente independente, e portanto $a_i = 0$, para $i = 1, \ldots, s$. Portanto, o conjunto $\{\sigma_g(\theta), \sigma_{g^2}(\theta), \ldots, \sigma_{g^s}(\theta)\}$ é linearmente independente, e como esse conjunto está contido em $\mathbb{Q}(\theta)$, segue que $[\mathbb{Q}(\theta) : \mathbb{Q}] \geq s$. Mas, como $\mathbb{Q}(\theta) \subset \mathbb{K}$ e $[\mathbb{K} : \mathbb{Q}] = s$, segue que $\mathbb{K} = \mathbb{Q}(\theta)$. □

Teorema 2.6.3 *([13], p.71) Se $\mathbb{K}$ é um subcorpo $\mathbb{Q}(\zeta_p)$, com p primo, de modo que $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p) = \theta$ e $g \in G$ é tal que σ_g gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, então $\mathbb{Z}\sigma_g(\theta) + \ldots + \mathbb{Z}\sigma_{g^s}(\theta)$ é o anel dos inteiros algébricos de $\mathbb{K}$.*

Demonstração: Pelo Teorema 2.6.2, tem-se que $\mathbb{K} = \mathbb{Q}(\theta)$, logo uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ é $\{\sigma_g(\theta), \sigma_{g^2}(\theta), \ldots, \sigma_{g^s}(\theta)\}$. Se $\alpha \in \mathbb{Z}\sigma_g(\theta) + \ldots + \mathbb{Z}\sigma_{g^s}(\theta)$, então $\alpha = \sum_{i=1}^{s} a_i \sigma_{g^i}(\theta)$, onde $a_i \in \mathbb{Z}$, para $i = 1, \ldots, s$. Como $\sigma_{g^i}(\theta) = \zeta_p^{g^{s+i}} + \ldots + \zeta_p^{g^{rs+i}}$, segue que $\sigma_{g^i}(\theta) = 0\zeta_p + 0\zeta_{p^2} + \ldots + \zeta_p^{g^{s+i}} + \ldots + \zeta_p^{g^{rs+i}} + \ldots + 0\zeta_p^{p-1}$. Assim, $\sigma_{g^i}(\theta) \in \mathbb{Z}[\zeta_p]$ e como $\sigma_{g^i}(\theta) \in \mathbb{K}$ segue que, $\sigma_{g^i}(\theta) \in \mathbb{K} \cap \mathbb{Z}[\zeta_p]$, e portanto $\mathbb{Z}\sigma_g(\theta) + \ldots + \mathbb{Z}\sigma_{g^s}(\theta) \subset \mathbb{A}_{\mathbb{K}}$. Agora, se $\alpha \in \mathbb{A}_{\mathbb{K}} \subseteq \mathbb{K}$, então existem $a_i \in \mathbb{Q}$, para $i = 1, \ldots, s$, tal que $\alpha = \sum_{i=1}^{s} a_i \sigma_{g^i}(\theta)$, e $\{\sigma_g(\theta), \sigma_{g^2}(\theta), \ldots, \sigma_{g^s}(\theta)\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim, podemos escrever $\alpha = \sum_{i=1}^{s} a_i \sigma_{g^i}(\theta) = \sum_{i=1}^{s} a_i \zeta_p^{g^{r+i}}$, e deste modo, com o mesmo raciocínio usado na demonstração do Teorema 2.6.1, α pode ser escrito como $\alpha = \sum_{i=1}^{p-1} b_i \zeta_p^i$, onde $b_i \in \mathbb{Q}$, para $i = 1, \ldots, p-1$. Como $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, segue que $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$. Assim $\alpha \in \mathbb{Z}[\zeta_p]$, onde $b_i \in \mathbb{Z}$ para $i = 1, \ldots, p-1$, e consequentemente $a_i \in \mathbb{Z}$, para $i = 1, \ldots, s$. Portanto $\alpha \in \sum_{i=1}^{s} \mathbb{Z}\sigma_{g^i}(\theta)$, ou seja,

$\mathbb{A}_{\mathbb{K}} \subset \sum_{i=1}^{s} \mathbb{Z}\sigma_{g^i}(\theta)$. Assim, concluímos que $\mathbb{A}_{\mathbb{K}} = \sum_{i=1}^{s} \mathbb{Z}\sigma_{g^i}(\theta)$. □

Exemplo 2.6.1 *Seja $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_5)$, tal que $[\mathbb{Q}(\zeta_5) : \mathbb{K}] = 2$. Assim, $[\mathbb{K} : \mathbb{Q}] = 2$. Se $G = Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, então $G \simeq \mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, e pelo Teorema 2.4.2, segue que $\mathbb{Q}(\zeta_5)$ é uma extensão cíclica de $\mathbb{Q}$. Como $\sigma_2 \in G$ e $o(\sigma_2) = 4$, que é igual a ordem do grupo G, segue que $G =< \sigma_2 >$, e assim, pelo Lema 2.6.1 o conjunto $\{\zeta_5^{2^3}, \zeta_5^{2^5}, \zeta_5^{2^4}, \zeta_5^{2^6}\} = \{\zeta_5^3, \zeta_5^2, \zeta_5, \zeta_5^4\}$ é linearmente independente. Agora, se $H = Gal(\mathbb{Q}(\zeta_5)/\mathbb{K})$, e como $[\mathbb{Q}(\zeta_5) : \mathbb{K}] = 2$, segue que $o(H) = 2$. Como $\{\overline{1}, \overline{4}\}$ é o único subgrupo de $\mathbb{Z}_5^*$ de ordem 2, segue que $H =< \sigma_4 >= \{\sigma_1, \sigma_4\}$. Sendo $\theta = Tr_{\mathbb{Q}(\zeta_5)/\mathbb{K}}(\zeta_5)$, obtemos que $\theta = \sigma_1(\zeta_5) + \sigma_4(\zeta_5) = \zeta_5 + \zeta_5^4$, e assim, pelo Teorema 2.6.2, temos que $\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^4)$. Portanto, pelo Teorema 2.6.3, o anel de inteiros algébricos $\mathbb{A}_{\mathbb{K}}$ de $\mathbb{K}$ é $\mathbb{Z}\sigma_2(\zeta_5 + \zeta_5^4) + \mathbb{Z}\sigma_4(\zeta_5 + \zeta_5^4) = \mathbb{Z}(\zeta_5^2 + \zeta_5^3) + \mathbb{Z}(\zeta_5 + \zeta_5^4)$.*

Um fato importante é que o Teorema 2.6.3 não se aplica para potências de primos, mesmo a extensão ciclotômica $\mathbb{Q}(\zeta_{p^r})$ sendo cíclica. Isto segue do fato que, dado um subcorpo $\mathbb{K}$ da extensão ciclotômica $\mathbb{Q}(\zeta_{p^r})$ tal que $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{K}] = r$ e $[\mathbb{K} : \mathbb{Q}] = s$, e σ_g gera o grupo $G = Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$, segue que o conjunto $\{\zeta_{p^r}^{g^{s+1}}, \ldots, \zeta_{p^r}^{g^{rs+1}}, \zeta_{p^r}^{g^{s+2}}, \ldots, \zeta_{p^r}^{g^{rs+2}}, \ldots, \zeta_{p^r}^{g^{s+s}}, \ldots, \zeta_{p^r}^{g^{rs+s}}\}$ não é linearmente independente. Abaixo, daremos um exemplo mostrando este fato.

Exemplo 2.6.2 *Sejam $p = 3$, $r = 2$ e $\mathbb{K} \subset \mathbb{Q}(\zeta_{3^2}) = \mathbb{Q}(\zeta_9)$ tal que $[\mathbb{Q}(\zeta_9) : \mathbb{K}] = 2$ e $[\mathbb{K} : \mathbb{Q}] = 3$. Tem-se que $\mathbb{Q}(\zeta_9)$ é uma extensão ciclotômica cíclica, pois $G = Gal(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \simeq \mathbb{Z}_9^*$, e pelo Teorema 2.4.2, segue que $\mathbb{Z}_9^*$ é cíclico. Se $\sigma_2 \in G$, então $o(\sigma_2) = 6$, e deste modo $< \sigma_2 >= G$, pois $o(G) = 6$. Agora, tem-se que o conjunto $\{\zeta_9^{2^4}, \zeta_9^{2^7}, \zeta_9^{2^5}, \zeta_9^{2^8}, \zeta_9^{2^6}, \zeta_9^{2^9}\} = \{\zeta_9^7, \zeta_9^2, \zeta_9^5, \zeta_9^4, \zeta_9, \zeta_9^8\}$ não é linearmente independente, uma vez que, como o polinômio ciclotômico $p(x)$ de $\mathbb{Q}(\zeta_9)$ é dado por $p(x) = x^6 + x^3 + 1$, segue que $\zeta_9^6 + \zeta_9^3 + 1 = 0$, e assim $\zeta_9^3 = -1 - \zeta_9^6$. Deste modo, $\zeta_9^4 = -\zeta_9 - \zeta_9^7$ e $\zeta_9^5 = -\zeta_9^2 - \zeta_9^8$, ou seja, os elementos ζ_9^4 e ζ_9^5 se escrevem como combinação linear de elementos de $\{\zeta_9^7, \zeta_9^2, \zeta_9^5, \zeta_9^4, \zeta_9, \zeta_9^8\}$. Assim, o conjunto $\{\zeta_9^7, \zeta_9^2, \zeta_9^5, \zeta_9^4, \zeta_9, \zeta_9^8\}$ não é linearmente independente, e portanto o Teorema 2.6.3, não se aplica.*

2.7 Conclusão

Neste capítulo, tínhamos como objetivo mostrar quando o grupo $\mathbb{Z}_n^*$ é cíclico, pois o grupo de Galois de uma extensão ciclotômica é isomorfo ao grupo $\mathbb{Z}_n^*$. Agora, como todo corpo abeliano está contido em uma extensão ciclotômica, segue que os estudos dos corpos abelianos é equivalente ao estudo dos subcorpos de corpos ciclotômicos. Mas, uma das grandes dificuldades nossa, é determinar a cara destes subcorpos, assim, como o seu anel de inteiros. Assim, sabendo quando uma extensão ciclotômica é cíclica, vimos um método de como determinar a cara destes subcorpos, quando estes subcorpos estiverem contidos em corpos ciclotômicos da forma $\mathbb{Q}(\zeta_p)$, com p primo. Além disso, vimos que este mesmo método, não se aplica quando consideramos o corpo ciclotômico da forma $\mathbb{Q}(\zeta_{p^r})$, com p primo e r um inteiro maior que 1, mesmo esta extensão ciclotômica sendo cíclica. Com isto, uma das perspectivas para futuros, é encontrar métodos que ajudem a resolver este problema.

Capítulo 3

Lema de Kummer e Reticulados Algébricos

3.1 Introdução

Este capítulo representa a parte central deste trabalho, pois nele apresentamos métodos que nos ajudam a decompor os ideais primos em uma determinada extensão e apresentamos os reticulados e suas respectivas densidades de centro. Assim, na Seção 3.2, apresentamos a decomposição de um ideal em uma certa extensão verificando que, quando o ideal pertence a um anel de Dedekind, este ideal se decompõe unicamente em ideais primos. Por fim demonstramos o Lema de Kummer e apresentamos exemplos da decomposição de um ideal em uma extensão. Na Seção 3.3, definimos reticulados e empacotamentos esféricos. Já na Seção 3.4, apresentamos o método de Minkowiski que nos fornece um método de gerar reticulados via ideais dos anéis de inteiros algébricos de um corpo de números.

3.2 Decomposição de Ideais Primos em uma Extensão

Nesta seção, apresentamos a decomposição de ideais primos em uma extensão juntamente com suas principais propriedades. Um dos principais resultados desta seção é o Lema de Kummer.

Dados $A \subset B$ anéis e $\mathfrak{a}$ um ideal de A, denotamos por $\mathfrak{a}B$, o ideal de B formado pelos elementos da forma $\sum_{i=1}^{n} x_i y_i$, onde $x_i \in \mathfrak{a}$ e $y_i \in B$, para $i = 1, 2, \ldots, n$. Além disso, consideramos $\mathbb{K} \subset \mathbb{L}$ corpos de números, onde $[\mathbb{L} : \mathbb{K}] = n$.

Lema 3.2.1 *([1], p.47) Sejam $A \subset B$ anéis. Se $\mathfrak{p}$ é um ideal primo de B, então $A \cap \mathfrak{p}$ é um ideal primo de A.*

Demonstração: Consideremos a inclusão $i : A \to B$, a projeção canônica $h : B \to B/\mathfrak{p}$ e a composição $f = h \circ i$. O núcleo de f é $A \cap \mathfrak{p}$ e portanto $(A/(A \cap \mathfrak{p})) \simeq f(A) \subset B/\mathfrak{p}$. Desse modo, $A/(A \cap \mathfrak{p})$ é um domínio, e assim $A \cap \mathfrak{p}$ é um ideal primo de A. □

Lema 3.2.2 *([1], p.48) Se um ideal primo $\mathfrak{p}$ de um anel A contém um produto $\mathfrak{a}_1 \ldots \mathfrak{a}_n$ de ideais de A, então $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$.*

Demonstração: Se $\mathfrak{a}_i \nsubseteq \mathfrak{p}$, para $i = 1, \ldots, n$, então, para $i = 1, \ldots, n$, existe um elemento $\alpha_j \in \mathfrak{a}_i - \mathfrak{p}$. Assim, $\alpha_1 \ldots \alpha_n$ não pertence a $\mathfrak{p}$, pois $\mathfrak{p}$ é um ideal primo, e se $\alpha_1 \ldots \alpha_n \in \mathfrak{a}_1 \ldots \mathfrak{a}_n \subset \mathfrak{p}$, então α_i a pertence $\mathfrak{p}$, para $i = 1, \ldots, n$, o que é um absurdo. Portanto, $\mathfrak{a}_i \subset \mathfrak{p}$, para algum $i = 1, 2, \ldots, n$. □

Lema 3.2.3 *([1], p.48) Todo ideal não nulo de um anel A de Dedekind contém um produto de ideais primos não nulos de A.*

Demonstração: Seja F o conjunto de todos os ideais não nulos de A que não contém um produto de ideais primos não nulos de A. Se $F \neq \emptyset$, então, como A é Noetheriano, segue que F tem um elemento maximal $\mathfrak{m}$, onde $\mathfrak{m}$ não é primo e

$\mathfrak{m} \neq A$. Como $\mathfrak{m}$ não é um ideal primo, segue que existem $x, y \in A - \mathfrak{m}$ tal que $xy \in \mathfrak{m}$. Os ideais $\mathfrak{m}+xA$ e $\mathfrak{m}+yA$ contêm $\mathfrak{m}$, mas como $\mathfrak{m}$ é maximal, segue que esses ideais não estão em F. Assim, existem ideais primos não nulos $\mathfrak{p}_1 \dots \mathfrak{p}_s$ e $\mathfrak{q}_1 \dots \mathfrak{q}_t$ tais que $\mathfrak{p}_1 \dots \mathfrak{p}_s \subset \mathfrak{m}+xA$ e $\mathfrak{q}_1 \dots \mathfrak{q}_t \subset \mathfrak{m}+yA$. Como $\mathfrak{m} = \mathfrak{m}+xyA = (\mathfrak{m}+xA)(\mathfrak{m}+yA)$, segue que $\mathfrak{p}_1 \dots \mathfrak{p}_s\mathfrak{q}_1 \dots \mathfrak{q}_t \subset \mathfrak{m}$, o que é um absurdo, pois $\mathfrak{m} \in F$. □

Teorema 3.2.1 *([1], p.50) Se A é um anel de Dedekind e $\mathfrak{a}$ é um ideal não nulo de A, então existem ideais primos não nulos $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ de A e inteiros positivos $e_1, \dots, e_g$ tal que $\mathfrak{a} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, e esta expressão é única.*

Demonstração: Pelo Lema 3.2.3, segue que existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_s$, não nulos, tal que $\mathfrak{p}_1 \dots \mathfrak{p}_s \subset \mathfrak{a}$. Provemos que $\mathfrak{a}$ é um produto de ideais primos por indução sobre s. Assim, se $s = 1$, obtemos que $\mathfrak{p}_1 \subset \mathfrak{a}$. Agora, como $\mathfrak{p}_1$ é maximal, pois A é um anel de Dedekind, segue que $\mathfrak{p}_1 = \mathfrak{a}$. Agora, por hipótese de indução, supomos que todo ideal de A que contém um produto de $s-1$ ideais primos não nulos de A é um produto de ideais primos de A. Assim, como $\mathfrak{p}_1 \dots \mathfrak{p}_s \subset \mathfrak{a}$ e como A é Dedekind, segue que $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{m}$ de A. Seja $\mathfrak{m}^{-1}$ o ideal fracionário inverso de $\mathfrak{m}$. Como $\mathfrak{p}_1 \dots \mathfrak{p}_s \subset \mathfrak{a} \subset \mathfrak{m}$, segue pelo Lema 3.2.2, que $\mathfrak{m}$ contém um dos $\mathfrak{p}_i's$, digamos $\mathfrak{p}_s \subset \mathfrak{m}$. Como $\mathfrak{p}_s$ é maximal, segue que $\mathfrak{p}_s = \mathfrak{m}$. Assim, $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_{s-1} \subset \mathfrak{a}\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = A$. Por hipótese de indução obtemos que $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_{s-1}$ e portanto $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_{s-1}\mathfrak{p}_s$, como queríamos. Agora, para a unicidade, suponhamos que $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ são ideais primos não nulos de A tal que, $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$. Agora, como $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{q}_1$, segue pelo Lema 3.2.2, que $\mathfrak{q}_1$ contém um dos $\mathfrak{p}_i$, para $i = 1, 2, \dots, r$, e sem perda de generalidade, podemos supor que $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$. Como $\mathfrak{q}_1$ é maximal e $\mathfrak{p}_1 \neq A$ segue que $\mathfrak{p}_1 = \mathfrak{q}_1$. Portanto, $\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$. De modo análogo, segue que $r = s$ e $\mathfrak{p}_i = \mathfrak{q}_i$, para $i = 2, 3, \dots, r$. □

Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações e $\mathbb{A}_{\mathbb{K}}$ o anel de inteiros algébricos. Pela Proposição 1.7.3 segue que $\mathbb{A}_{\mathbb{K}}$ é um anel de Dedekind, e pelo Teorema 3.2.1, segue que todo ideal não nulo de $\mathbb{A}_{\mathbb{K}}$ pode ser fatorado de modo único como um produtos de ideais primos não nulos de $\mathbb{A}_{\mathbb{K}}$.

