



Universidade Estadual Paulista

Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Wanderson Tenório

Reticulados modulares em
espaços euclidianos

São José do Rio Preto

2013

Wanderson Tenório

Reticulados modulares em espaços euclidianos

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

Orientador: Prof.º Dr. Antonio Aparecido de Andrade

São José do Rio Preto
2013

Wanderson Tenório

Reticulados modulares em espaços euclidianos

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

BANCA EXAMINADORA:

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

Prof.º Dr. Edson Donizete de Carvalho
UNESP-Ilha Solteira

Prof.º Dr. Clotilzio Moreira dos Santos
UNESP-São José do Rio Preto

São José do Rio Preto, 22 de fevereiro de 2013.

Ao meu querido avô,
Antônio (*in memoriam*)
dedico.

Agradecimentos

Com a realização deste trabalho agradeço:

À minha família, especialmente, aos meus pais, Moisés e Fátima, ao meu irmão William, à avó Arlinda e meus tios, Gilmar e Sueli, por darem sempre o incentivo e suporte necessários aos meus estudos, que culminam com a escrita e defesa deste trabalho.

À Daniella pelo carinho, compreensão e amor, que fizeram que meus dias se tornassem melhores durante essa jornada.

Ao Prof.^o Dr. Antonio Aparecido de Andrade, pela confiança, paciência e ajuda desde meus primeiros passos na graduação. Externo aqui minha gratidão pelas oportunidades de aprendizado, acadêmicas e pessoais, proporcionadas por ele a mim.

À Prof.^a Eva Bayer-Fluckiger, sua secretária Monique Kiener e seus assistentes pela hospitalidade e disposição com que me receberam na École Polytechnique Fédérale de Lausanne, fazendo que minha estada em Lausanne-Suíça fosse bastante proveitosa em todos os sentidos.

À banca examinadora: Prof.^o Dr. Edson Donizete de Carvalho e Prof. Dr.^o Clotilzio Moreira dos Santos, pela gentileza em participar da avaliação deste trabalho.

Aos companheiros de morada, Rafael, Fábio, Guilherme, Gilberto, Roberto, Everton e William que tornaram mais agradável e proveitoso o período que estive em São José do Rio Preto.

A todos meus amigos que de alguma forma contribuíram não somente para a conclusão deste trabalho mas também para o meu crescimento como pessoa.

À FAPESP, pelo suporte financeiro dado aos processos 2010/13178-4 de Mestrado e ao processo 2012/00867-1 de Estágio de Pesquisa no Exterior, realizado no período de 01/06/2012 a 30/09/2012 na École Polytechnique Fédérale de Lausanne na Suíça.

Aos professores do Departamento de Matemática do IBILCE.

“Tenho pensamentos que, se pudesse revelá-los e fazê-los viver, acrescentariam nova luminosidade às estrelas, nova beleza ao mundo e maior amor ao coração dos homens.”

(Fernando Pessoa)

Resumo

O objetivo deste trabalho é apresentar resultados sobre modularidade de reticulados. Mais especificamente, apresentamos as propriedades de um reticulado modular num espaço euclidiano arbitrário e a relação entre as theta séries de reticulados modulares pares e formas modulares. Além disso, apresentamos o estudo de modularidade em reticulados ideais fornecendo condições de existência, construções e caracterização de reticulados ideais modulares para graus especiais em corpos ciclotômicos.

Palavras chave: reticulados, reticulados modulares, reticulados ideais.

Abstract

The aim of this work is to show results about modularity of lattices. More specifically, we show the properties of a modular lattice in an arbitrary Euclidean space and the relationship between theta series of even modular lattices and modular forms. Moreover, we show the study of modularity in ideal lattices giving existence conditions, constructions and characterization of modular ideal lattices for special levels over cyclotomic fields.

Key words: lattices, modular lattices, ideal lattices.

Lista de símbolos

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

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

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

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

$\mathbb{R}_+^\times$: conjunto dos números reais positivos (maiores que 0)

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

i : número complexo $\sqrt{-1}$

$\bar{x}$: conjugado complexo de x

$\#C$: cardinalidade do conjunto C

$R, \mathcal{O}, \mathfrak{o}$: anéis

$\mathfrak{a}, \mathfrak{p}, \mathfrak{P}, \mathfrak{I}, \mathfrak{Q}$: ideais

$R^\times$: conjunto das unidades do anel R

M, N : R -módulos

$\text{Hom}_R(M, N)$: conjunto dos homomorfismos de R -módulos

$\text{End}_R(M)$: conjunto $\text{Hom}_R(M, M)$

(a_{ij}) : matriz

$\det(a_{ij})$: determinante da matriz (a_{ij})

$M_n(\mathbb{Z})$: conjunto das matrizes quadradas $n \times n$ com entradas em $\mathbb{Z}$

$\text{GL}_n(\mathbb{Z})$: conjunto das matrizes de $M_n(\mathbb{Z})$ com determinante não nulo

G, H : grupos

$(G : H)$: índice de grupos

K, L, F : corpos

$K|F$: extensão de corpos

$[K : F]$: grau da extensão de corpos $K|F$

$\text{Tr}_{K|F}(x)$: traço do elemento x na extensão $K|F$

$N_{K|F}(x)$: norma do elemento x na extensão $K|F$

$N(\mathfrak{a})$: norma do ideal $\mathfrak{a}$

$\mathcal{O}_K$: anel de inteiros de um corpo de números K

d_K : discriminante do corpo de números K

$\mathcal{D}_{K|F}$: diferente da extensão $K|F$

$\mathcal{D}_{K|F}^{-1}$: codiferente da extensão $K|F$

$\phi(n)$: função de Euler do natural n

Introdução

Um reticulado modular é um reticulado integral que satisfaz uma condição de similaridade com seu reticulado dual. Tal conceito, introduzido por Quebbemman em [15], estende a bem conhecida noção de unimodularidade (ou autodualidade) e também os resultados que envolvem a theta série de um reticulado par satisfazendo tal propriedade.

Quebbemman notou que enfraquecendo a condição sobre o dual, a conexão de tais estruturas com formas modulares também se generalizava, estabelecendo que a theta série de reticulados modulares pares são formas modulares de peso $n/2$ para $\Gamma_0(\ell)$, onde n é o posto do reticulado e ℓ o grau de modularidade do reticulado. Além disso, através de uma condição mais forte em reticulados modulares, introduziu o conceito de analiticidade extrema para reticulados [16], noção que está fortemente ligada a empacotamentos esféricos densos.

A importância das ideias introduzidas por ele se deve ao fato de que, além das importantes consequências da relação com formas modulares cujos exemplos podem ser encontrados em [7], reticulados modulares tem sido utilizados numa abordagem recente como códigos Wiretap em canais Gaussianos e Rayleigh Fading.

Com base nos conceitos e resultados estabelecidos em [15], Bayer-Fluckiger aborda em [2] e [6] os aspectos de modularidade em reticulados ideais, que foram introduzidos e estudados por ela em [3] e [1]. Reticulados dados por esse caminho são ótimas ferramentas para a teoria de codificação visto que alguns parâmetros são expressos por propriedades e relações da teoria dos números algébricos. Como referência para o uso de reticulados ideais em teoria de códigos podemos citar [4] e [5]. Especificamente, nos trabalhos [2] e [6], Bayer-Fluckiger fornece construções de reticulados ideais modulares de graus especiais através de corpos ciclotômicos e resultados com condições suficientes para a existência de reticulados ideais modulares de certos graus e do tipo traço em corpos ciclotômicos.