Definição 3.2.1 *Se* $\mathfrak{p} = A \cap \mathfrak{q}$*, dizemos que* $\mathfrak{q}$ *está* ***acima*** *de* $\mathfrak{p}$*.*

Proposição 3.2.1 *([1], p.71) Se* $\mathfrak{p}$ *é um ideal primo, não nulo, de* $\mathbb{A}_{\mathbb{K}}$ *e* $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$ *é a decomposição do ideal* $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$*, em ideais primos de* $\mathbb{A}_{\mathbb{L}}$*, então os ideias* $\mathfrak{p}_i's$ *são os únicos ideais primos de* $\mathbb{A}_{\mathbb{L}}$*, cuja interseção com* $\mathbb{A}_{\mathbb{K}}$ *coincide com* $\mathfrak{p}$*.*

Demonstração: Para cada $i = 1, \ldots, g$, tem-se que $\mathfrak{p} \subseteq \mathfrak{p}\mathbb{A}_{\mathbb{L}} \subseteq \mathfrak{q}_i$. Assim, pelo Lema 3.2.1, segue que $\mathfrak{q}_i \cap \mathbb{A}_{\mathbb{K}}$, para $i = 1, 2, \ldots, g$, é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ que contém $\mathfrak{p}$. Como $\mathfrak{p}$ é maximal e $\mathfrak{q}_i \cap \mathbb{A}_{\mathbb{K}} \neq \mathbb{A}_{\mathbb{K}}$, segue que $\mathfrak{p} = \mathfrak{q}_i \cap \mathbb{A}_{\mathbb{K}}$, para $i = 1, 2, \ldots, g$. Assim, se $\mathfrak{b}$ é um ideal primo de $\mathbb{A}_{\mathbb{L}}$, tal que $\mathfrak{p} = \mathfrak{b} \cap \mathbb{A}_{\mathbb{K}}$. Assim $\mathfrak{b} = \mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, e deste modo, pelo Lema 3.2.2 tem-se que $\mathfrak{q}_i \subseteq \mathfrak{b}$, para algum i. Como $\mathfrak{q}_i$ é maximal, segue que $\mathfrak{b} = \mathfrak{q}_i$. □

Sejam $\mathfrak{p} \subset \mathbb{A}_{\mathbb{K}}$ um ideal primo e $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$ a decomposição de $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ em ideais primos de $\mathbb{A}_{\mathbb{L}}$. O número g é chamado de **número de decomposição** de $\mathfrak{p}$ na extensão $\mathbb{L}/\mathbb{K}$. Os expoentes e_i ou $e(\mathfrak{q}_i, \mathfrak{p})$, para $i = 1, 2, \ldots, g$, são chamados de **índice de ramificação** de $\mathfrak{q}_i$ sobre $\mathbb{A}_{\mathbb{K}}$. Quando $e_i > 1$, para algum $i = 1, 2, \ldots, g$, dizemos que $\mathfrak{p}$ se **ramifica** em $\mathbb{L}$.

Pelo Lema 3.2.1, vemos que $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ pode ser visto como um subcorpo de $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}_i$, para $i = 1, 2, \ldots, g$, uma vez que, como $\mathbb{A}_{\mathbb{K}} \subset \mathbb{A}_{\mathbb{L}}$, tem-se que a inclusão $\mathbb{A}_{\mathbb{K}} \subset \mathbb{A}_{\mathbb{L}}$ induz um homomorfismo de anés $\mathbb{A}_{\mathbb{K}} \to \mathbb{A}_{\mathbb{L}}/\mathfrak{p}_i$, e como o núcleo é $\mathbb{A}_{\mathbb{K}} \cap \mathfrak{q}_i = \mathfrak{p}$, obtém-se a imersão $\mathbb{A}_{\mathbb{K}}/\mathfrak{p} \to \mathbb{A}_{\mathbb{L}}/\mathfrak{q}_i$. Os corpos $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ e $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}_i$, para $i = 1, 2, \ldots, g$, são chamados de **corpos residuais** associados a $\mathfrak{p}$ e $\mathfrak{q}_i$. Indicamos por f_i ou $f(\mathfrak{q}_i, \mathfrak{p})$ a **dimensão** $[\mathbb{A}_{\mathbb{L}}/\mathfrak{q}_i : \mathbb{A}_{\mathbb{K}}/\mathfrak{p}]$ e chamamos de **grau residual** de $\mathfrak{q}_i$ sobre $\mathbb{A}_{\mathbb{K}}$, para $i = 1, 2, \ldots, g$.

Teorema 3.2.2 *([1], p.71) Sejam* $\mathbb{K} \subset \mathbb{L}$ *corpos de números tal que* $[\mathbb{L} : \mathbb{K}] = n$*, e* $\mathbb{A}_{\mathbb{K}}$ *e* $\mathbb{A}_{\mathbb{L}}$ *seus respectivos anéis de inteiros algébricos. Se* $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ *são os ideais primos de* $\mathbb{A}_{\mathbb{L}}$ *acima de um ideal primo* $\mathfrak{p}$ *de* $\mathbb{A}_K$*, então*

$$\sum_{i=1}^{g} e_i f_i = [\mathbb{A}_L/\mathfrak{p}\mathbb{A}_{\mathbb{L}} : \mathbb{A}_{\mathbb{K}}/\mathfrak{p}] = n,$$

onde $e_1, \ldots, e_g$ *e* $f_1, \ldots, f_g$ *são os índices de ramificações e os graus residuais, respectivamente.*

Definição 3.2.2 *Sejam* $\mathbb{K} \subset \mathbb{L}$ *corpos de números tal que* $[\mathbb{L} : \mathbb{K}] = n$, $\mathbb{A}_{\mathbb{K}}$ *e* $\mathbb{A}_{\mathbb{L}}$ *seus respectivos anéis de inteiros algébricos. Dizemos que um ideal* $\mathfrak{p}$ *de* $\mathbb{A}_{\mathbb{K}}$ *é,*

(a) ***totalmente decomposto*** *em* $\mathbb{L}$*, se* $g = n$ *e assim* $e_i = f_i = 1$ *para todo* $i = 1, 2, \ldots, g$*,*

(b) ***inerte*** *em* $\mathbb{L}$*, se* $g = 1$*,* $e_1 = 1$ *e assim* $f_1 = n$*,*

(c) ***totalmente ramificado*** *em* $\mathbb{L}$*, se* $g = 1$ *e consequentemente* $f_1 = 1$ *e* $e_1 = n$*,*

(d) ***ramificado*** *em* $\mathbb{L}$ *se existir um ideal primo* $\mathfrak{q}_i$ *de* $\mathbb{A}_{\mathbb{L}}$ *que esta acima de* $\mathfrak{p}$ *tal que* $e_i > 1$ *para algum* $i = 1, 2, \ldots, g$*.*

Teorema 3.2.3 *([1], p.74) Seja* $\mathbb{K}$ *um corpo de números. Uma condição necessária e suficiente para que um ideal primo* $p\mathbb{Z}$ *de* $\mathbb{Z}$ *se ramifique em* $\mathbb{A}_{\mathbb{K}}$ *é que* p *divida* $D_{\mathbb{K}}$*.*

Proposição 3.2.2 *([12], p.84) Se* $\mathfrak{p}$ *é um ideal primo não nulo de* $\mathbb{A}_{\mathbb{K}}$*, então* $N(\mathfrak{p}) = p^f$*, onde* f *é o grau de inércia de* $\mathfrak{p}$*.*

Teorema 3.2.4 (Lema de Kummer) *([2], p.186) Sejam* $\mathbb{K}$ *um corpo de números de grau* n*,* $\mathbb{A}_{\mathbb{K}}$ *o seu anel de inteiros algébricos e* $\theta \in \mathbb{A}_{\mathbb{K}}$ *tal que* $\mathbb{K} = \mathbb{Q}(\theta)$*. Sejam* p *um número primo tal que* p *não divide* $[\mathbb{A}_{\mathbb{K}} : \mathbb{Z}[\theta]]$ *e* $p(x)$ *o polinômio minimal de* θ *sobre* $\mathbb{Z}[x]$*. Se* $\overline{p(x)} = \overline{p_1}(x)^{e_1}\overline{p_2}(x)^{e_2} \ldots \overline{p_g}(x)^{e_g}$ *é a fatoração do polinômio minimal* $p(x)$ *como o produto de polinômios irredutíveis distintos sobre* $\mathbb{Z}_p[x]$*, então existem ideias primos distintos* $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_g$ *de* $\mathbb{A}_{\mathbb{K}}$ *acima de* $p\mathbb{Z}$*, no qual* $p\mathbb{Z}$ *decompõe-se de modo único da forma*

$$p\mathbb{A}_{\mathbb{K}} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_g^{e_g},$$

onde $\mathfrak{q}_i = (p, p_i(\theta)) = p\mathbb{A}_{\mathbb{K}} + p_i(\theta)\mathbb{A}_{\mathbb{K}}$ *e* $[\mathbb{A}_{\mathbb{K}}/\mathfrak{q}_i : \mathbb{Z}/p\mathbb{Z}] = \partial p_i(x) = f_i$*, onde* $\partial p_i(x)$ *denota o grau de* $p_i(x)$*, para* $i = 1, 2, \ldots, g$*.*

Demonstração: Considere a aplicação

$$\phi_j : \mathbb{Z}[\theta] \to \mathbb{Z}_p[\overline{\theta_j}],$$

para $j = 1, \ldots, g$, no qual consideremos $\mathfrak{q}_j = Ker(\phi_j)$, sendo $\overline{\theta_j}$ uma raiz de $\overline{p_j}(x)$. Mostremos que $\mathfrak{q}_j = p\mathbb{A}_\mathbb{K} + p_j(\theta)\mathbb{A}_\mathbb{K}$. Tem-se que $p\mathbb{A}_\mathbb{K} + p_j(\theta)\mathbb{A}_\mathbb{K} \subseteq \mathfrak{q}_j$, para $j = 1, \ldots, g$, pois se $x \in p\mathbb{A}_\mathbb{K} + p_j(\theta)\mathbb{A}_\mathbb{K}$, então $x = py + p_j(\theta)w$, onde $y, w \in \mathbb{A}_\mathbb{K}$. Assim, $\phi_j(x) = \overline{py} + \overline{p_j}(\overline{\theta_j})\overline{w} = \overline{0}$, pois $\overline{p} = \overline{0}$ e $\overline{\theta_j}$ é raiz de $\overline{p_j}$. Portanto $x \in Ker(\phi_j) = \mathfrak{q}_j$. Por outro lado, se $\alpha \in \mathfrak{q}_j$, então $\alpha = g(\theta)$, para algum $g(x) \in \mathbb{Z}[\theta]$. Como $\overline{g}(\overline{\theta_j}) = p_j(g(\theta)) = 0$ e $\overline{p_j}$ é o polinômio minimal de $\overline{\theta_j}$ sobre $\mathbb{Z}_p[x]$, segue que existe $h(x) \in \mathbb{Z}[x]$ tal que $\overline{g}(x) = \overline{p_j}(x)\overline{h}(x)$. Assim, tem-se que $g(x) - p_j(x)h(x) \in p\mathbb{Z}[x]$ e consequentemente

$$\alpha = (g(\theta) - p_j(\theta)h(\theta)) + p_j(\theta)h(\theta) = (g - p_jh)(\theta) + p_j(\theta)h(\theta) \in p\mathbb{A}_\mathbb{K} + p_j(\theta)\mathbb{A}_\mathbb{K}.$$

Assim, $\mathfrak{q}_j = p\mathbb{A}_\mathbb{K} + p_j(\theta)\mathbb{A}_\mathbb{K}$, para $j = 1, 2, \ldots, g$. Agora mostraremos que $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ são os únicos ideias primos de $\mathbb{A}_\mathbb{K}$, que estão acima de $p\mathbb{Z}$. Tem-se que $\mathfrak{q}_1^{e_1}, \ldots, \mathfrak{q}_g^{e_g} \subseteq p\mathfrak{a}_\mathbb{K}$, pois, para quaisquer ideais, $\mathfrak{a}, \mathfrak{m}, \mathfrak{m}_1 \in \mathbb{A}_\mathbb{K}$, tem-se que $(\mathfrak{a}+\mathfrak{m})(\mathfrak{a}+\mathfrak{m}_1) \subseteq \mathfrak{a}+\mathfrak{m}\mathfrak{m}_1$, assim $\mathfrak{q}_1^{e_1}, \ldots, \mathfrak{q}_g^{e_g} \subseteq p\mathbb{A}_\mathbb{K} + (p_1(\theta)^{e_1}p_2(\theta)^{e_2} \ldots p_g(\theta)^{e_g})\mathbb{A}_\mathbb{K}$. Agora, como por hipótese $\overline{p}(x) = \overline{p_1}(x)^{e_1} \ldots \overline{p_g}(x)^{e_g}$, segue que $\overline{p}(x) - (\overline{p_1}(x)^{e_1}p_2(\theta)^{e_2} \ldots \overline{p_g}(x)^{e_g}) = \overline{0}$. Logo, $p(x) - p_1(x)^{e_1} \ldots p_g(x)^{e_g} \in p\mathbb{Z}[x]$, e como $p(\theta) = 0$, segue que

$$p(\theta) - p_1(\theta)^{e_1} \ldots p_g(\theta)^{e_g} = p_1(\theta)^{e_1} \ldots p_g(\theta)^{e_g} \in p\mathbb{A}_\mathbb{K}.$$

Assim, tem-se que $\mathfrak{q}_1^{e_1}, \ldots, q_g^{e_g} \subseteq p\mathfrak{a}_\mathbb{K}$. Notemos que não existe um outro ideal primo $\mathfrak{b}$ de $\mathbb{A}_\mathbb{K}$ que divide $p\mathbb{A}_\mathbb{K}$. Assim, $\mathfrak{q}_1, \ldots, q_g$ são os únicos ideias primos de $\mathbb{A}_\mathbb{K}$, que estão acima de $p\mathbb{Z}$, portanto $p\mathbb{A}_\mathbb{K} = \prod_{j=1}^{g} \mathfrak{q}_j^{e(\mathfrak{q}_j, p\mathbb{Z})}$. Note que $e(\mathfrak{q}_j, p\mathbb{Z}) \leq e_j$, para todo $j = 1, \ldots, g$, assim pelo Teorema 3.2.2, tem-se que

$$n = \sum_{j=1}^{g} e(\mathfrak{q}_j, p\mathbb{Z})f(\mathfrak{q}_j, p\mathbb{Z}) = \sum_{j=1}^{g} e(\mathfrak{q}_j, p\mathbb{Z})\partial(p_j) \leq \sum_{j=1}^{g} e_j\partial(p_j) = \partial(p) = n.$$

Portanto, $e(\mathfrak{q}_j, p\mathbb{Z}) = e_j$, para $j = 1, \ldots, g$. □

Exemplo 3.2.1 *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{21})$ e $\mathbb{A}_\mathbb{K} = \mathbb{Z}[\zeta_{21}]$ o seu anel de inteiros algébricos. O polinômio minimal de ζ_{21} sobre $\mathbb{Q}$ é*

$$f(x) = 1 - x + x^3 - x^4 + x^6 - x^8 + x^9 - x^{11} + x^{12}.$$

Agora vamos obter as fatorações de $3\mathbb{A}_{\mathbb{K}}$ *e* $7\mathbb{A}_{\mathbb{K}}$ *usando o Lema de Kummer. Para* $3\mathbb{A}_{\mathbb{K}}$ *tem-se que* $f(x) \equiv p_1(x)^2 (mod\, 3\mathbb{Z}[x])$*, onde* $p_1(x) = 1+x+x^2+x^3+x^4+x^5+x^6$*. Assim, obtemos que* $g = 1$*,* $e_1 = 2$ *e* $f_1(x) = \partial(p_1(x)) = 6$*. Consequentemente, pelo Lema de Kummer, segue que* $\mathfrak{p}_1 = (3, p_1(\zeta_{21})) = 3\mathbb{A}_{\mathbb{K}} + p_1(\zeta_{21})\mathbb{A}_{\mathbb{K}}$ *é o único ideal primo acima de* $3\mathbb{Z}$ *e* $3\mathbb{A}_{\mathbb{K}} = \mathfrak{p}_1^2$*. Observe que* $3\mathbb{A}_{\mathbb{K}}$ *se ramifica em* $\mathbb{K}$*, pois* $e_1 > 1$*, mas não é totalmente ramificado. Para* $7\mathbb{A}_{\mathbb{K}}$ *tem-se que* $f(x) \equiv q_1(x)^6 q_2(x)^6 (mod\, 7\mathbb{Z}[x])$*, onde* $q_1(x) = 3 + x$ *e* $q_2(x) = 5 + x$*. Assim, obtemos que* $g = 2$*,* $e_1 = e_2 = 6$*,* $f_1(x) = \partial(q_1(x)) = 6$ *e* $f_2(x) = \partial(q_2(x)) = 6$*. Assim, pelo Lema de Kummer, segue que* $\mathfrak{q}_1 = (7, q_1(\zeta_{21})) = 7\mathbb{A}_{\mathbb{K}} + q_1(\zeta_{21})\mathbb{A}_{\mathbb{K}}$ *e* $\mathfrak{q}_2 = (7, q_2(\zeta_{21})) = 7\mathbb{A}_{\mathbb{K}} + q_2(\zeta_{21})\mathbb{A}_{\mathbb{K}}$*. Logo* $7\mathbb{A}_{\mathbb{K}} = \mathfrak{q}_1^6.\mathfrak{q}_2^6$*, e deste modo* $7\mathbb{A}_{\mathbb{K}}$ *se ramifica em* $\mathbb{K}$*.*

Sejam $\mathbb{K}$ um corpo de números com grupo de Galois cíclico, $\mathbb{L}$ uma extensão galoisiana de $\mathbb{K}$, com grupo de Galois $G = Gal(\mathbb{L}/\mathbb{K})$, e $\mathbb{A}_{\mathbb{K}}$ e $\mathbb{A}_{\mathbb{L}}$ os anéis de inteiros algébricos de $\mathbb{K}$ e $\mathbb{L}$, respectivamente.

Definição 3.2.3 *Sejam* $\mathfrak{q}, \mathfrak{q}'$ *dois ideais de* $\mathbb{A}_{\mathbb{L}}$*. Dizemos que* $\mathfrak{q}, \mathfrak{q}'$ *são* $\mathbb{K}$***-conjugados*** *se existir* $\sigma \in G$ *tal que* $\sigma(\mathfrak{q}) = \mathfrak{q}'$*. Quando,* $\mathbb{K} = \mathbb{Q}$*, diremos apenas que são* ***conjugados****.*

Lema 3.2.4 *([1], p.89) Se* A *é um anel e* $\mathfrak{b}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *são ideais primos de* A *tal que* $\mathfrak{b}$ *não está contido em* $\mathfrak{p}_i$*, para todo* $i = 1, \ldots, r$*, então existe um elemento* $b \in \mathfrak{b}$ *tal que* b *não pertence a* $\mathfrak{p}_i$*, para todo* $i = 1, \ldots, r$*.*

Demonstração: Sem perda de generalidade podemos considerar o caso em que $\mathfrak{p}_j$ não está contido em $\mathfrak{p}_i$, para $i = 1, 2, \ldots, r$, $i \neq j$. Sejam $x_{ij} \in \mathfrak{p}_j - \mathfrak{p}_i$, com $i \neq j$, $1 \leq i, j \leq r$, e $a_i \in \mathfrak{b} - \mathfrak{p}_i$. Se $\mathfrak{b}_i = a_i \prod_{i \neq j} x_{ij}$, então $b_i \in \mathfrak{b}$, $b_i \in A - \mathfrak{p}_i$ e $b_i \in \mathfrak{p}_j$, para $i \neq j$. Tomando $b = b_1 + \ldots + b_r$, tem-se que $b \in \mathfrak{b}$ e $b \equiv b_i (mod\, \mathfrak{p}_i)$. Assim, $b \in \mathfrak{b} - \bigcup_{i=1}^{r} \mathfrak{p}_i$ é o elemento desejado. □

Proposição 3.2.3 *([1], p.89) Se $\mathfrak{p}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$, então os ideais primos $\mathfrak{q}_i$, para $i = 1, 2, \ldots, g$, que estão acima de $\mathfrak{p}$, são dois a dois conjugados, têm o mesmo grau residual f e o mesmo índice de ramificação e. Portanto, $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \left(\prod_{i=1}^{g} \mathfrak{q}_i\right)^e$, e assim $n = efg$.*