Sendo a proposta deste trabalho o estudo de modularidade em reticulados e, especialmente, em reticulados ideais, estruturamos o texto em três capítulos da seguinte forma:

- Inicialmente fazemos uma breve discussão sobre formas bilineares e espaços euclidianos, cuja referência foi [10], e que serão usadas como preliminares para a formalização da teoria de reticulados em espaços euclidianos abstratos, onde apresentamos os conceitos relacionados com a definição de reticulados. Para o desenvolvimento das propriedades envolvidas neste estudo utilizamos como base a referência [12], no entanto, é possível encontrar tais tópicos para consulta em [7]. Também neste capítulo, apresentamos o conceito de modularidade e as propriedades básicas de reticulados com esta condição. Para isto, foram usados os artigos [15] e [16].
- No capítulo seguinte, tratamos da exposição das propriedades das theta séries de reticulados pares. Com este propósito, desenvolvemos algumas ferramentas que culminam na identidade para theta séries do reticulado e seu reticulado dual e, com as propriedades introduzidas, apresentamos brevemente os tópicos iniciais da teoria de formas modulares que nos permitem relacionar a theta série de reticulados unimodulares pares com formas modulares. Em seguida, apresentamos a generalização desta relação para reticulados modulares pares. Para esta finalidade, fizemos uso dos livros [19] e [8]. Para uma leitura mais detalhada sobre formas modulares recomendamos a referência [9].
- No capítulo final, apresentamos a teoria de reticulados ideais cujos principais resultados decorrem de [1] e [3]. Além disso, fornecemos condições de existência, construções e uma caracterização de reticulados ideais modulares de graus específicos em corpos ciclotômicos. Para isto, foram utilizados os artigos [2] e [6].

Sumário

Introdução	v
1 Reticulados	1
1.1 Formas bilineares e espaços euclidianos	1
1.2 Reticulados em espaços euclidianos	6
1.3 Isometrias, similaridades e reescalares	12
1.4 Dualidade	13
1.5 Empacotamentos	17
1.6 Modularidade	21
2 Theta séries e formas modulares	24
2.1 Theta séries	24
2.2 Theta séries como formas modulares	30
2.3 Theta séries de reticulados modulares pares	34
3 Reticulados ideais	40
3.1 Caracterização	40
3.2 Modularidade em corpos ciclotômicos	48
Conclusões e perspectivas	59
Referências	62
A Apêndice: Tópicos em teoria dos números algébricos	64
A.1 Domínios de Dedekind	64
A.2 Traços, normas e elementos integrais	66
A.3 Ramificação de ideais primos	67
A.4 Ramificação em extensões de Galois	70
A.5 Corpos de números e seus anéis de inteiros	71
A.6 Corpos ciclotômicos	73

Capítulo 1

Reticulados

Neste capítulo, abordaremos a teoria de reticulados (sob a perspectiva da teoria dos números) em espaços euclidianos abstratos. Para tal proposta, faremos uso de algumas noções e propriedades sobre módulos, formas bilineares e espaços euclidianos. Com isso, para que se tenha justificada tais terminologias ao longo do texto, desenvolvemos brevemente estes conceitos na primeira seção. De posse de tais ferramentas, iniciamos, na seção seguinte, o estudo detalhado das propriedades envolvidas com conceito de reticulado em espaços euclidianos, seguidos dos conceitos de dualidade e modularidade.

1.1 Formas bilineares e espaços euclidianos

Consideremos R um anel comutativo com unidade e M um R -módulo.

Definição 1.1.1. Uma aplicação $b : M \times M \longrightarrow R$ é chamada uma *forma bilinear de M em R* se satisfaz as seguintes condições:

- (i) para cada $x \in M$, a aplicação $y \longmapsto b(x, y)$ é R -linear;
- (ii) para cada $y \in M$, a aplicação $x \longmapsto b(x, y)$ é R -linear.

Se, além do mais, valer

$$b(x, y) = b(y, x) \text{ , para todo } x, y \in M \text{ ,}$$

a forma bilinear b em questão é dita *simétrica*.

Denotando o conjunto das formas bilineares de M em R por $L^2(M, R)$, notemos que, munido da adição e da ação de R em $L^2(M, R)$ dadas por

$$(b_1 + b_2)(x) = b_1(x) + b_2(x) \quad \text{e} \quad (\lambda b)(x) = \lambda b(x) ,$$

$L^2(M, R)$ possui a estrutura de R -módulo. Consideremos, agora, o R -módulo $\text{Hom}_R(M, R) = M^*$, chamado *módulo dual* de M . Tem-se então o seguinte resultado para M^* .

Proposição 1.1.2. *Seja M um R -módulo livre finitamente gerado. Se $\mathcal{B} = \{x_1, x_2, \dots, x_l\}$ é uma R -base de M , então $\{f_1, f_2, \dots, f_l\} \subset M^*$ é uma R -base para M^* satisfazendo $f_i(x_j) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker, para $i, j = 1, 2, \dots, l$.*

Demonstração: Seja $f \in M^*$. Assim, para $x = \sum_{i=1}^l \alpha_i x_i \in M$, com $\alpha_i \in R$, escrevendo $a_i = f(x_i)$ para $i = 1, 2, \dots, l$, segue que

$$f(x) = f\left(\sum_{i=1}^l \alpha_i x_i\right) = \sum_{i=1}^l \alpha_i f(x_i) = \sum_{i=1}^l \alpha_i a_i .$$

Portanto, tem-se que $f = \sum_{i=1}^l a_i f_i$, já que $f_i(x) = \sum_{j=1}^l \alpha_j f_i(x_j) = \alpha_i$. Agora, supondo

$$\sum_{i=1}^l \beta_i f_i = 0 ,$$

para $\beta_i \in R$ e avaliando a expressão em x_i , tem-se que $\beta_i f_i(x_i) = 0$ e, portanto, $\beta_i = 0$, para $i = 1, \dots, l$. Portanto, $\{f_1, f_2, \dots, f_l\}$ é uma base para M^* . ■

Agora, fixada uma forma bilinear $b \in L^2(M, R)$, é possível observar que a aplicação

$$\begin{aligned} \varphi_b : M &\longrightarrow M^* \\ y &\longmapsto \varphi_b(y)(x) = b(x, y) \end{aligned} \tag{1.1}$$

é um homomorfismo de R -módulos, uma vez que b é uma forma bilinear de M em R .

Definição 1.1.3. Dizemos que uma forma bilinear b de M em R é *não-degenerada* se o homomorfismo φ_b de R -módulos definido em (1.1) é um isomorfismo.

Considerando, ainda, M um R -módulo munido de forma bilinear b de M em R não-degenerada, tem-se que os R -módulos

$$\text{End}_R(M) \quad \text{e} \quad L^2(M, R) \tag{1.2}$$

são isomorfos e que dependem da forma bilinear b fixada. De fato, tomando $A \in \text{End}_R(M)$, tem-se que a aplicação $(x, y) \mapsto b(x, Ay)$ é uma forma bilinear de M em R . Reciprocamente, dado $h \in L^2(M, R)$ e fixando $y \in M$, tem-se que $h_y(x) = h(x, y)$ é uma aplicação linear e daí $h_y \in M^*$. Sendo b bilinear, segue que existe $y' \in M$ tal que $\varphi_b(y') = h_y$. Assim, tem-se que $y \mapsto y'$ é uma aplicação linear de M em M , ou seja, está em $\text{End}_R(M)$. Além disso, vemos que tais aplicações são as respectivas aplicações inversas uma da outra.

O próximo resultado fornece uma condição suficiente para que uma forma bilinear seja não-degenerada.

Proposição 1.1.4. *Se M é um R -módulo livre finitamente gerado e $b \in L^2(M, R)$, então são equivalentes:*

- (1) *b é uma forma bilinear não-degenerada;*
- (2) *se $\{x_1, x_2, \dots, x_l\}$ é uma R -base de M , então $\det(b(x_i, x_j)) \in R^\times$.*

Demonstração: O resultado segue do fato que, se $y = \sum_{j=1}^l \alpha_j x_j \in M$, então

$$\varphi_b(y)(x_i) = b(x_i, y) = \sum_{j=1}^l \alpha_j b(x_i, x_j)$$

e, portanto, $(b(x_i, x_j))$ é a matriz de φ_b escrita na base $\{\varphi_b(x_1), \varphi_b(x_2), \dots, \varphi_b(x_l)\}$. Deste modo, φ_b é um isomorfismo se, e somente se, $(b(x_i, x_j))$ é inversível, o que equivale a afirmar que $\det(b(x_i, x_j)) \in R^\times$. ■

Com isso, dado M um R -módulo livre finitamente gerado com base $\mathcal{B} = \{x_1, x_2, \dots, x_l\}$ junto com b uma forma bilinear não-degenerada de M em R , segue que existe uma correspondência entre a base $\{f_1, f_2, \dots, f_l\}$ de M^* e os elementos $\{x_1^*, x_2^*, \dots, x_l^*\}$ de M dados por $x_i^* := \varphi_b^{-1}(f_i)$, onde $i = 1, 2, \dots, l$. A Proposição 1.1.5 relaciona tais elementos com sua respectiva base de M .

Proposição 1.1.5. *Se M é um R -módulo livre finitamente gerado com uma base $\mathcal{B} = \{x_1, x_2, \dots, x_l\}$ e b é uma forma bilinear não-degenerada de M em R , então o conjunto $\mathcal{B}^* = \{x_1^*, x_2^*, \dots, x_l^*\}$ é uma R -base de M satisfazendo*

$$b(x_i, x_j^*) = \delta_{ij} ,$$

onde $i, j = 1, 2, \dots, l$. A base $\mathcal{B}^*$ é chamada base dual de $\mathcal{B}$ para M .

Demonstração: Seja $x \in M$. Sendo φ_b^{-1} sobrejetora, segue que existe $f = \sum_{i=1}^l \alpha_i f_i \in M^*$ com $\alpha_i \in R$, para $i = 1, 2, \dots, l$, tal que

$$x = \varphi_b^{-1}(f) = \sum_{i=1}^l \alpha_i \varphi_b^{-1}(f_i) = \sum_{i=1}^l \alpha_i x_i^* .$$

Além disso, se $\sum_{i=1}^l \beta_i x_i^* = 0$, para $\beta_i \in R$, então

$$0 = \sum_{i=1}^l \beta_i x_i^* = \sum_{i=1}^l \beta_i \varphi_b^{-1}(f_i) = \varphi_b^{-1}\left(\sum_{i=1}^l \beta_i f_i\right),$$

implicando em $\sum_{i=1}^l \beta_i f_i = 0$, já que φ_b^{-1} é injetora. Sendo $\{f_1, f_2, \dots, f_l\}$ uma R -base de M^* , segue que $\beta_i = 0$, para $i = 1, 2, \dots, l$. Portanto, $\mathcal{B}^*$ é uma R -base de M . Além disso, tem-se que

$$b(x_i, x_j^*) = \varphi_b(x_j^*)(x_i) = \varphi_b(\varphi_b^{-1}(f_j))(x_i) = f_j(x_i) = \delta_{ij},$$

o que prova a proposição. ■

Notem-se que a base $\mathcal{B}^*$ é única para cada R -base $\mathcal{B}$ de M , pois caso exista outra base $\{x'_1, x'_2, \dots, x'_l\}$ de M satisfazendo $b(x_i, x'_j) = \varphi_b(x'_j)(x_i) = \delta_{ij}$, como φ_b^{-1} é injetora, segue que existem $g_1, g_2, \dots, g_l \in M^*$ tal que $x'_j = \varphi_b^{-1}(g_j)$ e daí, $g_j(x_i) = \delta_{ij}$, ou seja, $g_j = f_j$, para todo $j = 1, 2, \dots, l$. Com isso, tem-se a seguinte relação entre uma base e sua base dual.

Corolário 1.1.6. *Se M é um R -módulo livre finitamente gerado e b é uma forma bilinear simétrica e não-degenerada de M em R , então para toda base $\mathcal{B}$ de M vale $(\mathcal{B}^*)^* = \mathcal{B}$.*

De agora em diante, passaremos a considerar módulos especiais munidos de uma forma bilinear, os espaços euclidianos. Estes espaços serão o ambiente de trabalho para o desenvolvimento das próximas seções.

Definição 1.1.7. Um espaço euclidiano (E, b) , é um espaço vetorial E sobre $\mathbb{R}$ de dimensão finita munido de uma forma bilinear $b : E \times E \rightarrow \mathbb{R}$ simétrica, não-degenerada e positiva¹.

Tem-se que, como definida, tal estrutura herda através da norma definida por

$$\|x\| = b(x, x)^{1/2}$$

a estrutura de espaço de vetorial normado e, conseqüentemente, a de espaço topológico, dado pela métrica

$$d(x, y) = \|x - y\|,$$

para quaisquer $x, y \in E$. Com isso, temos, para $x \in E$ e $r \in \mathbb{R}_+^\times$, definida a bola fechada de centro x e raio r pelo conjunto

$$B[x, r] = \{y \in E ; \|x - y\| \leq r\}.$$

¹Que satisfaz $b(x, x) > 0$ para todo $x \in E$.

Exemplo 1.1.8. Munido do produto escalar usual $\cdot$, tem-se que $\mathbb{R}^n$ é um espaço euclidiano. Um outro exemplo de espaço euclidiano é o conjunto $M_n(\mathbb{R})$ das matrizes quadradas $n \times n$ com entradas em $\mathbb{R}$ munidas da forma traço $(A, B) \mapsto \text{tr}(AB^t)$, onde tr representa a soma dos elementos da diagonal principal. Mais geralmente, podemos considerar o espaço euclidiano $2n^2$ -dimensional $(M_n(\mathbb{C}), \text{Re}(\text{tr}^*))$, onde a forma bilinear em questão é dada por $(A, B) \mapsto \text{Re}(\text{tr}^*(A\overline{B}^t))$.

No que segue, apresentamos o conceito de isometria entre espaços euclidianos.

Definição 1.1.9. Sejam (E_1, b_1) e (E_2, b_2) espaços euclidianos. Uma *isometria* é um $\mathbb{R}$ -linear isomorfismo $\sigma : E_1 \longrightarrow E_2$ satisfazendo a relação

$$b_2(\sigma(x), \sigma(y)) = b_1(x, y) \text{ , para todo } x, y \in E_1.$$

Outra importante noção é a de similaridade entre espaços euclidianos.

Definição 1.1.10. Uma *similaridade* é uma aplicação $\mathbb{R}$ -linear $\sigma : E_1 \longrightarrow E_2$ que satisfaz

$$b_2(\sigma(x), \sigma(y)) = cb_1(x, y) \text{ , para todo } x, y \in E_1 \text{ ,}$$

para algum $c \in \mathbb{R}_+^\times$. Neste caso, a similaridade é dita ter *norma* c .