Demonstração: Suponhamos que existam dois ideais primos $\mathfrak{q}$ e $\mathfrak{q}'$ acima de $\mathfrak{p}$ tal que $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$, para todo $\sigma \in G$. Como $\mathfrak{q}$ e $\mathfrak{q}'$ são maximais, suponhamos que $\mathfrak{q}$ não esteja contido em $\sigma(\mathfrak{q}')$, para todo $\sigma \in G$. Considere, agora, um elemento $\alpha \in \mathfrak{q} - \bigcup_{\sigma \in G} \sigma(\mathfrak{q}')$ como obtido no Lema 3.2.4. Como $\alpha \in \mathbb{A}_{\mathbb{K}}$, segue que $\sigma(\alpha) \in \mathbb{A}_{\mathbb{K}}$. Assim, $\prod_{\sigma \in G} \sigma(\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha)$ é um elemento de $\mathfrak{q}$, e consequentemente é um elemento de $\mathbb{A}_{\mathbb{K}} \cap \mathfrak{q}$. Por outro lado, tem-se que $\sigma(\alpha)$ não pertence a q', pois, caso contrário teríamos $\sigma^{-1}(\sigma(\alpha)) = \alpha \in \sigma^{-1}(\mathfrak{q}')$, contradizendo a hipótese feita sobre α. Desse modo, $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$ não pertence a $\mathfrak{q}'$, pois $\mathfrak{q}'$ é um ideal primo. Assim, $\mathfrak{p}$ não está contido em $\mathfrak{q}'$, o que é absurdo. □

Proposição 3.2.4 *([15], p.57) Se p é um número primo e $\mathbb{A}_{\mathbb{K}}$ é o anel de inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, então o ideal $p\mathbb{A}_{\mathbb{K}}$ é da forma $p\mathbb{A}_{\mathbb{K}} = (1 - \zeta_p)^{p-1}\mathbb{A}_{\mathbb{K}}$.*

Demonstração: Se $1 \leq k, j \leq p-1$, então existe um inteiro t, com $1 \leq t \leq p-1$, tal que $j \equiv kt (mod\, p)$. Assim,

$$1 - \zeta_p^j = 1 - (\zeta_p^k)^t = (1 - \zeta_p^k)(1 + \zeta_p^k + \ldots + (\zeta_p^k)^{t-1}),$$

e portanto, $(1-\zeta_p^k)|(1-\zeta_p^j)$. Analogamente, tem-se que $(1-\zeta_p^j)|(1-\zeta_p^k)$. Assim, $1-\zeta_p^j$ e $1-\zeta_p^k$ são associados em $\mathbb{A}_{\mathbb{K}}$. Pelo Lema 2.5.1, tem-se que $p = \prod_{j=1}^{p-1}(1-\zeta_p^j)$, e deste modo, segue que existe um elemento inversível β em $\mathbb{A}_{\mathbb{K}}$ tal que $p = (1-\zeta_p)^{p-1}\beta$. Assim, $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_p)^{p-1}\mathbb{A}_{\mathbb{K}}$ e $(1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$. Finalmente, segue pelo Teorema 3.2.2 que o grau residual de $(1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ sobre $\mathbb{Z}$ é 1. □

Proposição 3.2.5 *([15], p.58) Sejam p um número primo e r um inteiro maior que 1. Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ e $\mathbb{A}_{\mathbb{K}}$ é o anel de inteiros algébricos de $\mathbb{K}$, então o ideal $p\mathbb{A}_{\mathbb{K}}$ é da forma $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{(p-1)p^{r-1}}\mathbb{A}_{\mathbb{K}}$.*

Demonstração: Demonstração análoga a da Proposição 3.2.4. □

Sejam $\mathfrak{p} \subseteq \mathbb{A}_{\mathbb{K}}$ um ideal primo, $\mathfrak{q} \subseteq \mathbb{A}_{\mathbb{L}}$ um ideal primo tal que $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$ e os conjuntos

$$D = D(\mathfrak{q}) = \{\sigma \in G\,;\, \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

e

$$E = E(\mathfrak{q}) = \{\sigma \in G\,;\, \sigma(x) \equiv x\,(mod\,\mathfrak{q})\,, \text{para todo}\, x \in \mathbb{A}_{\mathbb{K}}\}.$$

Os conjuntos D e E são subgrupos de G. Além disso, tem-se que $E \subset D$ uma vez que se $\sigma \in E$ então, $\sigma(x) - x \in \mathfrak{q}$, para todo $x \in \mathbb{A}_{\mathbb{K}}$. Em particular, $\sigma(x) \equiv x\,(mod\,\mathfrak{q})$, para todo $x \in \mathfrak{q}$. Assim, $\sigma(x) \in \mathfrak{q}$, para todo $x \in \mathfrak{q}$, e portanto $\sigma(\mathfrak{q}) \subseteq \mathfrak{q}$. Finalmente, como $\mathfrak{q}$ é um ideal maximal, segue que $\sigma(\mathfrak{q})$ é um ideal maximal. Assim, $\sigma(\mathfrak{q}) = \mathfrak{q}$, e portanto, $E \subset D$.

Definição 3.2.4 *Os subgrupos D e E de G são chamados* ***grupo de decomposição e grupo de inércia*** *de $\mathfrak{q}$ com relação a $\mathfrak{p}$, respectivamente.*

3.3 Reticulados

O objetivo, desta seção, é apresentar os conceitos de reticulados e de empacotamentos esféricos. Além disso, nesta seção, apresentamos a densidade de centro dos reticulados, com o objetivo de encontrar o melhor empacotamento esférico. Por fim, apresentamos uma tabela de reticulados e suas respectivas densidades de centro.

Definição 3.3.1 *Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subset \mathbb{K}$ um anel e $\{v_1, \ldots, v_m\}$ vetores de V linearmente independentes sobre $\mathbb{K}$ com $m \leq n$. Chama-se* **reticulado** *com base $\beta = \{v_1, \ldots, v_m\}$ ao conjunto dos elementos de V da forma*

$$\left\{ x = \sum_{i=1}^{m} a_i v_i,\ \textit{com}\ a_i \in A\,,\ \textit{para}\ i = 1, 2, \ldots, m \right\},$$

que denotamos por $\mathcal{H}_\beta$.

Seja $\mathcal{H}_\beta$ um reticulado com base $\{v_1, \ldots, v_n\}$. Se $\{w_1, \ldots, w_n\}$ é um conjunto de elementos de $\mathcal{H}_\beta$, então existem a_{ij} em $\mathbb{Z}$ tal que $w_i = \sum_{j=1}^{n} a_{ij} v_j$, para $i, j = 1, 2, \ldots, n$. Uma condição necessária e suficiente para que $\{w_1, \ldots, w_n\}$ seja uma base de $\mathcal{H}_\beta$ é que $det(a_{ij})$ seja um elemento inversível de $\mathbb{Z}$.

Definição 3.3.2 *Seja $\mathcal{H}_\beta \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\beta = \{v_1, \ldots, v_n\}$. Definimos a* **região fundamental** *de $\mathcal{H}_\beta$, com relação a base $\{v_1, \ldots, v_n\}$, por*

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n \ : \ x = \sum_{i=1}^{n} \lambda_i v_i, \ \textit{onde } 0 \leq \lambda_i < 1 \textit{ para } i = 1, 2, \ldots, n \right\}.$$

Sejam $\mathcal{H}_\beta \subset \mathbb{R}^n$ um reticulado, onde $\beta = \{v_1, \ldots, v_n\}$ é uma base de $\mathcal{H}_\beta$, e $\mathcal{P}_\beta$ a região fundamental de $\mathcal{H}_\beta$. Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \ldots, n$, definimos o **volume da região fundamental** $\mathcal{P}_\beta$, como o módulo do determinante da seguinte matriz

$$B = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{pmatrix},$$

ou seja, $Vol(\mathcal{H}_\beta) = \mid det(B) \mid$. Além disso, definimos o volume do reticulado $\mathcal{H}_\beta \subseteq \mathbb{R}^n$, com base $\beta = \{v_1, \ldots, v_n\}$, como $Vol(\mathcal{H}_\beta) = Vol(\mathcal{P}_\beta)$.

Um **empacotamento esférico** é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Deste modo, um empacotamento esférico pode ser descrito indicando apenas o conjunto dos centros das esferas e o raio. A **densidade de empacotamento** de um reticulado é definido como sendo a proporção do espaço do $\mathbb{R}^n$ coberta pela união das esferas.

Nosso interesse está nos empacotamento associado a um reticulado $\mathcal{H}_\beta$ em que as esferas tenham raio máximo. Deste modo, para a determinação deste raio, observe que fixado $k > 0$, a interseção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado $\mathcal{H}_\beta$ é um conjunto finito. Assim, o número $\mathcal{H}_{\beta_{\min}} = \min\{|\lambda|; \lambda \in \mathcal{H}_\beta, \lambda \neq 0\}$ está bem definido e $(\mathcal{H}_{\beta_{\min}})^2$ é chamado de **norma mínima** do reticulado. Como

$\rho = \mathcal{H}_{\beta_{\min}}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de $\mathcal{H}_\beta$ e obter um empacotamento, segue que, estudar os empacotamentos esféricos equivale ao estudo dos reticulados.

Seja $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ. A **densidade de empacotamento** de $\mathcal{H}_\beta$ é igual a

$$\Delta(\mathcal{H}_\beta) = \frac{\textit{volume da esfera}}{\textit{volume da região fundamental}} = \frac{\mathcal{V}\text{ol}(\mathcal{B}(\rho))}{\mathcal{V}\text{ol}(\mathcal{H}_\beta)} = \frac{\mathcal{V}\text{ol}(\mathcal{B}(1))\rho^n}{\mathcal{V}\text{ol}(\mathcal{H}_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por

$$\delta(\mathcal{H}_\beta) = \frac{\rho^n}{\mathcal{V}\text{ol}(\mathcal{H}_\beta)}.$$

e um dos principais problemas é encontrar reticulados com maior densidade de centro.

A tabela abaixo, apresenta exemplos de reticulados encontrados na literatura em ([14]) com densidade de centro ótima (dimensão de 1 à 8), e reticulados com densidades de centro recordes, mas não se sabe se essas densidades são ótimas.

dimensão	densidade	reticulado
0	0	Λ_0
1	$1/2$	$\Lambda_1 \cong A_1 \cong \mathbb{Z}$
2	$1/(2\sqrt{3})$	$\Lambda_2 \cong A_2$
3	$1/4\sqrt{2}$	$\Lambda_3 \cong A_3 \cong D_3$
4	$1/8$	$\Lambda_4 \cong D_4$
5	$1/8\sqrt{2}$	$\Lambda_5 \cong D_5$
6	$1/8\sqrt{3}$	$\Lambda_6 \cong E_6$
7	$1/16$	$\Lambda_7 \cong E_7$
8	$1/16$	$\Lambda_8 \cong E_8$
9	$1/16\sqrt{2}$	Λ_9
10	$1/16\sqrt{3}$	Λ_{10}
11	$1/18\sqrt{3}$	$\mathbb{K}_{11}$
12	$1/27$	$\mathbb{K}_{12}$
13	$1/18\sqrt{3}$	$\mathbb{K}_{13}$
14	$1/16\sqrt{3}$	Λ_{14}
15	$1/16\sqrt{2}$	Λ_{15}
16	$1/16$	Λ_{16}
17	$1/16$	Λ_{17}
18	$1/8\sqrt{3}$	Λ_{18}
19	$1/8\sqrt{2}$	Λ_{19}
20	$1/8$	Λ_{20}
21	$1/4\sqrt{2}$	Λ_{21}
22	$1/2\sqrt{3}$	Λ_{22}
23	$1/2$	Λ_{23}
24	1	Λ_{24}
25	$1/\sqrt{2}$	Λ_{25}
26	$1/\sqrt{3}$	Λ_{26}, T_{26}

dimensão	densidade	reticulado
27	$1/\sqrt{3}$	B_{27}
28	$2/3$	B_{28}
29	$1/\sqrt{3}$	B_{29}
30	$3^{13.5}/2^{22}$	Q_{30}
31	$3^{15}/2^{23.5}$	Q_{31}
32	$3^{16}/2^{24}$	Q_{32}
33	$3^{16.5}/2^{25}$	Q_{33}
34	$3^{16.5}/2^{25}$	Q_{34}
35	$2\sqrt{2}$	B_{35}
36	$2^{18}/3^{10}$	Ks_{36}
37	$4/\sqrt{2}$	D_{37}
38	8	P_{48p}
39	$3^{16}/2^{20}\sqrt{14}$	P_{48p}
40	$3^{17}/2^{22.5}$	P_{48p}
41	$3^{17}/2^{21.5}$	P_{48p}
42	$3^{18}/2^{22}$	P_{48p}
43	$3^{19}/2^{22.5}$	P_{48p}
44	$3^{20/2^{23}}$	P_{48p}
45	$3^{21}/2^{23.5}$	P_{48p}
46	$3^{21.5}/2^{23}$	P_{48p}
47	$3^{23}/2^{24}$	P_{48p}
48	$3^{24}/2^{24}$	P_{48n},P_{48p},P_{48q}
54	215.88	MW_{54}
56	1.5^{28}	$L_{56.2}(M)$,$\overline{L}_{56.2}(M)$
64	3^{16}	Ne_{64}
80	$2^{40.14}$	MW_{80}
128	$2^{97.40}$	MW_{128}

3.4 Reticulados Algébricos

Nesta seção, descrevemos o método de Minkowki para a geração de reticulados via ideias de corpos de números. Deste modo, apresentamos algumas propriedades de monomorfismos de um corpo de números, onde introduzimos o homomorfismo de Minkowski. Por fim, apresentamos um resultado que permite calcular a densidade de centro dos reticulados algébricos.

Se $\mathbb{K}$ é um corpo de números de grau n, então existem $\mathbb{Q}$-monomorfismos distintos $\sigma_j : \mathbb{K} \to \mathbb{C}$, para $j = 1, 2, \ldots, n$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$ diz-se que σ_j é **real**, caso contrário, σ_j é dito **imaginário**, para $j = 1, 2, \ldots, n$. Se r_1 é a quantidade de índices j, tal que $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, então $n - r_1$ é um número par. Assim, podemos escrever $r_1 + 2r_2 = n$, onde $2r_2$ indica a quantidade de monomorfismos imaginários. Dizemos que $\mathbb{K}$ é um **corpo totalmente complexo** quando todos os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ forem complexos e $\mathbb{K}$ é dito um **corpo totalmente real** quando todos os $\mathbb{Q}$-monomorfismos são reais.

Definição 3.4.1 *Seja x um elemento de $\mathbb{K}$. O homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \rightharpoonup \mathbb{R}^n$ definido por*

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathfrak{R}\sigma_{r_1+1}(x), \mathfrak{F}\sigma_{r_1+1}(x), \ldots, \mathfrak{R}\sigma_{r_1+r_2}(x), \mathfrak{F}\sigma_{r_1+r_2}(x)),$$

é um homomorfismo injetivo de anéis, chamado ***homomorfismo canônico (ou Minkowski)****, onde as notações $\mathfrak{R}(x)$ e $\mathfrak{F}(x)$ representam as partes real e imaginária do número complexo x, respectivamente.*

Na próxima proposição, veremos que através do homomorfismo canônico, podemos gerar reticulados no $\mathbb{R}^n$, via ideais inteiros. Uma das vantagens deste método é a obtenção de uma expressão para o volume de tais reticulados.

Proposição 3.4.1 *([1], p.56) Seja $\mathbb{K}$ um corpo de números de grau n. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $(x_j)_{1 \leq j \leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$, cujo volume é*

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

Demonstração: Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$, com respeito a base canônica do $\mathbb{R}^n$, são dadas por

$$(\sigma_1(x_j),\ldots,\sigma_{r1}(x_j),\mathfrak{R}\sigma_{r_1+1}(x_j),\mathfrak{F}\sigma_{r_1+1}(x_j),\ldots,\mathfrak{R}\sigma_{r_1+r_2}(x_j),\mathfrak{F}\sigma_{r_1+r_2}(x_j)) \quad (3.1)$$

Seja D a matriz que tem a j-ésima coluna dada pela Equação (3.1), ou seja,

$$D=\begin{pmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \mathfrak{R}(\sigma_{r_1+1}(x_1)) & \ldots & \mathfrak{R}(\sigma_{r_1+1}(x_j)) & \ldots & \mathfrak{R}(\sigma_{r_1+1}(x_n)) \\ \mathfrak{F}(\sigma_{r_1+1}(x_1)) & \ldots & \mathfrak{F}(\sigma_{r_1+1}(x_j)) & \ldots & \mathfrak{F}(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \mathfrak{R}(\sigma_{r_1+r_2}(x_1)) & \ldots & \mathfrak{R}(\sigma_{r_1+r_2}(x_j)) & \ldots & \mathfrak{R}(\sigma_{r_1+r_2}(x_n)) \\ \mathfrak{F}(\sigma_{r_1+r_2}(x_1)) & \ldots & \mathfrak{F}(\sigma_{r_1+r_2}(x_j)) & \ldots & \mathfrak{F}(\sigma_{r_1+r_2}(x_n)) \end{pmatrix}.$$

Agora, fazendo uso das fórmulas $\mathfrak{R}(z)=\frac{1}{2}(z+\overline{z})$, $\mathfrak{F}(z)=\frac{1}{2i}(z-\overline{z})$, para z em $\mathbb{C}$, e de algumas operações elementares, como a adição da (r_1+2l)-ésima linha com a anterior e em seguida pela subtração da (r_1+2l-1)-ésima coluna com a posterior, onde $l=1,\ldots,r_2$, obtemos que

$$det(D)=\begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \mathfrak{R}(\sigma_{r_1+1}(x_1)) & \ldots & \mathfrak{R}(\sigma_{r_1+1}(x_j)) & \ldots & \mathfrak{R}(\sigma_{r_1+1}(x_n)) \\ \mathfrak{F}(\sigma_{r_1+1}(x_1)) & \ldots & \mathfrak{F}(\sigma_{r_1+1}(x_j)) & \ldots & \mathfrak{F}(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \mathfrak{R}(\sigma_{r_1+r_2}(x_1)) & \ldots & \mathfrak{R}(\sigma_{r_1+r_2}(x_j)) & \ldots & \mathfrak{R}(\sigma_{r_1+r_2}(x_n)) \\ \mathfrak{F}(\sigma_{r_1+r_2}(x_1)) & \ldots & \mathfrak{F}(\sigma_{r_1+r_2}(x_j)) & \ldots & \mathfrak{F}(\sigma_{r_1+r_2}(x_n)) \end{vmatrix} =$$

$\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2} det(D_1)$, onde D_1 é a matriz,

$$\begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{pmatrix}.$$

Assim, $det(D) = \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2} 2^{r_2} det(D_2)$, onde D_2 é matriz,

$$\begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{pmatrix}.$$

Assim, obtemos que $det(D)$ é,

$$(-1)^{r_2}\left(\frac{1}{2}\right)^{\frac{r_2}{2}}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_j)} & \dots & \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n) \\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$= \left(\frac{1}{2i}\right)^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix} = (2i)^{-r_2}det(\sigma_j(x_k)).$$

Logo, $\det(D) = (2i)^{-r_2}\det(\sigma_j(x_k))$, para $j,k = 1,\dots,n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue pela Proposição 1.5.5, que $\det(\sigma_j(x_k)) \neq 0$ e portanto, $\det(D) \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$. Como $\{x_1,\dots,x_n\}$ é uma $\mathbb{Z}$-base de M, segue que se $m \in M$, então $m = \sum_{j=1}^{n} a_j x_j$, onde $a_j \in \mathbb{Z}$, para $j = 1,\dots,n$. Assim, $\sigma_{\mathbb{K}}(m) = \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j)$, onde $a_j \in \mathbb{Z}$, para $j = 1,\dots,n$, consequentemente,

$$\sigma_{\mathbb{K}}(M) = \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j);\ a_j \in \mathbb{Z} \right\}$$

é um reticulado no $\mathbb{R}^n$, cujo volume é dado por

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

□

Proposição 3.4.2 *([1], p.57) Se $\mathbb{K}$ é um corpo de números de grau n, $D_{\mathbb{K}}$ o discriminante de $\mathbb{K}$, $\mathbb{A}_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$, $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$ e r_2 a metade do número de monomorfismo imaginários, então $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathfrak{a})$ são reticulados, cujos volumes são dados por, $Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}$, $Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))N(\mathfrak{a})$, respectivamente.*