Note ainda que, da simetria de b , tem-se que, para quaisquer $x, y \in E$, vale a seguinte relação

$$b(x, y) = \frac{1}{2}(b(x+y, x+y) - b(x, x) - b(y, y)) \text{ .} \quad (1.3)$$

Uma outra propriedade importante dos espaços euclidianos é dada através do Teorema de Gram-Schmidt que mostra a existência de uma base $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ ortonormal² para E . Note que com isso, é possível identificar qualquer espaço euclidiano (E, b) n -dimensional com o espaço $(\mathbb{R}^n, \cdot)$, visto que a aplicação

$$\begin{aligned} \eta : E &\longrightarrow \mathbb{R}^n \\ x = \sum_{i=1}^n \alpha_i e_i &\longmapsto \eta(x) = \sum_{i=1}^n \alpha_i \epsilon_i \end{aligned} \quad (1.4)$$

onde $\{\epsilon_1, \epsilon_2, \dots, \epsilon_n\}$ é a base canônica de $\mathbb{R}^n$, é uma isometria. Portanto, sendo $\mathbb{R}^n$ munido da medida de Lebesgue μ_L , o isomorfismo η determina uma medida $\mu : \eta^{-1}(\Sigma) \longrightarrow \mathbb{R} \cup \{+\infty\}$ para E definida por

$$\mu(\eta^{-1}(A)) = \mu_L(A) \text{ ,}$$

²No sentido de que vale $b(e_i, e_j) = \delta_{ij}$, para $i, j = 1, 2, \dots, n$.

onde Σ representa a σ -álgebra dos conjuntos Lebesgue-mensuráveis de $\mathbb{R}^n$. De fato, μ é uma medida, pois $\mu(\emptyset) = 0$, $\mu(A) \geq 0$ para todo $A \in \eta^{-1}(\Sigma)$ e se $(A_n)_{n \in \mathbb{N}}$ é uma família de conjuntos em $\eta^{-1}(\Sigma)$ disjuntos dois a dois, então tem-se que

$$\mu\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \mu\left(\bigcup_{n \in \mathbb{N}} \eta^{-1}(B_n)\right) = \mu\left(\eta^{-1}\left(\bigcup_{n \in \mathbb{N}} B_n\right)\right) = \mu_L\left(\bigcup_{n \in \mathbb{N}} B_n\right) = \bigcup_{n \in \mathbb{N}} \mu_L(B_n) = \bigcup_{n \in \mathbb{N}} \mu(A_n),$$

e, além disso, possui a propriedade de invariância por translação, ou seja,

$$\mu(x + A) = \mu(A), \text{ para quaisquer } x \in E \text{ e } A \in \eta^{-1}(\Sigma),$$

já que a medida de Lebesgue μ_L possui tal propriedade. Note, ainda, que sendo η linear e invertível, tem-se que η é um homeomorfismo entre E e $\mathbb{R}^n$, e como os conjuntos abertos e fechados de $\mathbb{R}^n$ são Lebesgue-mensuráveis, segue que os abertos e fechados de E são mensuráveis em $\eta^{-1}(\Sigma)$.

1.2 Retículos em espaços euclidianos

Consideremos (E, b) um espaço euclidiano de dimensão n sobre $\mathbb{R}$.

Definição 1.2.1. Dizemos que um conjunto $L \subset E$ é um *reticulado*, se existem $v_1, v_2, \dots, v_m \in E$ linearmente independentes sobre $\mathbb{R}$ tais que

$$L = \{\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m ; \alpha_i \in \mathbb{Z} \text{ para } i = 1, 2, \dots, m\}.$$

O conjunto $\mathcal{B} = \{v_1, v_2, \dots, v_m\}$ é dito ser uma *base do reticulado* L . Além disso, dizemos que um reticulado L é *completo*, se $m = n$.

Exemplo 1.2.2. Um exemplo clássico e com fortes propriedades é a família dos reticulados $\mathbb{A}_n \subset \mathbb{R}^{n+1}$, para $n \geq 1$. Tal configuração é obtida considerando a base canônica $\{\epsilon_0, \epsilon_1, \dots, \epsilon_n\}$ de $\mathbb{R}^{n+1}$ e o hiperplano $H = \{x = \sum_{i=0}^n \alpha_i \epsilon_i ; \sum_{i=0}^n \alpha_i = 0\}$. Com isso, tem-se que $\mathbb{A}_n = \mathbb{Z}^{n+1} \cap H$, ou seja, explicitamente o reticulado é descrito por

$$\mathbb{A}_n = \{(\alpha_0, \alpha_1, \dots, \alpha_n) \in \mathbb{Z}^{n+1} ; \alpha_0 + \alpha_1 + \dots + \alpha_n = 0\}.$$

Note que apesar de que $\mathbb{A}_n$ esteja contido em $\mathbb{R}^{n+1}$, o reticulado tem posto n , pois, neste caso, os conjuntos $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ e $\mathcal{B}' = \{v'_1, v'_2, \dots, v'_n\}$, onde $v_i = \epsilon_i - \epsilon_0$ e $v'_i = \epsilon_i - \epsilon_{i-1}$, para $i = 1, 2, \dots, n$, são bases para o reticulado. A Figura 1.1 ilustra o reticulado $\mathbb{A}_2$.

Note que de acordo com a Definição 1.2.1, um reticulado L é um subgrupo abeliano livre e finitamente gerado de E . No entanto, tal condição não é suficiente

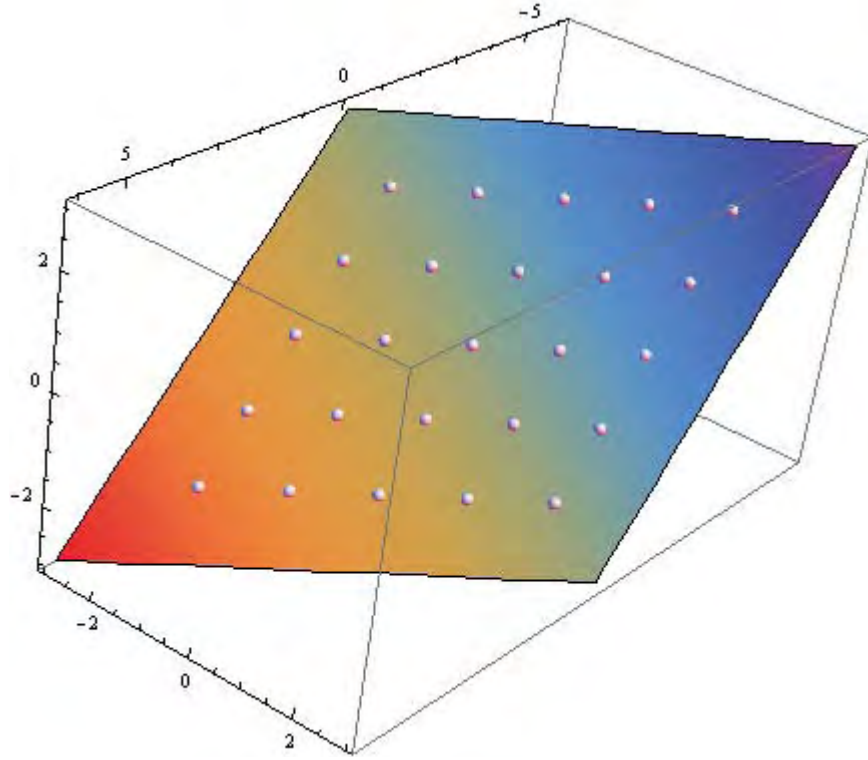


Figura 1.1: Reticulado $\mathbb{A}_2$.

para que um subgrupo de E seja um reticulado, como é o caso de $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ considerado no espaço euclidiano $(\mathbb{R}, \cdot)$. A seguir, veremos uma condição adicional suficiente para que um subgrupo de E tenha a estrutura de reticulado.

Teorema 1.2.3. *Um subgrupo L de E é um reticulado se, e somente se, L é discreto³.*

Demonstração: Seja L um reticulado em E com base $\mathcal{B}' = \{v_1, v_2, \dots, v_m\}$ tal que $m \leq n = \dim_{\mathbb{R}} E$ e tomemos um elemento $x = \sum_{i=1}^m \alpha_i v_i \in L$. Extendendo a base $\mathcal{B}'$ de L a uma base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ de E , tem-se que o conjunto aberto

$$G_x = \left\{ \sum_{i=1}^n \lambda_i v_i ; \lambda_i \in \mathbb{R} \text{ com } |\lambda_i - \alpha_i| < 1, \forall i = 1, 2, \dots, n \right\}$$

de E satisfaz $G_x \cap L = \{x\}$. Portanto, L é discreto. Reciprocamente, consideremos L um subgrupo discreto de E . Sejam $\mathcal{B} = \{v_1, v_2, \dots, v_r\}$ o maior subconjunto de L

³Dizemos que um subconjunto A de E é *discreto* se para todo $x \in A$, existe G um aberto de E tal que $A \cap G = \{x\}$. Equivalentemente, tem-se que:

- (i) A é discreto;
- (ii) para todo K compacto de E , tem-se que $K \cap A$ finito;
- (iii) para todo conjunto limitado U de E , tem-se que $U \cap A$ finito.

linearmente independente sobre $\mathbb{R}$, consideremos o subconjunto limitado

$$P = \left\{ x = \sum_{i=1}^r \alpha_i v_i \in E ; 0 \leq \alpha_i < 1 \right\}$$

de E . Assim, dado $x \in L - (\mathcal{B} \cup \{0\})$, segue, da maximalidade de $\mathcal{B}$, que o conjunto $\{v_1, v_2, \dots, v_r, x\}$ é linearmente dependente sobre $\mathbb{R}$ e daí existem $\beta_1, \beta_2, \dots, \beta_{r+1} \in \mathbb{R}$ não todos nulos, tal que

$$\sum_{i=1}^r \beta_i v_i + \beta_{r+1} x = 0 .$$

Em particular, $\beta_{r+1} \neq 0$, pois, caso contrário, contradizemos a independência linear de $\mathcal{B}$ sobre $\mathbb{R}$. Com isso, podemos escrever

$$x = \sum_{i=1}^r \lambda_i v_i \tag{1.5}$$

com $\lambda_i \in \mathbb{R}$, para $i = 1, 2, \dots, r$. Agora, consideremos para todo $j \in \mathbb{Z}$,

$$x_j = jx - \sum_{i=1}^r [j\lambda_i] v_i ,$$

onde $[j\lambda_i]$ denota a parte inteira do número real $j\lambda_i$. Assim,

$$x_j = j \sum_{i=1}^r \lambda_i v_i - \sum_{i=1}^r [j\lambda_i] v_i = \sum_{i=1}^r j\lambda_i v_i - \sum_{i=1}^r [j\lambda_i] v_i = \sum_{i=1}^r (j\lambda_i - [j\lambda_i]) v_i .$$

Como $0 \leq j\lambda_i - [j\lambda_i] < 1$, segue que $x_j \in P$ para todo $j \in \mathbb{Z}$. Além disso, $x_j \in L$, pois L é subgrupo com $jx, [j\lambda_i] v_i \in L$, para todo $j \in \mathbb{Z}$ e todo $i = 1, 2, \dots, r$. Portanto, para todo $j \in \mathbb{Z}$, segue que $x_j \in P \cap L$. Note, com isso, que L é um $\mathbb{Z}$ -módulo finitamente gerado, pois

$$x = x_1 + \sum_{i=1}^r [\lambda_i] v_i$$

para $j \in \mathbb{Z}$ e, deste modo, é gerado por $P \cap L$, que é finito já que P é limitado e L é discreto. Assim, do fato de $P \cap L$ ser finito e $\mathbb{Z}$ infinito, segue que existem $j, k \in \mathbb{Z}$ com $j \neq k$ tais que $x_j = x_k$, de onde segue que

$$(j - k)\lambda_i = [j\lambda_i] - [k\lambda_i] ,$$

o que mostra que $\lambda_i \in \mathbb{Q}$ para $i = 1, 2, \dots, r$ na Equação (1.5). Agora, sendo L finitamente gerado, consideremos d o produto dos denominadores dos coeficientes de seus geradores. Logo, tem-se que

$$dL \subset H = \sum_{i=1}^r \mathbb{Z} v_i .$$

Sendo H livre e L finitamente gerado, segue que existem, $\gamma_i \in \mathbb{Z}$, para $i = 1, 2, \dots, r$ e uma $\mathbb{Z}$ -base $\{w_1, w_2, \dots, w_r\}$ de H tal que $dL = \langle \gamma_1 w_1, \gamma_2 w_2, \dots, \gamma_r w_r \rangle_{\mathbb{Z}}$. Como dL é livre já que H é livre e dL e L isomorfos como $\mathbb{Z}$ -módulos, segue que L é livre e, assim, dL e L possuem mesmo posto sobre $\mathbb{Z}$. Mas, como $dL \subset H \subset L$ segue que H possui o mesmo posto de L sobre $\mathbb{Z}$. Deste modo, concluímos que $\gamma_i \neq 0$ para $i = 1, 2, \dots, r$ e que $\{w_1, w_2, \dots, w_r\}$ é linearmente independente sobre $\mathbb{R}$ pois, como $w_i = \sum_{j=1}^r \beta_{ij} v_j$ com $\det(\beta_{ij}) \neq 0$ já que $\{w_1, w_2, \dots, w_r\}$ é linearmente independente sobre $\mathbb{Z}$, segue que, para toda combinação linear real $\sum_{i=1}^r \alpha_i w_i = 0$, tem-se que

$$0 = \sum_{i=1}^r \alpha_i w_i = \sum_{i=1}^r \alpha_i \left(\sum_{j=1}^r \beta_{ij} v_j \right) = \sum_{j=1}^r \left(\sum_{i=1}^r \alpha_i \beta_{ij} \right) v_j.$$

Da independência linear de $\{v_1, v_2, \dots, v_r\}$, tem-se o seguinte sistema linear

$$\sum_{i=1}^r \alpha_i \beta_{ij} = 0 \text{ para } j = 1, 2, \dots, r.$$

Como $\det(\beta_{ij}) \neq 0$, segue que $\alpha_i = 0$ para $i = 1, 2, \dots, r$ e, portanto, $\{w_1, w_2, \dots, w_r\}$ é linearmente independente sobre $\mathbb{R}$, ou seja, L possui uma base que é linearmente independente sobre $\mathbb{R}$, provando ser um reticulado em E . ■

De agora em diante, passamos a considerar apenas reticulados completos, isto porque podemos sempre nos restringir ao espaço vetorial real gerado pelo reticulado. Portanto, ao longo deste texto, reticulados serão subgrupos discretos de posto maximal num espaço euclidiano (E, b) n -dimensional. Com essa presunção, é comum e equivalente definirmos os reticulados (no sentido da teoria dos números) como um par (L, b) , onde L é um grupo abeliano ($\mathbb{Z}$ -módulo) livre de posto finito e $b : L_{\mathbb{R}} \times L_{\mathbb{R}} \rightarrow \mathbb{R}$ uma forma bilinear simétrica, positiva e não-degenerada do $\mathbb{R}$ -espaço vetorial de dimensão finita $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$ em $\mathbb{R}$ obtido por extensão dos escalares (note que $L_{\mathbb{R}}$ possui dimensão igual ao posto de L como $\mathbb{Z}$ -módulo), deixando subentendido a imersão de L no espaço euclidiano $(L_{\mathbb{R}}, b)$ dada por $x \mapsto x \otimes 1$. Abaixo, consideraremos alguns conceitos e suas propriedades relativas ao estudo de reticulados.

Definição 1.2.4. Seja $\mathcal{F} = \{x_1, x_2, \dots, x_n\}$ uma família de vetores em E . Definimos o *discriminante* de $\mathcal{F}$ por

$$\Delta_{\mathcal{F}} = |\det(M_{\mathcal{F}})|,$$

onde as colunas de $M_{\mathcal{F}}$ são as coordenadas com relação a alguma base ortonormal de E .