Demonstração: Pelo Teorema 1.5.1, tem-se que $\mathfrak{a}$ e $\mathbb{A}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n. Assim, pela Proposição 3.4.1, segue que $\mathfrak{a}$ e $\mathbb{A}_{\mathbb{K}}$ são reticulados do $\mathbb{R}^n$, onde $Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}$, pois pela Proposição 1.5.5 tem-se que $D_{\mathbb{K}} = \det(\sigma_i(x_k))^2$, para $\{x_1, \ldots, x_n\}$ uma $\mathbb{Z}$-base de $\mathbb{A}_{\mathbb{K}}$. Para a segunda fórmula, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um subgrupo de $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ de índice $N(\mathfrak{a})$, uma vez que $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$ é isomorfo a $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})/\sigma_{\mathbb{K}}(\mathfrak{a})$. Além disso, como a região fundamental de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é a união disjunta de $N(\mathfrak{a})$ cópias de uma região fundamental de $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$, segue que $Vol(\sigma_{\mathbb{K}}(\mathbb{A}/\mathbb{K})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}$. Portanto $Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))N(\mathfrak{a})$. □

Exemplo 3.4.1 *Se $\mathbb{K} = \mathbb{Q}(\zeta_7)$, $\mathbb{A}_{\mathbb{K}}$ é o seu anel de inteiros algébricos, $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, dado por $\mathfrak{a} = (1-\zeta_7)\mathbb{A}_{\mathbb{K}}$, então $D_{\mathbb{K}} = -7^5$, $N(\mathfrak{a}) = 7$ e $r_2 = 3$. Assim, pela Proposição 3.4.2, obtemos que*

$$Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{7^2\sqrt{7}}{8} \quad e \quad Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{7^3\sqrt{3}}{8}.$$

Observação 3.4.1 *Seja $\mathbb{K}$ um corpo de números de grau n e $\mathbb{A}_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$. O reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$, onde $\mathfrak{a} \subseteq \mathbb{A}_{\mathbb{K}}$ é um ideal, será chamado neste trabalho de* ***reticulado algébrico****. Em consequência das Proposições 3.4.1 e 3.4.2, tem-se que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}((\mathfrak{a})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{a})))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})}. \tag{3.2}$$

Proposição 3.4.3 *([14], p.225) Se $\mathbb{K}$ é um corpo de números de grau n e $x \in \mathbb{K}$, então*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, \ \textit{se } \mathbb{K} \textit{ for totalmente real} \\ \frac{1}{2}, \ \textit{se } \mathbb{K} \textit{ for totalmente imaginário.} \end{cases} \tag{3.3}$$

Demonstração: Como $\sigma_{\mathbb{K}}(x) \in \mathbb{R}^n$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \ldots + (\sigma_{r_1}(x))^2 + \mathfrak{R}(\sigma_{r_1+1}(x))^2 + \mathfrak{F}(\sigma_{r_1+1}(x))^2 + \ldots + \\ + \mathfrak{R}(\sigma_{r_1+r_2}(x))^2 + \mathfrak{F}(\sigma_{r_1+r_2}(x))^2.$$

Observe que $\mathfrak{R}(\sigma_k(x))^2 + \mathfrak{F}(\sigma_k(x))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\overline{x})$, para $r_1+1 \leq k \leq r_1+r_2$. Com isso, obtemos que

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \ldots + (\sigma_{r_1}(x))^2 + (\sigma_{r_1+1}(x\overline{x})) + \ldots + (\sigma_{r_1+r_2}(x\overline{x})).$$

Agora, se $r_1 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x\overline{x})) + \ldots + (\sigma_{r_2}(x\overline{x})) = (\sigma_{r_2+1}(x\overline{x})) + \ldots + (\sigma_{r_2+r_2}(x\overline{x})),$$

pois sendo $\overline{\sigma}$ a conjugação complexa, vemos que $\sigma_{r_2+j}(x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(x\overline{x}) = \sigma_j(x\overline{x})$, para $j = 1, \ldots, r_2$. Portanto

$$2|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \ldots + \sigma_{r_2}(x\overline{x}) + \sigma_{r_2+1}(x\overline{x}) + \ldots + \sigma_{r_2+r_2}(x\overline{x}) = \\ = \sum_{i=1}^{n} \sigma_i(x\overline{x}),$$

e como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, para $i = 1, 2, \ldots, n$, concluímos que

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

Agora, se $r_2 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \ldots + \sigma_{r_1}(x\overline{x}),$$

pois $\sigma_i(x) = (\overline{\sigma} \circ \sigma_i)(x) = \sigma_i(\overline{x})$, para $i = 1, 2, \ldots, r_1$. Portanto,

$$|\sigma_{\mathbb{K}}(x)|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

o que prova a proposição. □

Observação 3.4.2 *Com base na Proposição 3.4.3, considerando* $\mathbb{K}$ *um corpo de números de grau* n *e* $\mathfrak{a}$ *um ideal não nulo de* $\mathbb{A}_{\mathbb{K}}$*, podemos escrever o raio de empacotamento do reticulado algébrico* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *como,*

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2}\min\{|\sigma_{\mathbb{K}}(x)|, x \in \mathfrak{a}, x \neq 0\} = \frac{1}{2}\min\left\{\sqrt{c_{\mathbb{K}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})}\ ,\ x \in \mathfrak{a},\ x \neq 0\right\}.$$

Assim, pela Observação 3.4.1, a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por:*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}, \tag{3.4}$$

onde, $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), x \in \mathfrak{a}, x \neq 0\}$.

3.5 Conclusão

Neste capítulo, apresentamos uma tabela de reticulados com as suas melhores densidade de centro em determinadas dimensões. Tem-se que até dimensão 8 é provado qual é a melhor densidade de centro para estes reticulados, mas para reticulados com dimensões acima de 8 temos qual é a maior densidade de centro, mas não se sabe se é a melhor. Assim, um dos grandes interesses sobre o estudo de reticulados algébricos, é de encontrar reticulados de dimensão 1 à 8 que possuam densidade de centro ótima, e de achar reticulados de dimensão acima de 8 que possuam densidade de centro melhor que as encontradas na literatura. Um dos métodos, que tem sido muito estudados, é o método descrito por Minkowski, que mostra que através dos ideais dos anéis de inteiros algébricos, podemos gerar reticulados via o homomorfismo de Minkowski. Assim, neste capítulo, vimos alguns resultados sobre fatoração de ideais, como, por exemplo, o Lema de Kummer, que permite decompor ideais. Uma das grandes dificuldades de determinar a densidade de centro destes reticulados gerado por ideais, é de calcular a função traço, assim, no próximo capítulo, daremos alguns resultados, que facilite o cálculo desta função.

Capítulo 4

Formas Quadráticas sobre Corpos Ciclotômicos

4.1 Introdução

No próximo capítulo apresentamos a construção de reticulados via corpos ciclotômicos. Primeiramente apresentamos resultados sobre formas quadráticas via corpos ciclotômicos, que serão útil na determinação da densidade de centro de um reticulado algébrico. Assim, na Seção 4.2, apresentamos resultados sobre formas quadráticas via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, com p primo. Na Seção 4.3, apresentamos as formas quadráticas sobre os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$, com p primo e r um inteiro maior ou igual à 1. Por fim, na Seção 4.4, apresentamos alguns fatos envolvendo o cálculo da função traço via os corpos ciclotômicos $\mathbb{Q}(\zeta_{pq})$, com p e q primos distintos. Além disso, apresentamos as formas quadráticas via os subcorpos de $\mathbb{Q}(\zeta_{pq})$.

4.2 Forma Quadrática Associada a $\mathbb{Q}(\zeta_p)$

Nesta seção, apresentamos alguns resultados sobre formas quadráticas via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um número primo, e também alguns fatos que

permitem minimizar a forma quadrática via esses corpos com $p > 2$.

Teorema 4.2.1 *([15], p.86) Se* $\mathbb{K} = \mathbb{Q}(\zeta_p)$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ *o anel de inteiros algébricos de* $\mathbb{K}$ *e* $\alpha = \sum_{i=0}^{p-2} a_i \zeta_p^i \in \mathbb{Z}[\zeta_p]$, *então*

$$Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0\leq i<j\leq p-2} (a_i - a_j)^2.$$

Demonstração: Como $\overline{\zeta_p} = \zeta_p^{-1}$ segue que $\overline{\alpha} = \sum_{i=0}^{p-2} a_i \zeta_p^{-i}$ e assim,

$$\alpha\overline{\alpha} = \left(\sum_{i=0}^{p-2} a_i\zeta_p^i\right)\left(\sum_{i=0}^{p-2} a_i\zeta_p^{-i}\right) = (a_0^2+\cdots+a_{p-2}^2)+(a_0a_1+a_1a_2+\cdots+a_{p-3}a_{p-2})(\zeta_p$$
$$+\zeta_p^{-1})+\cdots+(a_0a_{p-3}+a_1a_{p-2})(\zeta_p^{p-3}+\zeta_p^{-(p-3)})+a_0a_{p-2}(\zeta_p^{p-2}+\zeta_p^{-(p-2)}).$$

Por outro lado, fazendo $\alpha_i = \zeta_p^i + \zeta_p^{-i}$ e $A_i = a_0a_i + a_1a_{i+1} + \cdots + a_{p-2-i}a_{p-2}$, para $i = 0, 1, \ldots, p-3$, obtemos que $\alpha\overline{\alpha} = A_0 + A_1\alpha_1 + \cdots + A_{p-2}\alpha_{p-2}$. Pelo Lema 2.5.1, tem-se que $Tr_{K/\mathbb{Q}}(\zeta_p^j) = -1$, para $j = 1, \ldots, p-1$, e assim $Tr_{K/\mathbb{Q}}(\alpha_i) = -2$. Portanto,

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) &= (p-1)A_0 - 2(A_1 + A_2 + \cdots + A_{p-2}) = \\ &= (p-1)A_0 - 2(a_0a_1 + \cdots + a_{p-3}a_{p-2} + a_0a_2 + \cdots + a_{p-4}a_{p-2} + \cdots + \\ &+ a_0a_{p-3} + a_1a_{p-2} + a_0a_{p-2}). \end{aligned}$$

Assim,

$$Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i^2 + 2\sum_{0\leq i<j\leq p-2} a_ia_j\right],$$

e, portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i\right]^2. \tag{4.1}$$

Fazendo algumas operações no segundo membro da Equação (4.1), obtemos que

$$Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0\leq i<j\leq p-2} (a_i - a_j)^2, \tag{4.2}$$

o que prova o teorema. □

Note que, a Equação (4.2) é a definição da forma quadrática $Q_{p-1}(x)$ calculada em $x = (a_0, a_1, \cdots, a_{p-2})$. Quando não ocorrer problemas, usaremos Q em vez de Q_{p-1}.

Teorema 4.2.2 *([13], p.72) Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um subcorpo de $\mathbb{Q}(\zeta_p)$ com p primo, tal que $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}} = \theta$, e $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) =< \sigma_g >$, com $g \in \mathbb{Z}$. Se $y \in \mathbb{A}_{\mathbb{K}}$, então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{s} a_i^2 + r \sum_{1 \leq i < j \leq s} (a_i - a_j)^2 = Q_{r,s}(y),$$

com $y = a_1\sigma_g(\theta) + \ldots + a_s\sigma_g^s(\theta)$.

Demonstração: Como $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}$, segue que $\theta = \sum_{i=1}^{r} \sigma_g^{is}(\zeta_p) = \sum_{i=1}^{r} \zeta_p^{g^{is}}$. Deste modo, tem-se que $\sigma_g^i(\theta) = \sum_{j=1}^{r} \zeta_p^{g^{js+i}}$, para $i = 1, 2, \ldots, s$. Assim,

$$y = a_1(\zeta_p^{g^{s+1}} + \ldots + \zeta_p^{g^{rs+1}}) + a_2(\zeta_p^{g^{s+2}} + \ldots + \zeta_p^{g^{rs+2}}) + a_3(\zeta_p^{g^{s+3}} + \ldots + \zeta_p^{g^{rs+3}}) + \ldots +$$
$$+ a_s(\zeta_p^{g^{s+s}} + \ldots + \zeta_p^{g^{rs+s}}).$$

Pelo argumento usado no Lema 2.6.1, e pela definição de forma quadrática, podemos associar a y a $(p-1)$-upla $\underline{y} = (a_1, \ldots, a_1, a_2, \ldots, a_2, \ldots, a_s, \ldots, a_s)$, onde cada a_i, para $i = 1, 2, \ldots, s$, aparece r vezes. Assim, $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}) = Q_{p-1,1}(y)$, e deste modo

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}) = r\sum_{i=1}^{s} a_i^2 + \ r^2 \sum_{1 \leq i < j \leq s} (a_i - a_j)^2.$$

Agora, como $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}) = [\mathbb{Q}(\zeta_p) : \mathbb{K}]Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})$, segue que

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \frac{1}{r} Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}).$$

Portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{s} a_i^2 + r \sum_{1 \leq i < j \leq s} (a_i - a_j)^2 = Q_{r,s}(y),$$

o que prova o teorema. □

Proposição 4.2.1 *([8], p.41) Se $\mathfrak{p}$ é o ideal de $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ gerado por $1 - \zeta_p$, $\alpha \in \mathbb{Z}[\zeta_p]$ e $f(x) \in \mathbb{Z}[x]$ tal que $\alpha = f(\zeta_p)$, então*

$$\alpha \in \mathfrak{p} \Longleftrightarrow f(1) \equiv 0 (mod\, p).$$

Proposição 4.2.2 *([3], p.72) Se $p > 2$ então $Q(x) \geq 2p$, onde $x \in \mathfrak{p} = (1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ e $x \neq 0$. Além disso, $Q(x) = 2p$ para $x = 1 - \zeta_p$.*

Demonstração: Seja $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ um elemento de $\mathfrak{p}$ e supomos que $(a_0, \cdots, a_{p-2}) \in I_1 = \{(b_1, \cdots, b_n) \in \mathbb{Z}^n,\ |b_i| \leq 1\}$, para $i = 1, 2, \ldots, n$. Sejam r e s o número de $a_i's$ iguais a 1 e -1, respectivamente. Assim, o número de $a_i's$ nulos será $p-r-s-1$. Como a forma quadrática $Q(x)$ é totalmente simétrica, segue que

$$\begin{aligned} Q(a_0, \cdots, a_{p-2}) &= Q(1, \cdots, 1, -1, \cdots, -1, 0, \cdots, 0) = \\ &= r + s + 4rs + r(p-1-r-s) + s(p-1-r-s) = \\ &= r + s + 4rs + rp - r - r^2 - rs + sp - s - sr - s^2 = \\ &= 2rs + rp + sp - r^2 - s^2 = \\ &= -(r-s)^2 + p(r+s). \end{aligned}$$

Agora, quando $x \in \mathfrak{p}$, pela Proposição 4.2.1, tem-se que $f(1) \equiv 0 (mod\, p)$, ou seja, se $f(x) = a_0 + a_1 x + \cdots + a_{p-2}x^{p-2}$ então

$$f(1) = a_0 + \cdots + a_{p-2} = \sum_{i=0}^{p-2} a_i = r - s \equiv 0 (mod\, p),$$

e consequentemente $r = s$, tendo em vista o intervalo de variação de r e s. Portanto $Q(x) = 2pr$, e para $r = 1$ temos que $Q(x) = 2p$ é o valor mínimo. Se $(b_0, \cdots, b_{p-2})$ é uma $(p-1)$-upla de $I_2 - I_1$, então pelo Teorema 1.6.1, tomando $a_1 = 2$ e $r = 1$ teremos que $y = \frac{2}{2} = 1$, e assim

$$Q(b_0, \cdots, b_{p-2}) \geq Q(2, 1, \cdots, 1) = 4 + p - 2 + p - 2 = 4 + 2p - 4 = 2p.$$

Pelo Teorema 1.6.2, se $(b_0, \cdots, b_{p-2}) \in I_d - I_{d-1}$, com $d > 1$, então

$$Q(b_0, \cdots, b_{p-2}) \geq 2p,$$

o que demonstra a primeira parte da demonstração. Para a segunda parte, se $x = 1 - \xi_p \in \mathfrak{p}$, então

$$Q(x) = Q_{p-1}(1, -1, 0, \cdots, 0) = 1^2 + (-1)^2 + 4 + (p-3)1 + (p-3)1$$
$$= 6 + p - 3 + p - 3 = 2p - 6 + 6 = 2p,$$

e isto conclui a demonstração. □

4.3 Forma Quadrática Associada a $\mathbb{Q}(\zeta_{p^r})$

Nesta seção, veremos que a forma quadrática em corpos $\mathbb{Q}(\zeta_{p^r})$ é uma soma de p^{r-1} formas quadráticas. Além disso, apresentamos um resulado que permite calcular o traço sobre estes corpos e também resultados que serão muito úteis na minimização da forma quadrática quando $r > 1$, tomando valores em reticulados algébricos obtidos via esses corpos.

Sejam $\mathbb{K} = \mathbb{Q}(\xi_{p^r})$ e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ o anel de inteiros algébricos de $\mathbb{K}$. Se $x = \sum_{i=0}^{m-1} a_i \zeta_{p^r}^i \in \mathbb{Z}[\zeta_{p^r}]$, com $m = \phi(p^r)$, então existe uma única representação de x da forma

$$x = \sum_{j=0}^{t} x_j \zeta_{p^r}^j,$$

onde $t = p^{r-1} - 1$ e

$$x_j = \sum_{i=0,\, i \equiv j (mod\, p^{r-1})}^{m-1} a_i \zeta_{p^r}^i, \text{ para } j = 0, \cdots, t.$$

Lema 4.3.1 *([8], p.43) Se p é um número primo e r é um número inteiro positivo, então*

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = \begin{cases} 0, & se \quad mdc(k,\, p^r) < p^{r-1}, \\ -p^{r-1}, & se \quad mdc(k,\, p^r) = p^{r-1}, \\ p^{r-1}(p-1), & se \quad mdc(k,\, p^r) > p^{r-1}. \end{cases}$$

Demonstração: Como o polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é dado por $x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1$, onde $r > 1$, segue que $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = 0$. Agora, note que, se $mdc(k,\, p^r) = 1$, então $\zeta_{p^r}^k$ é um conjugado de ζ_{p^r}, ou seja, $\zeta_{p^r}^k$ é

raiz do mesmo polinômio minimal e assim possui o mesmo traço de ζ_{p^r}, e portanto $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = 0$. Assim, supondo que $mdc(k, p^r) > 1$, teremos que considerar três casos :

1º**caso:** Se $mdc(k, p^r) = p^s < p^{r-1}$, então $s \leq r-2$, e como $p^s|k$ segue que existe $k_1 \in Z$ tal que $k = p^s k_1$. Agora como, $\zeta_{p^r}^{p^s} = e^{\frac{2\pi i p^s}{p^r}} = \zeta_{p^{r-s}}$, segue que $\zeta_{p^r}^k = \zeta_{p^r}^{p^s k_1} = \zeta_{p^{r-s}}^{k_1}$, onde $mdc(p^{r-s}, k_1) = 1$, e assim

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}^{k_1}) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}).$$

Como $\mathbb{Q}(\zeta_{p^{r-s}}) \subset \mathbb{Q}(\zeta_{p^r})$ segue que

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_{p^{r-s}})] Tr_{\mathbb{Q}(\zeta_{p^{r-s}})/\mathbb{Q}}(\zeta_{p^{r-s}}).$$

Finalmente, como $Tr_{\mathbb{Q}(\zeta_{p^{r-s}})/\mathbb{Q}}(\zeta_{p^{r-s}}) = 0$, concluímos que $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}) = 0$, e portanto $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = 0$.

2º**caso:** Se $mdc(k, p^r) = p^{r-1}$, então $p^{r-1}|k$, ou seja, existe $k_1 \in \mathbb{Z}$ tal que $k = p^{r-1}k_1$. Observe que $mdc(k_1, p) = 1$. Agora, como $\zeta_{p^r}^k = \zeta_{p^r}^{k_1 p^{r-1}} = \zeta_{p^{r-(r-1)}}^{k_1} = \zeta_p^{k_1}$, segue que

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_p^{k_1}).$$

Desde que $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^r})$, segue que

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_p^{k_1}) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_p)] Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{k_1}).$$

Como $mdc(k_1, p) = 1$, segue pelo Lema 2.5.1, que $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{k_1}) = -1$ e como $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_p)] = p^{r-1}$, conluímos que $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = -p^{r-1}$.

3º**caso:** Se $mdc(k, p^r) > p^{r-1}$, então $mdc(k, p^r) = p^r$. Assim, $p^r|k$, ou seja, existe $k_1 \in \mathbb{Z}$, tal que $k = k_1 p^r$. Com isso obtemos que $\zeta_{p^r}^k = \zeta_{p^r}^{p^r k_1} = (\zeta_p^r)^{k_1} = 1^{k_1} = 1$. Agora como $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1)p^{r-1}$, segue que

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1) = (p-1)p^{r-1}.$$

□

Teorema 4.3.1 *([3], p.67) Se p é um número primo, r um número inteiro positivo,* $n = \Phi(p^r)$ *e* $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{n-1}\zeta_{p^r}^{n-1}$ *um inteiro algébrico de* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$*, então*

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}\tilde{Q}_r(\underline{x}),$$

onde $\underline{x} = (a_0, a_1, \cdots, a_{n-1})$*,* $\tilde{Q}_r(x) = Q_{p-1}(\underline{x_0}) + \cdots + Q_{p-1}(\underline{x_t})$*, com* $t = p^{r-1} - 1$ *e* $\underline{x_k} = (a_k, a_{p^{r-1}+k}, \cdots, a_{(p-2)p^{r-1}+k})$.

Demonstração: Pela Proposição 3.4.3, tem-se que $|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$. Pelo Lema 4.3.1, tem-se que os elementos $\zeta_{p^r}^k$, com $mdc(k, p^r) < p^{r-1}$, tem traço nulo. Deste modo, podemos considerar os elementos $\zeta_{p^r}^k$ tal que $mdc(k, p^r) \geq p^{r-1}$. Note que, se $mdc(k, p^r) > p^{r-1}$ então $mdc(k, p^r) = p^r$. Assim, $k = 0$ ou $k \geq p^r > (p-1)p^{r-1}$, o que não ocorre pois $1 \leq k \leq n-1 = (p-1)p^{r-1} - 1$. Logo, podemos considerar apenas os k tal que $mdc(k, p^r) = p^{r-1}$, e neste caso $k = p^{r-1}, 2p^{r-1}, \cdots, (p-2)p^{r-1}$. Tomando $x\overline{x} = A_0 + \sum_{i=1}^{m-1} A_i\alpha_i$, com $\alpha_i = \zeta_{p^r}^i + \zeta_{p^r}^{-i}$ e $A_j = \sum_{i=0}^{m-(j+1)} a_i a_{j+i}$, para $j = 0, \cdots, m-1$, tem-se

$$\begin{aligned}
|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= \frac{1}{2}\left(Tr_{\mathbb{K}/\mathbb{Q}}(A_0) + \sum_{i=1}^{n-1} Tr_{\mathbb{K}/\mathbb{Q}}(A_i\alpha_i)\right) = \\
&= \frac{1}{2}((p-1)p^{r-1}A_0 + Tr_{\mathbb{K}/\mathbb{Q}}(A_1\alpha_1) + \cdots + Tr_{\mathbb{K}/\mathbb{Q}}(A_{n-1}\alpha_{n-1})) = \\
&= \frac{1}{2}\left((p-1)p^{r-1}\sum_{i=0}^{n-1} a_i^2 + A_1 Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_1) + \cdots + A_{n-1}Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_{n-1})\right) = \\
&= \frac{(p-1)}{2}p^{r-1}\left(\sum_{i=0}^{n-1} a_i^2\right) - p^{r-1}\left(\sum_{j=1}^{p-2} A_{jp^{r-1}}\right) = \\
&= \frac{p^{r-1}}{2}\left((p-1)\left(\sum_{i=0}^{n-1} a_i^2\right) - 2\sum_{j=1}^{p-2} A_{jp^{r-1}}\right).
\end{aligned}$$

Escrevendo $(p-1)\left(\sum_{i=0}^{n-1} a_i^2\right) = (p-1)b_0 + \cdots + (p-1)b_t$, onde $t = p^{r-1} - 1$ e

$$\begin{cases} b_0 = a_0^2 + a_{p^{r-1}}^2 + \cdots + a_{(p-2)p^{r-1}}^2 \\ b_1 = a_1^2 + a_{p^{r-1}+1}^2 + \cdots + a_{(p-2)p^{r-1}+1}^2 \\ \vdots \\ b_t = a_t^2 + a_{p^{r-1}+t}^2 + \cdots + a_{(p-2)p^{r-1}+t}^2, \end{cases}$$

tem-se que $|\sigma_{\mathbb{K}}(x)|^2 = \dfrac{p^{r-1}}{2}\left((p-1)b_0 + \cdots + (p-1)b_t - 2\sum_{j=1}^{p-2} A_{jp^{r-1}}\right)$. Assim, $\sum_{j=1}^{p-2} A_{jp^{r-1}} = \sum a_i a_j$, onde a última soma é tomada sobre todos os $a_i's$, para $i = 0, \cdots, n-1$, satisfazendo $i < j$ e $i \equiv j (mod\, p^{r-1})$, uma vez que, tomando $a_i a_j$ tal que $i < j$ e $i \equiv j (mod\, p^{r-1})$, tem-se que $p^{r-1}|(i-j)$ o que implica que existe $u \in \{1, \cdots, p-2\}$ tal que $i - j = up^{r-1}$, ou seja, $j = i + up^{r-1}$. Logo $a_i a_j = a_i a_{i+up^{r-1}}$. Agora, observe que no primeiro somatório, um produto $a_i a_j$ aparece uma única vez, o que prova a igualdade. Podemos, agora, reescrever

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}((p-1)b_0 - 2d_0 + \cdots + (p-1)b_t - 2d_t),$$

onde $d_k = \sum a_i a_j$, para $i < j,\ j \equiv k (mod\, p^{r-1})$, e $k = 0, \cdots, t$. Assim

$$(p-1)b_k - 2d_k = Q_{p-1}(a_k, a_{k+p^{r-1}}, \cdots, a_{k+(p-2)p^{r-1}}),$$

para $k = 0, \cdots, t$, o que completa a demonstração. □

Exemplo 4.3.1 *Sejam $p = 11$, $r = 1$ e $x = 1 - \zeta_{11}$ um elemento de $\mathbb{Z}[\zeta_{11}]$. Se $x = (1, -1, 0, 0, 0, 0, 0, 0, 0, 0)$, então*

$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}\tilde{Q}_{10}(x) = \frac{1}{2}Q_{10}(1, -1, 0, 0, 0, 0, 0, 0, 0, 0) = \frac{1}{2}(10 + 10 + 2) = 11,$

ou seja, $|\sigma_{\mathbb{K}}(x)| = \sqrt{11}$.

Exemplo 4.3.2 *Sejam $p = 2$, $r = 3$ e $x = 1 - \zeta_8$ um elemento de $\mathbb{Z}[\zeta_8]$. Se $x = (1, -1, 0, 0)$, então*

$|\sigma_K(x)|^2 = \frac{4}{2}\tilde{Q}_3(x) = 2(Q_1(1) + Q_1(-1) + Q_1(0) + Q_1(0)) = 2(1 + 1 + 0 + 0) = 4,$

ou seja, $|\sigma(x)| = \sqrt{4} = 2$.

Proposição 4.3.1 *([8], p.41) Se* $\mathfrak{p}$ *é o ideal de* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ *gerado por* $1-\zeta_{p^r}$, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$, $f(x) \in \mathbb{Z}[x]$ *tal que* $\alpha = f(\zeta_{p^r})$, *então*

$$\alpha \in \mathfrak{p}^{i+1} \Longleftrightarrow f(1) \equiv f'(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 (mod\, p),$$

onde $f^{(i)}(x)$ *denota a i-ésima derivada de* $f(x)$, *para* $i = 0, 1, 2, \ldots, m$, *e* $m = \phi(p^r)$.

Proposição 4.3.2 *([3], p.82) Se* $r > 1$, *então* $\tilde{Q}_r(x) \geq 2(p-1)$, *para qualquer* $x \in \mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *e* $x \neq 0$. *Além disso,* $\tilde{Q}_r(x) = 2(p-1)$ *para* $x = 1-\zeta_{p^r}$.

Demonstração: Se $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, onde $m = \Phi(p^r)$, então podemos escrevê-lo de uma única maneira como $x = x_0 + x_1\zeta_{p^r} + \cdots + x_t\xi_{p^r}^t$, onde $t = p^{r-1} - 1$ e

$$\begin{cases} x_0 = a_0 + a_{p^{r-1}}\zeta_{p^r}^{p^{r-1}} + \cdots + a_{(p-2)p^{r-1}}\zeta_{p^r}^{(p-2)p^{r-1}}; \\ x_1 = a_1 + a_{p^{r-1}+1}\zeta_{p^r}^{p^{r-1}+1} + \cdots + a_{(p-2)p^{r-1}+1}\zeta_{p^r}^{(p-2)p^{r-1}+1}; \\ \vdots \\ x_t = a_t + a_{p^{r-1}+t}\zeta_{p^r}^{p^{r-1}+t} + \cdots + a_{(p-2)p^{r-1}+t}\zeta_{p^r}^{(p-2)p^{r-1}+t}. \end{cases}$$

Assim, pelo Teorema 4.3.1, tem-se que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}\tilde{Q}_r(x) = \frac{p^{r-1}}{2}\left(Q(\underline{x_1}) + \cdots + Q(\underline{x_t})\right).$$

Se $x \in \mathfrak{p}$ e se existir um único x_j não nulo na decomposição acima, então $Q(\underline{x_j}) \geq 2p$, e portanto $\tilde{Q}_r(x) \geq 2p > 2(p-1)$. Visto que $p-1$ é o menor valor que $Q(\underline{a})$ assume, com $\underline{a} \in \mathbb{Z}^{p-1}$, segue que se o número dos $a_i's$ não nulos for maior que 1, então

$$\tilde{Q}_r(x) \geq 2(p-1).$$

Finalmente, tem-se que o elemento $x = 1 - \xi_{p^r} \in \mathfrak{p}$ satisfaz $\tilde{Q}_r(x) = 2(p-1)$ e isto conclui a demonstração. □

4.4 Forma Quadrática Associada a $\mathbb{Q}(\zeta_{pq})$

Nesta seção, apresentamos resultados sobre o cálculo da função traço via os corpos ciclotômicos $\mathbb{Q}(\zeta_{pq})$, onde p e q são primos distintos.

Lema 4.4.1 *([8], p.66) Se p e q são números primos distintos então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = \begin{cases} 1, & se\ mdc(k,pq)=1 \\ 1-p, & se\ mdc(k,pq)=p \\ 1-q, & se\ mdc(k,pq)=q \\ (1-p)(1-q), & se\ mdc(k,pq)=pq. \end{cases}$$

Demonstração: Tem-se que $Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_{pq}^k))$, pois $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{pq})$. Pelo Lema 2.5.1, segue que, $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^k) = -1$, quando o $mdc(p,k)=1$. Também $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1) = [\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$. Analogamente, temos os mesmos resultados para $\mathbb{Q}(\zeta_q) \subset \mathbb{Q}(\zeta_{pq})$. Assim, temos 4 casos a considerar.

1º**caso:** Se $mdc(k,pq)=1$, então $mdc(p,q)=1$, segue que existem $r,\ s \in \mathbb{Z}$ tal que $pr+qs=1$. Assim $k = kpr+kqs$, com $mdc(q,kr) = mdc(p,ks) = 1$. Dessa forma, vemos que

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{kpr+kqs}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{kpr}\zeta_{pq}^{kps}) = \\ &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_q^{kr}\zeta_p^{ks}) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{kr}\zeta_p^{ks})) = \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{kr}) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q^{kr}) = \\ &= -Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}) = 1 \end{aligned}$$

2º**caso:** Se $mdc(k,pq)=p$, então existe $k_1 \in \mathbb{Z}$ tal que $k = k_1 p$, com $mdc(k_1,q)=1$. Assim, $\zeta_{pq}^k = \zeta_{pq}^{k_1 p} = \zeta_q^{k_1}$, e portanto,

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_q^{k_1}) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{k_1})) = \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q^{k_1})) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-1) = \\ &= -1(p-1) = 1-p. \end{aligned}$$

3º**caso:** Se $mdc(k,pq)=q$, então existe $k_2 \in \mathbb{Z}$ tal que $k = k_2 q$, onde $mdc(k_2,p)=1$. Assim, $\zeta_{pq}^k = \zeta_{pq}^{k_2 q} = \zeta_p^{k_2}$, e portanto,

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_p^{k_2}) = Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_q)}(\zeta_p^{k_2})) =$$
$$= Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{k_2})) = Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(-1) = -1(q-1) =$$
$$= 1 - q.$$

4º**caso:** Se $mdc(k, pq) = pq$, então existe $k_3 \in \mathbb{Z}$ tal que $k = (pq)k_3$. Logo $\zeta_{pq}^k = \zeta_{pq}^{(pq)k_3} = (\zeta_{pq}^{pq})^{k_3} = 1^{k_3} = 1$. Como $[\mathbb{Q}(\zeta_{pq}) : \mathbb{Q}] = (p-1)(q-1)$, segue que $Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(1) = (p-1)(q-1)$. □

Corolário 4.4.1 *([8], p.67) Se* $0 \leq k \leq pq$ *então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^p - \zeta_{pq}^q + \zeta_{pq}^{p+q}).\zeta_{pq}^k) = \begin{cases} -pq \text{ se } k = pq - p \text{ ou } k = pq - q \\ pq, \text{ se } k = 0 \text{ ou } k = pq - p - q, \\ 0, \text{ caso contrário,}. \end{cases}$$

Demonstração: Observe que $(1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q})\zeta_{pq}^k = \zeta_{pq}^k-\zeta_{pq}^{p+k}-\zeta_{pq}^{q+k}+\zeta_{pq}^{p+q+k}$, assim, tem-se 3 casos a considerar.

1º**caso:** Se $mdc(pq, k) = 1$, então pelo Lema 4.4.1, como o expoente de cada parcela é primo com pq, segue que o traço de cada uma dessas parcelas é 1. Assim

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^p - \zeta_{pq}^q + \zeta_{pq}^{p+q})\zeta_{pq}^i) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^i) - Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p+i}) -$$
$$-Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{q+i}) + Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p+q+i})$$
$$= 1 - 1 - 1 + 1 = 0.$$

2º**caso:** Se $k = 0$, então pelo Lema 4.4.1, obtemos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^p - \zeta_{pq}^q + \zeta_{pq}^{p+q})) = (p-1)(q-1) + p - 1 + q - 1 + 1 =$$
$$= pq.$$

Agora, se $k = pq - p - q$ então

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q})\zeta_{pq}^{pq-p-q}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{pq-p-q}-\zeta_{pq}^{pq-q}-\zeta_{pq}^{pq-p}+\zeta_{pq}^{pq}) =$$
$$= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{-p-q} - \zeta_{pq}^{-q} - \zeta_{pq}^{-p)} + 1) =$$
$$= 1 - (1-q) - (1-p) + (1-p)(1-q) =$$
$$= pq.$$

3º**caso:** Se $k = pq - p$, então

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^{p}-\zeta_{pq}^{q}+\zeta_{pq}^{p+q})\zeta_{pq}^{pq-p}) &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{pq-p}-1-\zeta_{pq}^{pq-p+q}-\zeta_{pq}^{q+pq}) = \\ &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p(q-1)}-1-\zeta_{pq}^{-p+q}+\zeta_{pq}^{q(1+p)}) = \\ &= 1-p-(1-p)(1-q)-1+1-q = \\ &= 1-p-pq+p+q-1-1+1-q = \\ &= -pq. \end{aligned}$$

Analogamente para $k = pq - q$, temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^{p}-\zeta_{pq}^{q}+\zeta_{pq}^{p+q})\zeta_{pq}^{pq-q}) = -pq,$$

e isto conclui a demonstração. □

Proposição 4.4.1 *([8], p.67) Se p e q são números primos distintos, $n = \Phi(pq)$ e x é um elemento de $\mathbb{Z}[\zeta_{pq}]$, com $x = a_0 + a_1\zeta_{pq} + \cdots + a_{n-1}\zeta_{pq}^{n-1}$, então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)A_0 + 2(1-p)\sum_{p|k} A_k + 2(1-q)\sum_{q|k} A_k + 2\sum_{p\nmid k,\, q\nmid k} A_k,$$

onde $A_k = \displaystyle\sum_{i=0}^{n-(k+1)} a_i a_{k+i}$, *para* $k = 0, 1, \cdots, n-1$.

Demonstração: Como $x\overline{x} = A_0 + \displaystyle\sum_{i=1}^{n-1} A_i\alpha_i$, segue que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(A_0) + \sum_{k=1}^{n-1} A_k Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_k),$$

com $\alpha_k = \zeta_{pq}^{k} + \zeta_{pq}^{-k}$. Pelo Lema 4.4.1, tem-se que

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) &= A_0(p-1)(q-1) + A_1 Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{1}+\zeta_{pq}^{-1}) + \cdots + \\ &\quad + A_{n-1} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{n-1}+\zeta_{pq}^{-n+1}) = \\ &= (p-1)(q-1)A_0 + 2(1-p)\sum_{p|k} A_k + 2(1-q)\sum_{q|k} A_k + 2\sum_{p\nmid k,\, q\nmid k} A_k, \end{aligned}$$

e isto conclui a demonstração. □

4.5 Forma Quadrática Associada a Subcorpos de $\mathbb{Q}(\zeta_{pq})$

Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos de números com $[\mathbb{L} : \mathbb{K}] = n$, $\sigma_{\mathbb{K}}$ e $\sigma_{\mathbb{L}}$ os homomorfismos canônicos de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Se $x \in \mathbb{K}$ e $c_{\mathbb{K}}$, $c_{\mathbb{L}}$ assume os valores no conjunto $\{1/2, 1\}$ conforme o corpo em questão seja real ou complexo, então

$$|\sigma_{\mathbb{L}}(x)|^2 = c_{\mathbb{L}} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = nc_{\mathbb{L}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

o que implica em

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{c_{\mathbb{K}}}{nc_{\mathbb{L}}} |\sigma_{\mathbb{L}}(x)|^2.$$

Sejam $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_p)$ de índice n e G o grupo de Galois de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{K}$. Assim, pelo Teorema 2.6.2, tem-se que $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$.

Observando a simetria de Q, pondo $u = (p-1)/n$, obtemos,

$$|\sigma_{\mathbb{K}}(x)|^2 = Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{n} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \frac{1}{2n} Q_{p-1}(a_0, \ldots, a_0, \ldots, a_u, \ldots, a_u),$$

onde cada a_i, para $i = 0, 1, 2, \ldots, u$, aparece repetido n vezes. Assim, chega-se a expressão,

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}((a_1^2 + \ldots + a_u^2) + n \sum_{i<j} (a_i - a_j)^2).$$

Sejam $\mathbb{K}_1 \subset \mathbb{Q}(\zeta_p)$, $\mathbb{K}_2 \subset \mathbb{Q}(\zeta_q)$ e $\{\alpha_1, \ldots, \alpha_u\}$, $\{\beta_1, \ldots, \beta_v\}$ bases integrais de $\mathbb{A}_{\mathbb{K}_1}$ e $\mathbb{A}_{\mathbb{K}_2}$, respectivamente, e

$$x = \sum_{j=1}^{v} \sum_{i=1}^{u} a_{ij} \alpha_i \beta_j = \sum_{j=1}^{v} x_j \beta_j \in \mathbb{K}_1 \mathbb{K}_2,$$

onde $x_j = \sum_{i=1}^{u} a_{ij} \alpha_i$, para $j = 1, 2, \ldots, r$.