Lema 1.2.5. *Sejam $\mathcal{F} = \{x_1, x_2, \dots, x_n\}$ e $\mathcal{F}' = \{x'_1, x'_2, \dots, x'_n\}$ dois conjuntos ordenados de vetores em E . Se $M_{\mathcal{F}}$ e $M_{\mathcal{F}'}$ são as respectivas matrizes de $\mathcal{F}$ e $\mathcal{F}'$ em relação a uma mesma base ortonormal de E , então*

$$(b(x_i, x'_j)) = M_{\mathcal{F}}^t M_{\mathcal{F}'} .$$

Em particular, se $M_{\mathcal{F}} = M_{\mathcal{F}'}$, então $M_{\mathcal{F}}^t M_{\mathcal{F}} = (b(x_i, x_j))_{n \times n}$ e $\det(G_{\mathcal{F}}) = (\det(M_{\mathcal{F}}))^2$.

Demonstração: Considerando $\{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n\}$ uma base ortonormal de E e escrevendo $x_i = \sum_{k=1}^n m_{ki} \varepsilon_k$ e $x'_j = \sum_{\ell=1}^n m'_{\ell j} \varepsilon_{\ell}$, tem-se que

$$b(x_i, x'_j) = \sum_{k=1}^n \left(\sum_{\ell=1}^n m_{ki} m'_{\ell j} \underbrace{b(\varepsilon_k, \varepsilon_{\ell})}_{\delta_{k\ell}} \right) = \sum_{k=1}^n m_{ki} m'_{kj} = \sum_{k=1}^n m_{ik}^t m'_{kj} ,$$

o que prova o resultado. ■

Definição 1.2.6. Dado um conjunto ordenado $\mathcal{F} = \{x_1, x_2, \dots, x_s\}$ de vetores em E , definimos a *matriz Gram de $\mathcal{F}$* por

$$G_{\mathcal{F}} = (b(x_i, x_j))_{s \times s} .$$

Para um reticulado L em E , definimos uma *matriz Gram de L* como sendo uma matriz Gram $G_{\mathcal{B}}$ de uma base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ de L .

Observe que, do Lema 1.2.5, uma matriz Gram $G_{\mathcal{B}}$ de L , para alguma base $\mathcal{B}$ de L , é $M_{\mathcal{B}}^t M_{\mathcal{B}}$, onde $M_{\mathcal{B}}$ é a matriz cujas colunas são as coordenadas dos vetores de $\mathcal{B}$ em relação a alguma base ortonormal de E . Tal matriz é conhecida por *matriz geradora de L* , já que é possível obter L por $M_{\mathcal{B}} \mathbb{Z}^n$. O próximo resultado nos diz a respeito de um importante invariante das matrizes Gram associadas a um reticulado.

Proposição 1.2.7. *Se L é um reticulado em E , então o determinante de uma matriz Gram de L é invariante, para qualquer base de L .*

Demonstração: Sejam $\mathcal{B}$ e $\mathcal{B}'$ bases distintas do reticulado L . Dada uma base ortonormal de E , sejam $M_{\mathcal{B}}$ e $M_{\mathcal{B}'}$ as respectivas matrizes cujas colunas são as coordenadas de $\mathcal{B}$ e $\mathcal{B}'$ em relação à base ortonormal fixada. Consideremos Q a matriz de mudança de base $\mathcal{B}$ para $\mathcal{B}'$, ou seja, a matriz $Q \in \text{GL}_n(\mathbb{Z})$ invertível (isto é, $\det(Q) = \pm 1$) tal que $M_{\mathcal{B}'} = M_{\mathcal{B}} Q$. Assim, do Lema 1.2.5, segue que

$$G_{\mathcal{B}'} = M_{\mathcal{B}'}^t M_{\mathcal{B}'} = (M_{\mathcal{B}} Q)^t M_{\mathcal{B}} Q = Q^t M_{\mathcal{B}}^t M_{\mathcal{B}} Q = Q^t G_{\mathcal{B}} Q ,$$

e, portanto, $\det(G_{\mathcal{B}}) = \det(G_{\mathcal{B}'})$, já que $\det(Q) = \det(Q^t) = \pm 1$. ■

A Proposição 1.2.7 nos permite a seguinte definição.

Definição 1.2.8. Dado um reticulado L , definimos o *determinante* e o *discriminante* de L , respectivamente, por

$$\det(L) = \det(G_{\mathcal{B}}) \quad \text{e} \quad \Delta_L = \Delta_{\mathcal{B}},$$

onde $\mathcal{B}$ é uma base de L .

Assim, com as definições e os resultados dados anteriormente, segue que

$$\det(L) = \Delta_L^2. \tag{1.6}$$

Exemplo 1.2.9. Sendo $\mathcal{B} = \{(1, 0), (1/2, \sqrt{3}/2)\}$ uma base do reticulado L em $(\mathbb{R}^2, \cdot)$, segue que a matriz Gram do reticulado L gerada por $\mathcal{B}$ é dada por

$$G_{\mathcal{B}} = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}.$$

Deste modo, o determinante do reticulado L em questão é igual a $\frac{3}{4}$.

Daqui até o fim da seção, abordaremos o importante conceito de integralidade e suas ramificações. Adiante, veremos como este se traduz em termos da dualidade e quais as suas consequências nos reticulados com essa propriedade.

Definição 1.2.10. Dizemos que um reticulado L em (E, b) é *integral*, se $b(x, y) \in \mathbb{Z}$, para quaisquer $x, y \in L$.

Assim, se L é integral, então $G_{\mathcal{B}} \in M_n(\mathbb{Z})$, para toda base $\mathcal{B}$ de L . Dentre os reticulados integrais, tem-se o caso mais refinado abaixo.

Definição 1.2.11. Dizemos que um reticulado é *par*, se $b(x, x) \in 2\mathbb{Z}$, para todo $x \in L$. Caso contrário, L é dito *ímpar*.

Da Equação (1.3), segue que se L é um reticulado par, então L é um reticulado integral.

Exemplo 1.2.12. O reticulado $L = \sqrt{2}\mathbb{Z}^2$ é um reticulado par em $\mathbb{R}^2$, onde uma matriz Gram é

$$G_{\mathcal{B}} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

para $\mathcal{B} = \{(\sqrt{2}, 0), (0, \sqrt{2})\}$ uma base de L .

Proposição 1.2.13. *Um reticulado L em E é par se, e somente se, umas das suas matrizes Gram tem entradas inteiras com diagonal par.*

Demonstração: Supondo L um reticulado par em E , tem-se que $b(x, x) \in 2\mathbb{Z}$ para todo $x \in L$ e, em particular, L é integral. Assim, se $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ é uma base de L , então as entradas da diagonal da matriz $G_{\mathcal{B}}$ são $b(v_i, v_i) \in 2\mathbb{Z}$, para $i = 1, 2, \dots, n$. Reciprocamente, suponhamos que para uma base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ de L a matriz Gram $G_{\mathcal{B}}$ possui entradas inteiras e diagonal par. Seja $x \in L$ dado por $x = \sum_{i=1}^n \alpha_i v_i$ com $\alpha_i \in \mathbb{Z}$. Sendo b simétrica, podemos escrever

$$b(x, x) = \sum_{i=1}^n \left(\sum_{j=1}^n \alpha_i \alpha_j b(v_i, v_j) \right) = \sum_{i=1}^n \alpha_i^2 b(v_i, v_i) + 2 \sum_{i=1}^n \left(\sum_{j>i}^n \alpha_i \alpha_j b(v_i, v_j) \right).$$

Como $b(v_i, v_j) \in \mathbb{Z}$ e, em particular, $b(v_i, v_i) \in 2\mathbb{Z}$ para $i = 1, 2, \dots, n$, segue que $b(x, x) \in 2\mathbb{Z}$ e, portanto, L é par. ■

Definição 1.2.14. Dizemos que um reticulado L é *unimodular*, se L é integral e $\det(L) = 1$.