Se Q' e Q'' são as formas quadráticas associadas a $\mathbb{K}_1$ e $\mathbb{K}_2$, respectivamente, então

$$Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{Q}}(x\overline{x}) = Q"(Q'(x_1), \ldots, Q'(x_v)).$$

4.6 Conclusão

Neste capítulo, apresentamos as formas quadráticas associadas aos corpos ciclotômicos, onde vimos, que a função traço de um elemento de um corpo de números $\mathbb{K}$ com o seu conjugado é equivalente a forma quadrática deste elemento. E como o objetivo deste trabalho é encontrar reticulados algébricos que possuam densidade de centro ótima, apresentamos alguns resultados que facilitem o cálculo da função traço, que está diretamente ligado ao cálculo da densidade de centro de um reticulado algébrico.

Capítulo 5

Construções Algébricas

5.1 Introdução

Este capítulo tem como objetivo apresentar resultados que facilitem o cálculo da densidade de centro dos reticulados algébricos. Além disso, apresentamos exemplos de reticulados algébricos de dimensão 2, 4, 6 e 8, com densidade de centro ótima. Assim, na Seção 5.2, apresentamos alguns reticulados algébricos obtidos via $\mathbb{Q}(\zeta_p)$ com suas respectivas densidade de centro. Na Seção 5.3, verificamos que a densidade de centro é periódica e apresentamos reticulados algébricos obtidos via $\mathbb{Q}(\zeta_{p^r})$, com p primo e $r \geq 1$. Para finalizar, na Seção 5.4, apresentamos os reticulados algébricos via $\mathbb{Q}(\zeta_{pq})$, onde p e q são primos distintos. Lembramos, que o uso do software MATHEMATICA foi indispensável nos cálculos apresentado neste capítulo.

5.2 Reticulados via $\mathbb{Q}(\zeta_p)$

Nesta seção, apresentamos um método para calcular a densidade de centro de reticulados algébricos via corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, com p primo. Antes, daremos um exemplo construtivo para ilustrar este resultado.

Exemplo 5.2.1 *Se* $\mathbb{K} = \mathbb{Q}(\zeta_3)$*, então* $[\mathbb{K} : \mathbb{Q}] = 2$*. Agora, seja* $\mathfrak{p}$ *um ideal primo de* $\mathbb{A}_{\mathbb{K}}$*, onde* $\mathfrak{p} = (1 - \zeta_3)\mathbb{A}_{\mathbb{K}}$*. Observe, pelo Teorema 2.5.1, que* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$*. Assim,*

se $x \in \mathfrak{p}$*, então existem* $a_0, a_1 \in \mathbb{Z}$*, tal que* $x = (1-\zeta_3)(a_0 + a_1\zeta_3)$*. Agora, como* $\overline{\zeta_3} = \zeta_3^{-1}$*, segue que* $\overline{x} = (1-\zeta_3^{-1})(a_0 + a_1\zeta_3^{-1})$*, e assim*

$$\begin{aligned} x\overline{x} &= (1-\zeta_3)(a_0+a_1\zeta_3)(1-\zeta_3^{-1})(a_0+a_1\zeta_3^{-1}) \\ &= a_0^2 + a_1^2 + (a_1-a_0)^2 + (a_0a_1 - a_0^2)(\zeta_3+\zeta_3^{-1}) + \\ &+ (a_0a_1 - a_1^2)(\zeta_3+\zeta_3^{-1}) + (-a_0a_1)(\zeta_3^2+\zeta_3^{-2}). \end{aligned}$$

Usando a linearidade do traço, o fato que $Tr_{\mathbb{K}/\mathbb{Q}}(a_i) = 2a_i$ *e o Lema 2.5.1, item(a), tem-se que*

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= Tr_{\mathbb{K}/\mathbb{Q}}(a_0^2 + a_1^2 + (a_1-a_0)^2 + (a_0a_1 - a_0^2)(\zeta_3+\zeta_3^{-1}) + \\ &+ (a_0a_1 - a_1^2)(\zeta_3+\zeta_3^{-1}) + (-a_0a_1)(\zeta_3^2+\zeta_3^{-2})) = \\ &= 2a_0^2 + 2a_1^2 + 2(a_1-a_0)^2 - 2(a_0a_1 - a_0^2) - 2(a_0a_1 - a_1^2) - 2(-a_0a_1) = \\ &= 6a_0^2 + 6a_1^2 - 6a_0a_1. \end{aligned}$$

Fazendo $t = min\{Tr_{\mathbb{K}/Q}(x\overline{x}); x \in \mathfrak{p}\, e\, x \neq 0\}$*, obtemos que* $t = 6$*, com* $a_0 = 0$ *e* $a_1 = 1$*. Agora, pela Proposição 2.5.1, tem-se que* $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_3) = -3$*, e pelas Proposições 1.8.3 e 1.8.4, temos que* $N(\mathfrak{p}) = N((1-\zeta_3)\mathbb{A}_{\mathbb{K}}) = N(1-\zeta_3)N(\mathbb{A}_{\mathbb{K}}) = N(1-\zeta_3)$*. Assim, pelo Lema 2.5.1, concluímos que* $N(\mathfrak{p}) = N(1-\zeta_3) = 3$*. Portanto, para calcular a densidade de centro do reticulado algébrico* $\sigma_{\mathbb{K}}(\mathfrak{p})$*, usamos a Observação 3.4.2, ou seja,*

$$\delta(\sigma_{\mathbb{K}}(1-\zeta_3)) = \delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})} = \frac{\frac{6}{4}}{\sqrt{3}.3} = \frac{1}{2\sqrt{3}} \simeq 0,288675,$$

que é a maior densidade conhecida em dimensão 2, que corresponde a densidade de centro do reticulado Λ_2.

Agora, vamos considerar ideais principais não nulos do anel de inteiros algébricos $\mathbb{A}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e calcular a densidade de centro dos reticulados algébricos obtidos via esses ideais. Deste modo, seja $\mathfrak{p} = \lambda\mathbb{A}_{\mathbb{K}}$ o ideal primo de $\mathbb{A}_{\mathbb{K}}$, com $\lambda = 1-\zeta_p$. Se $\alpha \in \mathfrak{p}$, com $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i$, temos que $\alpha \equiv \sum_{i=0}^{p-2} a_i (mod\, \mathfrak{p})$, uma vez que $\zeta_p \equiv 1 (mod\, \mathfrak{p})$. Assim, $\alpha \in \mathfrak{p}$ se, e somente se, $\sum_{i=0}^{p-2} a_i \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Como $1-\zeta_p \in \mathfrak{p}$, pela Proposição 4.2.2, segue que $Q(1, -1, 0, \cdots, 0) = 2p$, e assim

$$t_{\mathfrak{p}} = min\{Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}); \alpha \in \mathfrak{p},\, \alpha \neq 0\} = 2p.$$

Pelo Lema 2.5.1, tem-se que $N(\mathfrak{p}) = N(\lambda) = p$ e pela Proposição 2.5.1 tem-se que $D_{\mathbb{K}} = -p^{p-2}$. Assim, pela Observação 3.4.2, a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{p})$, onde o ideal $\mathfrak{p} = \lambda\mathbb{A}_{\mathbb{K}}$ é dada por

$$\delta(\sigma_K(\mathfrak{p})) = \frac{\left(\frac{2p}{4}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}}p} = \frac{p^{\frac{p-1}{2}}}{2^{\frac{p-1}{2}}p^{\frac{p}{2}}} = \frac{1}{p^{\frac{1}{2}}2^{\frac{p-1}{2}}}, \tag{5.1}$$

onde a melhor densidade de centro ocorre com $p = 3$.

5.3 Reticulados via $\mathbb{Q}(\zeta_{p^r})$

Nesta seção, apresentamos a densidade de centro de alguns reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$. Primeiramente, calculamos a densidade de centro dos reticulados $\sigma(\mathfrak{p}^i)$, para $i \geq 1$, onde $\mathfrak{p}$ é um ideal principal de $\mathbb{Z}[\zeta_{p^r}]$ gerado pelo elemento $1-\zeta_{p^r}$. Além disso, verificamos que a densidade de centro é periódica com período igual o grau da extensão ciclotômica de $\mathbb{Q}(\zeta_{p^r})$. Finalmente, analisamos quando os reticulados $\sigma(\mathfrak{p}^i)$, para $i \geq 1$, possuem a maior densidade de centro.

Proposição 5.3.1 *Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$, então a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{p}^j)$, para $j \in \mathbb{N}$, é periódica, ou seja,*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^n)) = \delta(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})),$$

com $m = \Phi(p^r)$ e $n \in \mathbb{N}$.

Demonstração: Pela Proposição 3.2.4, tem-se que $p\mathbb{A}_{\mathbb{K}} = \mathfrak{p}^m$, portanto $\mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ é a fatoração de $p\mathbb{A}_{\mathbb{K}}$ em ideais primos de $\mathbb{A}_{\mathbb{K}}$, e p se ramifica completamente. Logo, $\mathfrak{p}^{n+m} = \mathfrak{p}^n\mathfrak{p}^m = p\mathfrak{p}^n$, o que implica que $N(\mathfrak{p}^{n+m}) = p^{n+m}$. Como $\mathfrak{p}^{n+m} = p\mathfrak{p}^n$, segue que $x \in \mathfrak{p}^{n+m}$ se, e somente se, $x = py$, onde $y \in \mathfrak{p}^n$. Assim, pelo

Teorema 4.3.1, segue que

$$\begin{aligned}\tilde{Q}_r(x) &= \frac{2|\sigma(x)|^2}{p^{r-1}} = \frac{2|\sigma(py)|^2}{p^{r-1}} = \frac{2Tr_{\mathbb{K}/\ Q}(py\overline{py})}{p^{r-1}} = \\ &= \frac{2}{p^{r-1}}Tr_{\mathbb{K}/\ Q}(p^2y\overline{y}) = \frac{2}{p^{r-1}}p^2Tr_{K\mathbb{Q}}(y\overline{y}) = \\ &= p^2\frac{2}{p^{r-1}}Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = p^2\frac{2}{p^{r-1}}|\sigma(y)|^2 = \\ &= p^2\tilde{Q}_r(\underline{y}).\end{aligned}$$

Pela Proposição 3.4.3, segue que

$$\rho(\sigma_K(\mathfrak{p}^n)) = min\left\{\frac{|\sigma(x)|}{2};\, x \in \mathfrak{p}^n\,, x \neq 0\right\}$$

e

$$\begin{aligned}\rho(\sigma_K(\mathfrak{p}^{n+m})) &= min\left\{\frac{|\sigma(x)|}{2};\, x \in \mathfrak{p}^{n+m}\,, x \neq 0\right\} = \\ &= min\left\{\frac{|\sigma(x)|}{2};\, x \in p\mathfrak{p}^n\,, x \neq 0\right\} = p\rho(\sigma_K(\mathfrak{p}^n)).\end{aligned}$$

Assim, pela Observação 3.4.1, segue que

$$\begin{aligned}\delta(\sigma_K(\mathfrak{p}^{n+m})) &= \frac{2^{r_2}(\rho(\sigma_K(\mathfrak{p}^{n+m})))^m}{|D_K|^{\frac{1}{2}}p^{n+m}} = \frac{2^{r_2}(p\rho(\sigma_K(\mathfrak{p}^n)))^m}{|D_K|^{\frac{1}{2}}p^{n+m}} = \\ &= \frac{2^{r_2}p^m(\rho(\sigma_K(\mathfrak{p}^n)))^m}{|D_K|^{\frac{1}{2}}p^np^m} = \frac{2^{r_2}(\rho(\sigma_K(\mathfrak{p}^n)))^m}{|D_K|^{\frac{1}{2}}p^n} = \\ &= \delta(\sigma_K(\mathfrak{p}^n)),\end{aligned}$$

concluindo a demonstrção. □

Exemplo 5.3.1 *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_8)$ *e* $\mathfrak{p}$ *um ideal primo de* $\mathbb{A}_\mathbb{K}$*, onde* $\mathfrak{p} = (1-\zeta_8)\mathbb{A}_\mathbb{K}$*. Note que* $\mathbb{A}_\mathbb{K} = \mathbb{Z}[\zeta_8]$ *e* $[\mathbb{K} : \mathbb{Q}] = 4$*. Mostramos que* $\delta(\sigma_\mathbb{K}(\mathfrak{p}^2)) = \delta(\sigma_\mathbb{K}(\mathfrak{p}^{2+4}))$*. De fato,* $\mathfrak{p}^2 = (1 - 2\zeta_8 + \zeta_8^2)\mathbb{A}_\mathbb{K}$*, e assim dado* $x \in \mathfrak{p}^2$*, tem-se que*

$$x = (1 - 2\zeta_8 + \zeta_8^2)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3),$$

e seu conjugado é,

$$\overline{x} = (1 - 2\zeta_8^{-1} + \zeta_8^{-2})(a_0 + a_1\zeta_8^{-1} + a_2\zeta_8^{-2} + a_3\zeta_8^{-3}).$$

Portanto,

$$\begin{aligned} x\overline{x} = &(6a_0^2 - 8a_0a_1 + 6a_1^2 - 8a_1a_2 + 6a_2^2 + 8a_0a_3 - 8a_2a_3 + 6a_3^2)+ \\ &+(-4a_0^2 + 6a_0a_1 - 4a_1^2 + 6a_1a_2 - 4a_2^2 - 6a_0a_3 + 6a_2a_3 - 4a_3^2)\zeta_8+ \\ &+(4a_0^2 - 6a_0a_1 + 4a_1^2 - 6a_1a_2 + 4a_2^2 + 6a_0a_3 - 6a_2a_3 + 4a_3^2)\zeta_8^3. \end{aligned}$$

Pelo Lema 4.3.1, como o $mdc(1,8) = mdc(3,8) = 1 < 4$, *segue que* $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_8) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_8^3) = 0$, *e assim*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 4(6a_0^2 - 8a_0a_1 + 6a_1^2 - 8a_1a_2 + 6a_2^2 + 8a_0a_3 - 8a_2a_3 + 6a_3^2).$$

Fazendo $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), x \in \mathfrak{p}^2, x \neq 0\}$, *tem-se que* $t = 8$, *com* $a_3 = 0$ *e* $a_0 = a_1 = a_2 = -1$. *Pela Proposição 2.5.3, tem-se que* $D_{\mathbb{K}} = 2^8$ *e pelas Proposições 2.5.2 e 1.8.3, tem-se que* $N(\mathfrak{p}^2) = 2^2$. *Assim, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$, *é dado por*

$$\delta(\sigma_k(\mathfrak{p}^2)) = \frac{2^2}{2^4 2^2} = \frac{1}{16} = 0,0625.$$

Por outro lado, considere, agora $\mathfrak{p}^6 = \mathfrak{p}^2\mathfrak{p}^4$. *Pela Proposição 3.2.5, tem-se que* $\mathfrak{p}^4 = 2\mathbb{A}_{\mathbb{K}}$, *e assim* $\mathfrak{p}^6 = 2\mathfrak{p}^2\mathbb{A}_{\mathbb{K}}$. *Dessa forma, se* $x \in \mathfrak{p}^6$, *então*

$$x = 2(1 - 2\zeta_8 + \zeta_8^2)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$$

e seu conjugado é,

$$\overline{x} = 2(1 - 2\zeta_8^{-1} + \zeta_8^{-2})(a_0 + a_1\zeta_8^{-1} + a_2\zeta_8^{-2} + +a_3\zeta_8^{-3}).$$

Fazendo $x\overline{x}$ *obtemos que*

$$\begin{aligned} x\overline{x} = &(24a_0^2 - 32a_0a_1 + 24a_1^2 - 32a_1a_2 + 24a_2^2 + 32a_0a_3 - 32a_2a_3 + 24a_3^2)+ \\ &+(-16a_0^2 + 24a_0a_1 - 16a_1^2 + 24a_1a_2 - 16a_2^2 - 24a_0a_3 + 24a_2a_3 - 16a_3^2)\zeta_8+ \\ &+(16a_0^2 - 24a_0a_1 + 16a_1^2 - 24a_1a_2 + 16a_2^2 + 24a_0a_3 - 24a_2a_3 + 16a_3^2)\zeta_8^3. \end{aligned}$$

Usando, novamente o Lema 4.3.1, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_8) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_8^3) = 0$, *e assim*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 4(24a_0^2 - 32a_0a_1 + 24a_1^2 - 32a_1a_2 + 24a_2^2 + 32a_0a_3 - 32a_2a_3 + 24a_3^2).$$

Fazendo $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), x \in \mathfrak{p}^6, x \neq 0\}$, *obtemos que* $t = 32$. *Como,* $D_{\mathbb{K}} = 2^8$ *e* $N(\mathfrak{p}^6) = 2^6$, *segue que a densidade de cento do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{p}^6)$ *é dado por*

$$\delta(\sigma_k(\mathfrak{p}^6)) = \frac{2^6}{2^4 2^6} = \frac{1}{16} = 0,0625.$$

Portanto, concluímos que $\delta(\sigma_k(\mathfrak{p}^2)) = \delta(\sigma_k(\mathfrak{p}^6))$.

A seguir, nosso objetivo é mostrar que em um corpo ciclotômico $\mathbb{Q}(\zeta_{p^r}) = \mathbb{K}$, com p primo e $r > 2$, o ideal $\mathfrak{p} = (1 - \zeta_{p^r})^i \mathbb{A}_{\mathbb{K}}$ possui densidade de centro ótimo quando $i = 1$. Mas antes daremos um exemplo, para mostrar este resultado.

Exemplo 5.3.2 *Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde $p = 2$ e $r = 3$ e $\mathfrak{p}$ um ideal primo de $\mathbb{A}_{\mathbb{K}}$, com $\mathfrak{p} = (1-\zeta_8)\mathbb{A}_{\mathbb{K}}$. Pelo Teorema 2.5.5, tem-se que $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$, onde $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$ é uma base de $\mathbb{Z}[\zeta_8]$ como um $\mathbb{Z}$-módulo. Se $x \in \mathfrak{p}$, então*

$$x = (1 - \zeta_8)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3),$$

com $a_i \in \mathbb{Z}$, para $i = 0, 1, 2, 3$. Se $\overline{x}$ é o conjugado de x, então

$$\overline{x} = (1 - \zeta_8^{-1})(a_0 + a_1\zeta_8^{-1} + a_2\zeta_8^{-2} + a_3\zeta_8^{-3}).$$

Assim,

$$\begin{aligned} x\overline{x} = &(2a_0^2 - 2a_0a_1 + 2a_1^2 - 2a_1a_2 + 2a_2^2 + 2a_0a_3 - 2a_2a_3 + 2a_3^2)+ \\ &+(-a_0^2 + 2a_0a_1 - a_1^2 + 2a_1a_2 - a_2^2 - 2a_0a_3 + 2a_2a_3 - a_3^2)\zeta_8+ \\ &+(a_0^2 - 2a_0a_1 + a_1^2 - 2a_1a_2 + a_2^2 + 2a_0a_3 - 2a_2a_3 + a_3^2)\zeta_8^3. \end{aligned}$$

Pelo Lema 4.3.1, como o $mdc(1, 8) = mdc(3, 8) = 1 < 4$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_8) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_8^3) = 0$, e assim,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 4(2a_0^2 - 2a_0a_1 + 2a_1^2 - 2a_1a_2 + 2a_2^2 + 2a_0a_3 - 2a_2a_3 + 2a_3^2).$$

Agora, calculando $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}); x \in \mathfrak{p}, x \neq 0\}$, obtemos que $t = 8$, para $a_0 = a_1 = 1$ e $a_2 = a_3 = 0$. Por outro lado, pela Proposição 2.5.3, temos que $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_8, \zeta_8^2, \zeta_8^3) = 2^8$ e pelas Proposições 1.8.3, 1.8.4 e 1.5.5, obtemos que $N(\mathfrak{p}) = N(1-\zeta_8) = 2$. Portanto, a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{p})$, usando a Observação 3.4.2, é dado por

$$\delta(\sigma_{\mathbb{K}}(1 - \zeta_8)) = \frac{1}{2^n|D_{\mathbb{K}/\mathbb{Q}}|^{1/2}} \frac{t^{n/2}}{N(\mathfrak{p})} = \frac{1}{2^4|2^8|^{1/2}} \frac{8^2}{2} = \frac{1}{2^3} = \frac{1}{8} = 0,125,$$

que é a maior densidade em dimensão 4, e que corresponde a densidade de centro do reticulado Λ_4.

Pelos Exemplos 5.3.1 e 5.3.2 vemos que $\delta(\sigma_{\mathbb{K}}(1 - \zeta_8)) > \delta(\sigma_{\mathbb{K}}(1 - \zeta_8)^2)$.

Lema 5.3.1 *([3], p.75) O elemento* $1-\zeta_{p^r}^{p^{r-2}}$ *pertence a* $\mathfrak{p}^{p^{r-2}}$.

Teorema 5.3.1 *([8], p.48) Se* $r>2$ *e* $\mathfrak{p}=(1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *então a maior densidade de centro entre os reticulados* $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, *para* $i=1,\cdots,p^{r-2}$, *ocorre com* $i=1$.

Demonstração: Pelo Lema 5.3.1, temos que o elemento $x=1-\zeta_{p^r}^{p^{r-2}}$ pertence a $\mathfrak{p}^{p^{r-2}}$ e além disso, pela Proposição 4.3.2, temos que $\tilde{Q}_r(x)=2(p-1)$. Assim, para $i=1,\cdots,p^{r-2}$, temos que

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^i))=\frac{\sqrt{(p-1)p^{r-1}}}{2},$$

e a densidade de centro é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i))=\frac{((p-1)p^{r-1})^{n/2}}{2^{n/2}|D_{\mathbb{K}}|^{\frac{1}{2}}p^i},$$

onde $n=\Phi(p^r)$ e $|D_{\mathbb{K}}|=p^{p^{r-1}(pr-r-1)}$. Isto mostra que $\sigma_{\mathbb{K}}(\mathfrak{p})$ tem a maior densidade de centro dentre os reticulados considerados. □

Observamos que, quando $\mathbb{K}=\mathbb{Q}(\zeta_{p^r})$ com p primo maior que 2 e $r=2$, o ideal $\mathfrak{p}=(1-\zeta_{p^r})^i$ tem maior densidade de centro quando $i=2$. Veremos um exemplo, antes de mostrar este resultado.

Exemplo 5.3.3 *Se* $\mathbb{K}=\mathbb{Q}(\zeta_9)$, *então* $[\mathbb{K}:\mathbb{Q}]=6$ *e seu anel de inteiros algébricos é* $\mathbb{A}_{\mathbb{K}}=\mathbb{Z}[\zeta_9]$. *Seja* $\mathfrak{p}=(1-\zeta_9)^2\mathbb{A}_{\mathbb{K}}$. *Se* $x\in\mathfrak{p}$, *então*

$$x=(1-2\zeta_9+\zeta_9^2)(a_0+a_1\zeta_9+a_2\zeta_9^2+a_3\zeta_9^3+a_4\zeta_9^4+a_5\zeta_9^5)$$

e seu conjugado é

$$\overline{x}=(1-2\zeta_9^{-1}+\zeta_9^{-2})(a_0+a_1\zeta_9^{-1}+a_2\zeta_9^{-2}+a_3\zeta_9^{-3}+a_4\zeta_9^{-4}+a_5\zeta_9^{-5}).$$

Fazendo $x\overline{x}$ *obtemos que,*

$$\begin{aligned}x\overline{x}=&(6a_0^2-9a_0a_1+6a_1^2+\ldots+6a_5^2)+(-5a_0^2+11a_0a_1-5a_1^2+\ldots-5a_5^2)\zeta_9+\\&+(5a_0^2-11a_0a_1+5a_1^2+\ldots+5a_5^2)\zeta_9^2+(-a_0^2+4a_0a_1-a_1^2+\ldots-a_5^2)\zeta_9^4+\\&+(4a_0^2-7a_0a_1+4a_1^2+\ldots+4a_5^2)\zeta_9^5.\end{aligned}$$

Como $mdc(1,9)=mdc(2,9)=mdc(4,9)=mdc(5,9)=1<3$, *assim pelo Lema 4.3.1, segue que*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 6(6a_0^2 - 9a_0a_1 + 6a_1^2 + \ldots + 6a_5^2).$$

Tomando $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), x \in \mathfrak{p}, x \neq 0\}$, *temos que* $t = 18$, *com* $a_0 = 1$, $a_4 = a_5 = -1$ *e* $a_1 = a_2 = a_3 = 0$. *Como* $D_{\mathbb{K}} = -3^9$ *e* $N(\mathfrak{p}) = 3^2$, *obtemos que a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{p})$ *é dada por*

$$\delta(\sigma_{\mathbb{K}}(1-\zeta_9)^2) = \frac{3^6}{2^2 3^{13/2}} = \frac{1}{8\sqrt{3}} \approx 0,07217,$$

que é maior densidade de centro em dimensão 6, *que corresponde a densidade de centro do reticulado* Λ_6.

Teorema 5.3.2 *([8], p.48) Se* $r = 2, p > 2$ *e* $\mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *então a maior densidade de centro dos reticulados* $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, *para* $i = 1, \cdots, p$, *ocorre com* $i = 2$.

Demonstração: Mostramos que para $i = 2, \cdots, p$, o menor valor assumido por $\tilde{Q}_r(x)$ para $x \in \mathfrak{p}^i$ é 2p. Começamos com o caso $i = 2$ e sejam x um elemento de $\mathfrak{p}^2$ e os $x_i's$ como na Proposição 4.3.2. Se apenas um dos $x_i's$ é não nulo, então, pela Proposição 4.2.2, temos que

$$\tilde{Q}_r(x) \geq 2p,$$

para $x \in \mathfrak{p}$. Para $a \in \mathbb{Z}^{p-1}$ temos que o menor valor que $Q(a)$ assume é $p-1$. Assim, se o número dos $x_i's$ não nulos for maior do que 2, então $\tilde{Q}_r(x) \geq 3(p-1) \geq 2p$, uma vez que, $\tilde{Q}_r(x) = Q_{p-1}(x_0) + \cdots + Q_{p-1}(x_t)$, com $t = p^{r-1} - 1$, e portanto

$$\begin{aligned}\tilde{Q}_r(x) &= Q_{p-1}(a_0, a_{p^{r-1}}, \cdots, a_{(p-2)p^{r-1}}) + \cdots + Q_{p-1}(a_t, a_{p^{r-1}+t}, \cdots, a_{(p-2)p^{r-1}+t}) \geq \\ &\geq p-1+p-1+p-1 = \\ &= 3(p-1) \geq 2p.\end{aligned}$$

Assim, resta mostrar o caso em que apenas dois dos $x_i's$ não são nulos, digamos x_i e x_j. Mostramos, primeiramente, que neste caso $\tilde{Q}_r(x)$ não atinge o valor $2(p-1)$. Se isto ocorre, temos que $Q(x_i) = Q(x_j) = p-1$ e isto ocorre apenas nos casos seguintes:

1º caso : Se $x_i = \pm e_l$ e $x_j = \pm e_s$, então podemos supor, sem perda de generalidade, que $x_i = e_l$ e $x_j = -e_s$. Logo, existem a, $b \in \mathbb{N}$ tal que

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^a - \zeta_{p^r}^b = \zeta_{p^r}^a(1 - \zeta_{p^r}^{b-a}) = f(\zeta_{p^r}),$$

onde $f(x) = x^a - x^b$. Como $x \in \mathfrak{p}^2$, segue que pela Proposição 4.3.1, que

$$f'(1) \equiv a - b \equiv 0(mod\, p).$$

Como estamos considerando apenas dois dos $x_i's$ não nulos, segue que $a - b \equiv 0(mod\, p)$ não ocorre, o que é uma contradição.

2º caso : Se $x_i = (1, 1, \ldots, 1)$ e $x_j = \pm e_s$, temos que se $x \in \mathfrak{p}$ então $x_j = e_s$. Logo x é da forma

$$x = \xi_{p^r}^i x_i + \xi_{p^r}^j x_j = \xi_{p^r}^i + \xi_{p^r}^{p+i} + \cdots + \xi_{p^r}^{(p-2)p+i} + \xi_{p^r}^{j+s} = f(\xi_{p^r}),$$

onde $f(x) = x^i + \cdots + x^{j+s}$. Se $x \in \mathfrak{p}^2$, pela Proposição 4.3.1, segue que

$$f'(1) \equiv i + \cdots + (p-2)p + i + j + s \equiv i - j \equiv 0(mod\, p),$$

o que não ocorre, pois $i,\, j \in \{0, \cdots, p-1\}$.

3º caso : Se $x_i = (1, 1, \ldots, 1)$ e $x_j = \pm(-1, -1, \cdots, -1)$, então $x_j = (-1, -1, \cdots, -1)$ e

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} - \zeta_{p^r}^j - \cdots - \zeta_{p^r}^{(p-2)p+j} = f(\zeta_{p^r}),$$

onde $f(x) = x^i + \cdots + x^{(p-2)p+i} - x^j + \cdots + x^{(p-2)p+j}$. Se $x \in \mathfrak{p}^2$, então

$$f'(1) \equiv i - j \equiv 0(mod\, p),$$

o que novamente não ocorre.

Mostramos, assim, que para $x \in \mathfrak{p}^2$ e dois $x_i's$ não nulos, o valor $2(p-1)$ não é atingido por $\tilde{Q}_r(x)$. Mas, pelo Lema 1.6.1, o valor $2p-1$ também não é atingido, e portanto para $x \in \mathfrak{p}^2$ tem-se que $\tilde{Q}_r(x) \geq 2p$. Observe que o elemento $x = 1 - \zeta_{p^r}^p$ pertence a $\mathfrak{p}^i$, para $i = 1, \cdots, p$, e $\tilde{Q}_r(x) = 2p$. Como $|\sigma_{\mathbb{K}}(x)|^2 = \dfrac{p^{r-1}}{2}\tilde{Q}_r(x)$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}2p = p^r,$$

o que implica que $\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \dfrac{1}{2}min\{|\sigma(x)|,\, x \neq 0,\, x \in \mathfrak{p}^i\} = \dfrac{\sqrt{p^r}}{2}$, para $i = 1, 2, \cdots, p$. Como o ideal de menor norma é $\mathfrak{p}^2$, segue que $\sigma_K(\mathfrak{p}^2)$ tem a maior densidade de centro. Assim, para $i = 1, \cdots, p$, a maior densidade de centro é obtida em $\sigma_{\mathbb{K}}(\mathfrak{p})$ ou $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$. Para $r = 2$, temos que

$$\frac{\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2))}{\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))} = \left(\frac{p}{p-1}\right)^{\frac{(p-1)p}{2}-1} > 1.$$

Logo, $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$ é o mais denso dentre os reticulados considerados, e sua densidade de centro é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2)) = \frac{p^{(p-1)p}}{2^{\frac{(p-1)p}{2}}|D_{\mathbb{K}}|^{\frac{1}{2}}p^2},$$

o que conclui a demonstração. □

5.4 Reticulados via $\mathbb{Q}(\zeta_{pq})$

Nesta seção, apresentamos resultados que permitem calcular a densidade de centro de reticulados obtidos via as extensões ciclotômicas $\mathbb{Q}(\zeta_{pq})$, com p e q primos distintos. Em particular, apresentamos um resultado que permite encontrar reticulados de dimensão 8 com densidade de centro ótima, através de subcorpos de $\mathbb{Q}(\zeta_{pq})$.

Quando tratamos de ideais no anel de inteiros algébricos de corpos de números $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$, com p e q números primos distintos, a fatoração dos ideais $p\mathbb{A}_{\mathbb{L}}$ ou $q\mathbb{A}_{\mathbb{K}}$ em produtos de ideais primos de $\mathbb{A}_{\mathbb{L}}$ assume algumas particularidades interessantes. Vamos denotar o grupo de decomposição de um ideal de $\mathbb{A}_{\mathbb{L}}$ acima de $p\mathbb{Z}$ por $D_{\mathbb{L}}(p)$, enquanto que $D_{\mathbb{K}}(p)$ irá representar o grupo de decomposição de um ideal acima de $p\mathbb{Z}$ em $\mathbb{K} = \mathbb{Q}(\zeta_p)$.

Observação 5.4.1 *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$ e $\mathbb{A}_{\mathbb{L}}$ seu anel de inteiros algébricos, $\overline{\sigma}$ a conjugação complexa de $\mathbb{Q}(\zeta_{pq})$ e $p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_g)^e$, como na Proposição 3.2.3. Quando $\overline{\sigma}$ não pertence ao grupo $D_{\mathbb{L}}(p)$, então para cada $i = 1,\ldots,g$, existe um único índice $k\,, k \neq i$, tal que $\overline{\sigma}(\mathfrak{p}_i) = \overline{\mathfrak{p}_i} = \mathfrak{p}_k$. Neste caso, $\overline{\sigma}(\overline{\mathfrak{p}_i}) = \mathfrak{p}_i$. Aplicando $\overline{\sigma}$ ao ideal $p\mathbb{A}_{\mathbb{L}}$ obtemos,*

$$p\mathbb{A}_{\mathbb{L}} = (\overline{\mathfrak{p}_1\mathfrak{p}_2}\ldots\overline{\mathfrak{p}_g})^e.$$

Podemos supor $\overline{\mathfrak{p}_g} = \mathfrak{p}_1$, $\overline{\mathfrak{p}_{g-1}} = \mathfrak{p}_2$, e assim sucessivamente. Reordenando os ideais de maneira conveniente, obtemos

$$p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_{g/2}\overline{\mathfrak{p}_1\mathfrak{p}_2}\ldots\overline{\mathfrak{p}_{g/2}})^e.$$

Deste modo, para saber em que situações teremos a fatoração acima, precisamos caracterizar quando $\overline{\sigma}$ pertence ao grupo de decomposição.

Proposição 5.4.1 *([8], p.70) Com as notações acima, $\overline{\sigma}$ pertence a $D_{\mathbb{L}}(p)$ se, e somente se, $\overline{\sigma}$ pertence a $D_{\mathbb{K}}(p)$.*

Demonstração: Seja $\sigma_i \in D_{\mathbb{K}}(q)$ definido por $\sigma_i(\zeta_p^i)$. Para cada $\sigma_i \in D_{\mathbb{K}}(q)$, tem-se que existem $q-1$ extensões $\sigma_{i,j}$ de $D_{\mathbb{L}}(q)$. Cada σ_{ij} é definido por seu valor em ζ_{pq}. Sejam u e v tais que $1 = pu + qv$. Desse modo, segue que

$$\sigma_{i,j}(\zeta_{pq}) = \sigma_{i,j}(\zeta_{pq}^{pu+qv}) = \sigma_{i,j}(\zeta_{pq}^{pu})\sigma_{i,j}(\zeta_{pq}^{qv}) = \sigma_{i,j}(\zeta_q^u)\sigma_{i,j}(\zeta_p^v) = \zeta_q^{uj}\zeta_p^{vi} = \zeta_{pq}^{puj+qvi}.$$

Assim, $\overline{\sigma} \in D_{\mathbb{L}}(q)$ se, e somente se, existem i, j tais que $puj + qvi \equiv -1 (mod\, pq)$, ou seja, $puj + qvi \equiv -1 (mod\, p)$ e $puj + qvi \equiv -1 (mod\, q)$. Note que, o segundo caso sempre vale, já que j pode assumir qualquer valor não nulo módulo q. Ja o primeiro caso, é equivalente a $\overline{\sigma} \in D_{\mathbb{K}}(p)$, assim concluímos a prova. □

Corolário 5.4.1 *([8], p.71) A conjugação complexa $\overline{\sigma}$ pertence a $D_{\mathbb{L}}(p)$ se, e somente se, $o_q(p) \equiv 0 (mod\, 2)$*

Exemplo 5.4.1 *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{21})$, $p = 7$ e $q = 3$. Como $o_3(7) = 1$, segue pelo Corolário 5.4.1, que $\overline{\sigma}$ não pertence a $D_{\mathbb{K}}(7)$. Assim, o ideal $7\mathbb{A}_{\mathbb{K}}$ se decompõe como na Observação 5.4.1. Agora como $o_7(3) = 6$, segue que $\overline{\sigma}$ pertence a $D_{\mathbb{K}}(3)$, assim o ideal $3\mathbb{A}_{\mathbb{K}}$ não se decompõe como na Obseravação 5.4.1.*

Lema 5.4.1 *([8], p.77) Sejam $\mathbb{L}$ um corpo de números e $\mathbb{K}$ um subcorpo de $\mathbb{L}$ tal que $[\mathbb{L} : \mathbb{K}] = h$ seja ímpar. Se q é um número primo e se em $\mathbb{A}_{\mathbb{L}}$ a decomposição de $q\mathbb{A}_{\mathbb{L}}$ é da forma $q\mathbb{A}_{\mathbb{L}} = \mathfrak{q}_1 \dots \mathfrak{q}_{s/2}\overline{\mathfrak{q}_1 \dots \mathfrak{q}_{s/2}}$, para algum $s \in \mathbb{N}$, então a decomposição de $q\mathbb{A}_{\mathbb{K}}$ em ideias primos é da forma*

$$q\mathbb{A}_{\mathbb{K}} = \mathfrak{q}_1 \dots \mathfrak{q}_{t/2}\overline{\mathfrak{q}_1 \dots \mathfrak{q}_{t/2}},$$

para algum $t \in \mathbb{N}$.

Demonstração: Consideremos em $\mathbb{A}_{\mathbb{K}}$ um ideal primo $\mathfrak{q}$ que divide $q\mathbb{A}_{\mathbb{K}}$. Assim, $\mathfrak{q}\mathbb{A}_L = \mathfrak{b}_1 \dots \mathfrak{b}_t$, onde t divide h, ou seja, t é ímpar. Por outro lado, se $\overline{\mathfrak{q}} = \mathfrak{q}$, então $\mathfrak{b}_1 \dots \mathfrak{b}_t = \overline{\mathfrak{b}_1 \dots \mathfrak{b}_t}$, e para cada ideal $\mathfrak{b}_i$, $i = 1, \dots, t$, existe $j \neq i$ tal que $\overline{b_i} = \mathfrak{b}_j$. Assim, os ideais acima de $\mathfrak{q}$ aparecem aos pares, o que contraria a hipótese sobre a paridade de t. Logo, $\overline{\mathfrak{q}} \neq \mathfrak{q}$, e portanto o lema está provado. □

Lema 5.4.2 *([16], p.97) Sejam $\mathbb{K}$ um corpo de número, $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$ e $G = Gal(\mathbb{K}/\mathbb{Q})$. Se $\sigma(\mathfrak{a}) = \mathfrak{a}$, para todo $\sigma \in G$ e $x \in \mathfrak{a}$, então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x) \equiv 0 (mod\, r),$$

onde $r\mathbb{Z} = \mathfrak{a} \cap \mathbb{Z}$.