Exemplo 1.2.15. Um exemplo de reticulado unimodular em $\mathbb{R}^n$ é $L = \mathbb{Z}^n$. De fato, tem-se que L integral com $\det(L) = 1$, visto que a base canônica do $\mathbb{R}^n$ é uma base para L .

1.3 Isometrias, similaridades e reescalares

Nesta seção, apresentamos as equivalências entre reticulados. Observe, no entanto, que tal abordagem não será com relação à estrutura de módulo, visto que sendo um reticulado L um $\mathbb{Z}$ -módulo livre de posto maximal n , tem-se que sempre L é isomorfo (como $\mathbb{Z}$ -módulo) a $\mathbb{Z}^n$. Nosso tratamento será com relação as propriedades métricas do reticulado, como veremos a seguir:

Definição 1.3.1. Sejam L_1 e L_2 reticulados nos espaços euclidianos (E_1, b_1) e (E_2, b_2) , respectivamente. Dizemos que L_1 é *isomorfo* (ou *isométrico*) a L_2 , se existe uma isometria $\sigma : E_1 \rightarrow E_2$ com $\sigma(L_1) = L_2$. Neste caso, denotamos $L_1 \simeq L_2$.

Abaixo introduzimos o conceito de reticulados similares.

Definição 1.3.2. Sejam L_1 e L_2 reticulados nos espaços euclidianos (E_1, b_1) e (E_2, b_2) , respectivamente. Dizemos que L_1 é *similar* a L_2 , se existe uma similaridade σ de E_1 em E_2 tal que $\sigma(L_1) = L_2$. Neste caso, denotamos $L_1 \sim L_2$.

Exemplo 1.3.3. Os reticulados $\mathbb{Z}^2$ e $\sqrt{2}\mathbb{Z}^2$ são similares, visto que a transformação linear $\sigma : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ dada por $x \mapsto \sqrt{2}x$ é uma similaridade de norma 2, já que satisfaz

$$\sigma(x)\sigma(y) = 2xy, \text{ para quaisquer } x, y \in \mathbb{R}^2.$$

Além disso, tem-se que $\sigma(\mathbb{Z}^2) = \sqrt{2}\mathbb{Z}^2$. Portanto, $\mathbb{Z}^2 \sim \sqrt{2}\mathbb{Z}^2$.

Definição 1.3.4. Sejam L um reticulado em (E, b) e $c \in \mathbb{R}^\times$. Definimos cL o reticulado reescalado de L por c como L no espaço euclidiano (E, cb) .

Proposição 1.3.5. Se os reticulados L_1 e L_2 em (E_1, b_1) e (E_2, b_2) são, respectivamente, similares com norma c , então ${}^cL_1 \simeq L_2$.

Demonstração: Tal resultado segue de forma imediata do fato de que uma similaridade de (E_1, b_1) para (E_2, b_2) com norma c , é uma isometria de (E_1, cb_1) para (E_2, b_2) . ■

Proposição 1.3.6. Se L é um reticulado em (E, b) , então, para todo $c \in \mathbb{R}_+^\times$, vale ${}^cL \simeq \sqrt{c}L$.

Demonstração: A transformação linear $\sigma : (E, cb) \longrightarrow (E, b)$ dada por $x \mapsto \sqrt{c}x$ é uma isometria entre os espaços euclidianos, visto que satisfaz

$$b(\sigma(x), \sigma(y)) = b(\sqrt{c}x, \sqrt{c}y) = cb(x, y),$$

para quaisquer $x, y \in E$. Além disso, tem-se $\sigma(L) = \sqrt{c}L$. Portanto, cL e $\sqrt{c}L$ são isométricos. ■

Exemplo 1.3.7. Como consequência das Proposições 1.3.5 e 1.3.6, segue que $\mathbb{Z}^2 \simeq {}^2\mathbb{Z}^2 \simeq \sqrt{2}\mathbb{Z}^2$.

1.4 Dualidade

Como usual, seja (E, b) um espaço euclidiano n -dimensional. A seguir, introduzimos o importante conceito de reticulado dual.

Definição 1.4.1. Seja L um reticulado em E . Definimos o *reticulado dual* de L por

$$L^\# = \{x \in E ; b(x, L) \subseteq \mathbb{Z}\}.$$

A proposição a seguir justifica a terminologia do reticulado com respeito a dualidade.

Proposição 1.4.2. Se L é um reticulado com base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ e $\mathcal{B}^* = \{v_1^*, v_2^*, \dots, v_n^*\}$ é a base dual de $\mathcal{B}$ para E , então

$$L^\# = \{\alpha_1 v_1^* + \alpha_2 v_2^* + \dots + \alpha_n v_n^* ; \alpha_i \in \mathbb{Z}, \text{ para } i = 1, 2, \dots, n\} .$$

Demonstração: Notemos que $\mathcal{B}^* \subset L^\#$, já que para todo $x = \sum_{j=1}^n \alpha_j v_j \in L$ tem-se que

$$b(v_i^*, x) = b(v_i^*, \sum_{j=1}^n \alpha_j v_j) = \sum_{j=1}^n \alpha_j b(v_i^*, v_j) = \sum_{j=1}^n \alpha_j \delta_{ij} = \alpha_j \in \mathbb{Z} .$$

Assim,

$$b\left(\sum_{i=1}^n \beta_i v_i^*, \sum_{j=1}^n \alpha_j v_j\right) = \sum_{i=1}^n \beta_i b\left(v_i^*, \sum_{j=1}^n \alpha_j v_j\right) = \sum_{i=1}^n \beta_i \alpha_j \in \mathbb{Z} ,$$

e portanto, $\sum_{i=1}^n \mathbb{Z} v_i^* \subset L^\#$. Por outro lado, sendo $\mathcal{B}^*$ uma $\mathbb{R}$ -base para E , tem-se que se $x \in L^\#$ podemos escrever $x = \sum_{i=1}^n \beta_i v_i^*$, com $\beta_i \in \mathbb{R}$. Com isso, como $b(x, v_j) \in \mathbb{Z}$, para $j = 1, 2, \dots, n$, pois $x \in L^\#$ e $v_j \in L$, segue que

$$b(x, v_j) = b\left(\sum_{i=1}^n \beta_i v_i^*, v_j\right) = \sum_{i=1}^n \beta_i b(v_i^*, v_j) = \sum_{i=1}^n \beta_i \delta_{ij} = \beta_j \in \mathbb{Z},$$

o que prova a proposição. ■

Exemplo 1.4.3. Considerando em $(\mathbb{R}^2, \cdot)$ o reticulado $L = \sqrt{2}\mathbb{Z}^2$, tem-se que seu reticulado dual é $L^\# = \frac{1}{\sqrt{2}}\mathbb{Z}^2$, pois sendo $\mathcal{B} = \{(\sqrt{2}, 0), (0, \sqrt{2})\}$ uma base de L , tem-se que $\mathcal{B}^* = \{(\frac{1}{\sqrt{2}}, 0), (0, \frac{1}{\sqrt{2}})\}$.

Corolário 1.4.4. Se L é um reticulado, então $(L^\#)^\# = L$.

Demonstração: Como $(\mathcal{B}^*)^* = \mathcal{B}$, segue, pela Proposição 1.4.2, que $(L^\#)^\# = L$. ■

Proposição 1.4.5. Se L é um reticulado e $c \in \mathbb{R}^\times$, então $(cL)^\# = c^{-1}L^\#$.