Sejam p e q primos distintos satisfazendo a condição $o_p(q) \equiv o_q(p) \equiv 1(mod\, 2)$ e $\mathbb{K}_1 \subseteq \mathbb{Q}(\zeta_p)$, $\mathbb{K}_2 \subseteq \mathbb{Q}(\zeta_q)$, tais que $[\mathbb{Q}(\zeta_p) : \mathbb{K}_1] = h_p$ e $[\mathbb{Q}(\zeta_q) : \mathbb{K}_2] = h_q$ sejam ímpares. Sejam ainda $[\mathbb{K}_1 : \mathbb{Q}] = n_1$ e $[\mathbb{K}_2 : \mathbb{Q}] = n_2$. O corpo $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$ tem grau n_1n_2, e sendo $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos linearmente disjuntos, ou seja, se tem discriminantes relativamente primos e satisfazem $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$, então pelos Teoremas 2.5.9 e 2.5.3 seu discriminante é dado por

$$D_{\mathbb{K}} = p^{n_2(n_1-1)} q^{n_1(n_2-1)}.$$

Em $\mathbb{K}$, sejam r_p e r_q a quantidade de primos acima de p e q, respectivamente. Sendo h_p e h_q ímpares vale as decomposições

$$p\mathbb{A}_{\mathbb{K}} = (\mathfrak{p}_1 \dots \mathfrak{q}_{r_p/2} \overline{\mathfrak{p}_1 \dots \mathfrak{p}_{r_p/2}})^{n_2}$$

$$e$$

$$q\mathbb{A}_{\mathbb{K}} = (\mathfrak{q}_1 \dots \mathfrak{q}_{r_q/2} \overline{\mathfrak{q}_1 \dots \mathfrak{q}_{r_q/2}})^{n_1}.$$

Seja $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_{r_p/2} \mathfrak{q}_1 \dots \mathfrak{q}_{r_q/2}$. Sua norma é $N(\mathfrak{a}) = p^{n_2/2} q^{n_1/2}$, e se $x \in \mathfrak{a}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{h_p h_q} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x})$. Como h_p e h_q são ímpares e em $\mathbb{Z}[\zeta_{pq}]$, a forma quadrática pela Proposição 4.4.1, é par, segue pelo Lema 5.4.2, que $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 2pq$. Com isso a expressão para a densidade de centro é dada por:

$$\delta = \frac{(2pq)^{n_1n_2/2}}{p^{n_2(n_1-1)/2} q^{n_1(n_2-1)/2} p^{n_2/2} q^{n_1/2} 2^{n_1n_2}} = \frac{1}{2^{n_1n_2/2}}. \tag{5.2}$$

Assim, quando $n_1n_2 = 8$ a densidade de centro é $\delta = \dfrac{1}{16} = 0,06250$, que é a mesma densidade de centro do reticulado E_8. A seguir construiremos alguns reticulados de dimensão 8 que possuem densidade de centro ótimo.

Exemplo 5.4.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{55})$, $\mathbb{K}_1 = \mathbb{Q}(\zeta_5)$ *e* $\mathbb{K}_2 \subset \mathbb{Q}(\zeta_{11})$ *de modo que* $[\mathbb{Q}(\zeta_{11}) : \mathbb{K}_2] = 5$. *Assim, tomando* $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$ *temos que* $[\mathbb{K} : \mathbb{Q}] = 8$. *O polinômio minimal de* ζ_{55} *sobre* $\mathbb{Q}$ *é dado por*

$$f(x) = x^{40} - x^{39} + x^{35} - x^{34} + \ldots + x^{10} - x^6 + x^5 - x + 1.$$

Agora vamos fatorar os ideais $5\mathbb{A}_{\mathbb{L}}$ *e* $11\mathbb{A}_{\mathbb{L}}$ *em produto de ideias primos utilizando o Lema de Kummer. Assim*

(a) $f(x) \equiv p_1(x)^4 p_2(x)^4 (mod\, 5\mathbb{Z}[x])$, *onde*

$$p_1(x) = x^5 + 4x^4 + 4x^3 + x^2 + 3x + 4$$

e

$$p_2(x) = x^5 + 2x^4 + 4x^3 + x^2 + x + 4,$$

com $g = 2$, $e_1 = e_2 = 4$ *e* $f_1 = f_2 = 5$. *Logo* $\mathfrak{p}_1 =< 5, p_1(\zeta_{55}) >$ *e* $\mathfrak{p}_2 =< 5, p_2(\zeta_{55}) >$. *Portanto,* $5\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2)^4$.

(b) $f(x) \equiv q_1(x)^{10} q_2(x)^{10} q_3(x)^{10} q_4(x)^{10} (mod\, 11\mathbb{Z}[x])$, *onde*

$$q_1(x) = x + 2 \ , \ q_2(x) = x + 6$$

e

$$q_3(x) = x + 7 \ , \ q_4(x) = x + 8,$$

com $g = 4$, $e_1 = e_2 = e_3 = e_4 = 10$ *e* $f_1 = f_2 = f_3 = f_4 = 1$. *Logo* $\mathfrak{q}_1 =< 11, q_1(\zeta_{55}) >$, $\mathfrak{q}_2 =< 11, q_2(\zeta_{55}) >$, $\mathfrak{q}_3 =< 11, q_3(\zeta_{55}) >$ *e* $\mathfrak{q}_4 =< 11, q_4(\zeta_{55}) >$. *Portanto,* $11\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4)^{10}$. *Como*

$$o_5(11) = 1 \equiv 1 (mod\, 2) \text{ e } o_{11}(5) = 5 \equiv 1 (mod\, 2),$$

segue pelo Corolário 5.4.1, que a conjugação $\overline{\sigma} \notin D_{\mathbb{L}}(5)$ *e* $\overline{\sigma} \notin D_{\mathbb{L}}(11)$, *como* $\mathfrak{q}_2 = \overline{\mathfrak{q}_1}$, $\mathfrak{q}_4 = \overline{\mathfrak{q}_3}$ *e* $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$, *segue que* $5\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\overline{\mathfrak{p}_1})^4$ *e* $11\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_3\overline{\mathfrak{q}_1\mathfrak{q}_3})^{10}$. *Agora, como* $[\mathbb{K}_1 : \mathbb{Q}] = 4$ *e* $[\mathbb{K}_2 : \mathbb{Q}] = 2$, *consideremos as decomposições em* $\mathbb{A}_{\mathbb{K}}$ *da seguinte forma,* $5\mathbb{A}_{\mathbb{K}} = (\mathfrak{p}_1\overline{\mathfrak{p}_1})^4$ *e* $11\mathbb{A}_{\mathbb{K}} = (\mathfrak{q}_1\mathfrak{q}_3\overline{\mathfrak{q}_1\mathfrak{q}_3})^2$. *Se* $\mathfrak{a} = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{q}_3 \subset \mathbb{A}_{\mathbb{K}}$, *então sua*

norma é $N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{q}_1)N(\mathfrak{q}_3) = 5.11.11 = 5.11^2$. *Como* $\sigma(\mathfrak{a}\overline{\mathfrak{a}}) = \mathfrak{a}\overline{\mathfrak{a}}$, *segue pelo Lema 5.4.2, que para* $x \in \mathfrak{a}$ *tem-se que* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \in \mathfrak{a}\overline{\mathfrak{a}} \cap \mathbb{Z} = 55\mathbb{Z}$, *ou seja,* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 55h$, *com* $h \in \mathbb{N}$. *Pela Proposição 4.4.1, como* $p = 5$ *e* $q = 11$ *segue que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ *é par. Logo,* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{5}Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ *também é par, e assim* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 2.55$. *Determinamos, agora uma base para* $\mathbb{K}$. *Como* $\mathbb{K}_1 = \mathbb{Q}(\zeta_5)$, *segue que*

$$B_1 = \{1, \zeta_5, \zeta_5^2, \zeta_5^3\} = \{1, \zeta_{55}^{11}, \zeta_{55}^{22}, \zeta_{55}^{33}\}$$

é uma base para $\mathbb{K}_1$. *Agora, como* $\mathbb{K}_2 \subset \mathbb{Q}(\zeta_{11})$, *segue pelo Teorema 2.6.2 que,* $\mathbb{K}_2 = \mathbb{Q}(\theta)$, *onde*

$$\theta = \zeta_{11} + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9.$$

Logo uma base para $\mathbb{K}_2$ *é*

$$B_2 = \{1, \zeta_{11} + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9\} = \{1, \zeta_{55}^5 + \zeta_{55}^{15} + \zeta_{55}^{20} + \zeta_{55}^{25} + \zeta_{55}^{45}\}.$$

Portanto, tem-se que $B = B_1 \times B_2$ *é uma base para* $\mathbb{K}$, *onde*

$$\begin{aligned} B = \{&1, \zeta_{55}^5 + \zeta_{55}^{15} + \zeta_{55}^{20} + \zeta_{55}^{25} + \zeta_{55}^{45}, \zeta_{55}^{11}, \zeta_{55}^{16} + \zeta_{55}^{26} + \zeta_{55}^{31} + \zeta_{55}^{36} + \zeta_{55}, \zeta_{55}^{22}, \\ &\zeta_{55}^{27} + \zeta_{55}^{37} + \zeta_{55}^{42} + \zeta_{55}^{47} + \zeta_{55}^{12}, \zeta_{55}^{33}, \zeta_{55}^{38} + \zeta_{55}^{48} + \zeta_{55}^{53} + \zeta_{55}^{3} + \zeta_{55}^{23}\}. \end{aligned}$$

Dado $x \in \mathbb{K}$, *tem-se que*

$$\begin{aligned} x = a_0 + a_1(\zeta_{55}^5 + \zeta_{55}^{15} + \zeta_{55}^{20} + \zeta_{55}^{25} + \zeta_{55}^{45}) + a_2\zeta_{55}^{11} + a_3(\zeta_{55}^{16} + \zeta_{55}^{26} + \zeta_{55}^{31} + \zeta_{55}^{36} + \zeta_{55}) + a_4\zeta_{55}^{22} + \\ + a_5(\zeta_{55}^{27} + \zeta_{55}^{37} + \zeta_{55}^{42} + \zeta_{55}^{47} + \zeta_{55}^{12}) + a_6\zeta_{55}^{33} + a_7(\zeta_{55}^{38} + \zeta_{55}^{48} + \zeta_{55}^{53} + \zeta_{55}^{3} + \zeta_{55}^{23}). \end{aligned}$$

Usando os fatos que $\overline{\zeta_{55}} = \zeta_{55}^{-1}$ *e que* $\zeta_{55}^{40} = \zeta_{55}^{39} - \zeta_{55}^{35} + \zeta_{55}^{34} + \ldots - \zeta_{55}^5 + \zeta_{55} - 1$, *tem-se que*

$$\begin{aligned} x\overline{x} = (a_0^2 - a_0a_1 + \ldots + 3a_7^2) + (-a_1a_2 + a_1a_2 + \ldots + a_4a_7)\zeta_{55} + a_5a_7\zeta_{55}^3 + \\ + (a_1a_2 - a_2a_3 + \ldots - a_4a_7)\zeta_{55}^4 + \ldots + (-2a_1a_4 + 2a_0a_5 + \ldots - a_5a_7)\zeta_{55}^{39}. \end{aligned}$$

Usando o Lema 4.4.1, obtemos que

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = &8a_0^2 - 8a_0a_1 + 24a_1^2 - 4a_0a_2 + 2a_1a_2 + \ldots + \\ &+ 2a_4a_7 - 12a_5a_7 - 8a_6a_7 + 24a_7^2 \geq 2.55. \end{aligned}$$

Tomando $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})\,;\, x \in \mathfrak{a}\, e\, x \neq 0\}$, *temos que* $t = 110$, *com* $a_0 = a_4 = -1$, $a_1 = a_3 = a_5 = a_6 = 1$, $a_2 = 2$ *e* $a_7 = 0$. *Pelos Teoremas 2.5.3 e 2.5.9 tem-se que* $D_{\mathbb{K}} = 5^6 11^4$, *portanto pela Observação 3.4.2, segue que a densidade de centro do reticulado algébrico* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é:*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{1}{2^4} = 0,0625.$$

Exemplo 5.4.3 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{259})$, $\mathbb{K}_1 \subset \mathbb{Q}(\zeta_7)$, $\mathbb{K}_2 \subset \mathbb{Q}(\zeta_{37})$, *de modo que,* $[\mathbb{Q}(\zeta_7) : \mathbb{K}_1] = 3$, $[\mathbb{Q}(\zeta_{37}) : \mathbb{K}_2] = 9$. *Assim,* $[\mathbb{K}_1 : \mathbb{Q}] = 2$ *e* $[\mathbb{K}_2 : \mathbb{Q}] = 4$. *Tomando* $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$, *tem-se que* $[\mathbb{K} : \mathbb{Q}] = 8$. *O polinômio minimal de* ζ_{259} *sobre* $\mathbb{Q}$ *é dado por*

$$f(x) = x^{216} - x^{215} + x^{209} + \ldots + x^7 - x + 1.$$

Agora, vamos fatorar os ideais $7\mathbb{A}_{\mathbb{L}}$ *e* $37\mathbb{A}_{\mathbb{L}}$ *em produto de ideais primos, utilizando o Lema de Kummer. Assim,*

(a) $f(x) \equiv p_1(x)^6 p_2(x)^6 p_3(x)^6 p_4(x)^6 (mod\, 7\mathbb{Z}[x])$, *onde*

$$p_1(x) = x^9 + 3x^6 + 4x^5 + 4x^4 + 2x^3 + 2x^2 + 5x + 6,$$

$$p_2(x) = x^9 + x^7 + 2x^6 + 2x^5 + 2x^4 + 6x^3 + 3x^2 + x + 6,$$

$$p_3(x) = x^9 + 2x^8 + 5x^7 + 5x^6 + 3x^5 + 3x^4 + 4x^3 + 6$$

e

$$p_4(x) = x^9 + 6x^8 + 4x^7 + x^6 + 5x^5 + 5x^4 + 5x^3 + 6x^2 + 6,$$

com $g = 4$, $e_1 = e_2 = e_3 = e_4 = 6$ *e* $f_1 = f_2 = f_3 = f_4 = 9$. *Deste modo, tem-se que* $\mathfrak{p}_i =< 7, p_i(\zeta_{259}) >$, *para* $i = 1, 2, 3, 4$. *Portanto,* $7\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^6$.

(b) $f(x) \equiv q_1(x)^{36} q_2(x)^{36} (mod\, 37\mathbb{Z}[x])$, *onde*

$$q_1(x) = x^3 + 9x^2 + 8x + 36$$

e

$$q_2(x) = x^3 + 29x^2 + 28x + 36,$$

com $g = 2$, $e_1 = e_2 = 36$ *e* $f_1 = f_2 = 3$. *Deste modo, tem-se que* $\mathfrak{q}_i =< 37, q_i(\zeta_{259}) >$, *para* $i = 1, 2$. *Portanto,* $37\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_2)^{36}$.

Agora, como $o_{37}(7) = 9 \equiv 1(mod\,2)$ *e* $o_7(37) = 3 \equiv 1(mod\,2)$, *segue pelo Corolário 5.4.1 que a conjugação* $\overline{\sigma} \notin D_{\mathbb{L}}(7)$ *e* $\overline{\sigma} \notin D_{\mathbb{L}}(37)$. *Como* $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$, $\mathfrak{p}_4 = \overline{\mathfrak{p}_3}$ *e* $\mathfrak{q}_2 = \overline{\mathfrak{q}_1}$, *segue que* $7\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_3\overline{\mathfrak{p}_1\mathfrak{p}_3})^6$ *e* $37\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\overline{\mathfrak{q}_1})^{36}$. *Pelo Lema 5.4.1, tomamos as decomposições em* $\mathbb{A}_{\mathbb{K}}$ *da seguinte forma,* $7\mathbb{A}_{\mathbb{K}} = (\mathfrak{p}_1\mathfrak{p}_3\overline{\mathfrak{p}_1\mathfrak{p}_3})^4$ *e* $37\mathbb{A}_{\mathbb{K}} = (\mathfrak{q}_1\overline{\mathfrak{q}_1})^2$. *Tomando* $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_3\mathfrak{q}_1 \subset \mathbb{A}_{\mathbb{K}}$, *tem-se que* $N(\mathfrak{a}) = 7^2 37$. *Usando o mesmo raciocínio do Exemplo 5.4.2, tem-se que* $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})\,;\, x \in \mathfrak{a}\, e\, x \neq 0\} = 2.7.37$. *Como* $D_{\mathbb{K}/\mathbb{Q}} = 7^4 37^6$, *segue que a densidade de centro do reticulado algébrico* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})} = \frac{\left(\frac{2.7.37}{4}\right)^{\frac{8}{2}}}{|7^4 37^6|^{\frac{1}{2}}7^2 37} = \frac{1}{2^4} = 0,0625.$$

De modo análogo aos Exemplos 5.4.2 e 5.4.3, é possível obter reticulados algébricos, com densidade de centro igual ao do reticulado E_8, para os seguintes pares de primos distintos da seguinte tabela.

(p,q)	(p,q)	(p,q)
(7,37)	(7,109)	(11,157)
(11,317)	(19,101)	(19,149)
(19,157)	(19,227)	(23,29)
(23,173)	(23,197)	(23,269)
(23,317)	(31,101)	(31,149)
(31,317)	(43,181)	(43,229)
(43,317)	(47,53)	(47,61)
(47,157)	(47,173)	(47,269)

5.5 Conclusão

O objetivo deste trabalho, foi construir reticulados algébricos de dimensão 1 à 8 com densidade de centro ótima. Porém, conseguimos obter apenas reticulados

algébricos com densidade de centro ótima para dimensão $2, 4, 6$ e 8, já para dimensão $3, 5$ e 7 não foi possível. Assim, fica como objetivo para os próximos trabalhos, encontrar métodos que ajudem a encontrar estes reticulados. Além disto, um dos objetivos para trabalhos futuros é melhorar a densidade centro, para reticulados com dimensão acima de 8. Vale ressaltar que o uso do software MATHEMATICA, será muito útil para este objetivo.

Referências Bibliográficas

[1] SAMUEL, P. **Algebric Theory of Numbers**. Paris: Hermann, 1970.

[2] STEWART, I. N. TALL, D. O. **Algebraic Number Theory**. London: Chapman and Hall, 1987.

[3] FLORES, A. L. **Representação Geométrica de Ideais de Corpos de Números.** 1996. 86f. Dissertação (Mestrado em Matemática) - Instituto de Matemática, Estatística e de Computação Científica, Universidade Estadual de Campinas, Campinas, 1996.

[4] GARCIA, A.; LEQUAIN, Y. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 2002.

[5] MONTEIRO, L. H. J. **Teoria de Galois**. In: Colóquio Brasileiro de Matemática, 7, 1969. Poços de Caldas. Atas ... Rio de Janeiro: IMPA, 1969.

[6] LANG, S. **Álgebra**. New York: Springer-Verlag, 2002.

[7] QUILLES, C. R. O. **Discriminante de Corpos de Números**. 2006. 140f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2006.

[8] FLORES, A. L. **Reticulados em Corpos Abelianos**. 2000. 129. Dissertação (Doutorado em Engenharia Elétrica) - Faculdade de En-

genharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, 2000.

[9] SIMONATO, A. L. **Reticulados em Corpos Ciclotômicos**. 2000. 66f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2000.

[10] WASHINGTON, L. **Introduction to Cyclotomic Fields**. New York: Springer-Verlag, 1982.

[11] MARCUS, D. A. **Number Fields**. New York: Springer-Verlag, 1977.

[12] ENDLER, O. **Teoria dos Números Algébricos**. Rio de Janeiro: IMPA, 1986.

[13] Ferrari, A.J. **Reticulados Algébricos via Corpos Abelianos**. 2008. 115f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[14] CONWAY, J.H.; SLOANE, N. J. A. **Sphere Packing, Lattices and Groups**. New York: Springer-Verlag, 1999

[15] ALVES, C. **Reticulados via Corpos Ciclotômicos**. 2005. 140f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[16] Carvalho, M.F.C. **Representação Geométrica de Ideais**. 2004. 110f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2004.

[17] BOUTROS, J; VITERBO, E.; RATELLO, C.; BELFIORE, J. C. Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels. **IEEE Transactions Information Theory**, New-York, v.42, No. 2, p. 502-518, Março 1996.

[18] NOBREGA, T. P. N.; INTERLANDO, J.C.; FLORES, A. L. **Families of Lattices from Subfields of $\mathbb{Q}(\zeta_{pq})$ and Their Applications to Rayleigh Fading Channels**; Proceedings of the International Telecommunications Symposium; 2002, Natal - RN; Brasil.