Demonstração: Seja $y \in L^\#$. Para todo $x \in L$, tem-se que $b(cx, c^{-1}y) = b(x, y) \in \mathbb{Z}$ e, portanto, tem-se que $c^{-1}L^\# \subset (cL)^\#$. Por outro lado, se $y \in (cL)^\#$, então $b(cx, y) \in \mathbb{Z}$, para todo $x \in L$. Da $\mathbb{R}$ -linearidade de b , segue que $cy \in L^\#$, ou seja, $y \in c^{-1}L^\#$ e, portanto, $(cL)^\# \subset c^{-1}L^\#$. ■

Alguns invariantes do reticulado dual $L^\#$ dependem exclusivamente dos invariantes de L como é possível notarmos nos resultados a seguir:

Proposição 1.4.6. Se L é um reticulado, então $\det(L^\#) = \det(L)^{-1}$.

Demonstração: Dadas $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ uma base de L e $\mathcal{B}^* = \{v_1^*, v_2^*, \dots, v_n^*\}$ a base dual de $\mathcal{B}$ para E , segue da relação $b(v_i, v_j^*) = \delta_{ij}$ que

$$I_n = (b(v_i, v_j^*)) = (b(v_i, \sum t_{kj} v_k)) = (\sum t_{kj} b(v_i, v_k)) = (b(v_i, v_k)) T ,$$

onde T é a matriz $(t_{kj}) \in \text{GL}_n(\mathbb{R})$ dada por $t_{kj} = b(v_k^*, v_j^*)$ e sendo $v_j^* = \sum t_{ij} v_i$, tem-se que

$$b(v_k^*, v_j^*) = b(v_k^*, \sum t_{ij} v_i) = \sum t_{ij} b(v_k^*, v_i) = t_{kj} .$$

Deste modo, segue que $(b(v_i, v_j))^{\text{--}1} = T = T^t$, pois b é simétrica e, portanto, tem-se o resultado já que $\det(L^\#) = \det(b(v_k^*, v_j^*))$. ■

Proposição 1.4.7. *Se M é uma matriz geradora do reticulado L , então $(M^t)^{-1}$ é a matriz geradora de $L^\#$.*

Demonstração: Sejam $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ uma base de L e $\mathcal{B}^* = \{v_1^*, v_2^*, \dots, v_n^*\}$ a base dual de $\mathcal{B}$ para E e sejam M e M^* as respectivas matrizes geradoras de L e $L^\#$ cujas colunas são, respectivamente, as coordenadas de $\mathcal{B}$ e $\mathcal{B}^*$ em relação a uma base ortonormal de E fixada. Como $b(v_i, v_j^*) = \delta_{ij}$, segue que $M^t M^* = I_n$ e, com isso, tem-se que $M^* = (M^t)^{-1}$. ■

No que segue, veremos como as propriedades de integralidade e unimodularidade de um reticulado estão relacionadas com condições sobre seu reticulado dual.

Proposição 1.4.8. *Um reticulado L é integral se, e somente se, $L \subset L^\#$.*

Demonstração: Seja $x \in L$. Como, por hipótese, $b(x, y) \in \mathbb{Z}$ para todo $y \in L$, segue que $x \in L^\#$ e daí tem-se que $L \subset L^\#$. Reciprocamente, se $x, y \in L$, então $b(x, y) \in \mathbb{Z}$, já que $x \in L^\#$. ■

Com o propósito já discutido acima, apresentamos a seguir uma importante noção para reticulados, que permitirá caracterizar o determinante de um reticulado integral.

Definição 1.4.9. Sejam L_1 e L_2 reticulados em (E, b) com respectivas bases $\mathcal{B}_1$ e $\mathcal{B}_2$. Definimos o invariante relativo a L_1 e L_2 por

$$\chi(L_1, L_2) = |\det(M_{\mathcal{B}_2, \mathcal{B}_1})| ,$$

onde $M_{\mathcal{B}_2, \mathcal{B}_1} \in \text{GL}_n(\mathbb{R})$ é matriz de mudança de base de $\mathcal{B}_2$ para $\mathcal{B}_1$.

Proposição 1.4.10. *Se L_1 , L_2 e L_3 são reticulados em (E, b) , então valem as seguintes propriedades:*

1. $\chi(L_1, L_1) = 1$.
2. $\chi(L_1, L_2) = \chi(L_2, L_1)^{-1}$.
3. $\chi(L_1, L_2) \cdot \chi(L_2, L_3) = \chi(L_1, L_3)$.
4. $L_2 \subset L_1 \Rightarrow \chi(L_1, L_2) = (L_1 : L_2)$, onde $(L_1 : L_2)$ denota o índice de grupos de L_2 em L_1 .

Demonstração: As propriedades (1), (2) e (3) são imediatas das propriedades das matrizes de mudança de base. Agora, supondo L_1 um reticulado com base $\mathcal{B}_1 = \{v_1, v_2, \dots, v_n\}$ e $L_2 \subset L_1$, segue que existem $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$ positivos tal que $\mathcal{B}_2 = \{\alpha_1 v_1, \alpha_2 v_2, \dots, \alpha_n v_n\}$ é uma base para L_2 . Com isso, tem-se que $M_{\mathcal{B}_2, \mathcal{B}_1} = (\text{diag}(\alpha_i))_{n \times n}$ e, portanto, $\chi(L_1, L_2) = \prod_{i=1}^n \alpha_i$. Agora, como

$$L_1/L_2 \simeq \bigoplus_{i=1}^n \mathbb{Z}v_i / \bigoplus_{i=1}^n \mathbb{Z}\alpha_i v_i \simeq \bigoplus_{i=1}^n \mathbb{Z}/\alpha_i \mathbb{Z} ,$$

segue que $(L_1 : L_2) = \prod_{i=1}^n \alpha_i$. ■

Notemos que o discriminante Δ_L de L é igual a $\chi(L_0, L)$, onde L_0 é um reticulado gerado por uma base ortonormal de E .

Proposição 1.4.11. *Se L é um reticulado integral, então $\det(L) = (L^\# : L)$.*

Demonstração: Sendo L integral, pela Proposição 1.4.8, segue que $L \subset L^\#$, e com isso

$$\begin{aligned} (L^\# : L) &= \chi(L^\#, L) \\ &= \chi(L^\#, L_0) \chi(L_0, L) \\ &= \chi(L_0, L^\#)^{-1} \chi(L_0, L) \\ &= \Delta_{L^\#}^{-1} \Delta_L \\ &= \Delta_L^2 \\ &= \det(L) , \end{aligned}$$

o que prova a proposição. ■

Corolário 1.4.12. *Um reticulado L é unimodular se, e somente se, $L = L^\#$.*

Demonstração: Segue como consequência imediata da Proposição 1.4.11. ■

1.5 Empacotamentos

Consideremos (E, b) um espaço euclidiano n -dimensional.

Definição 1.5.1. Seja L um reticulado em E . Definimos a *norma* de L por

$$\min(L) = \inf\{b(x, x) ; x \in L, x \neq 0\} .$$

Observamos que a norma de um reticulado L é a menor norma (com relação à norma definida na Seção 1.1 para E), ao quadrado, de um ponto do reticulado. Outra noção geométrica importante é seguinte:

Definição 1.5.2. Dado L um reticulado em E , definimos a *região de Voronoi* de $x_0 \in L$ por

$$V_L(x_0) = \{x \in E ; \|x - x_0\| \leq \|x - y\| , \forall y \in L\} .$$

Observe que, geometricamente, podemos dizer que a região de Voronoi de um ponto $x_0 \in L$ é o conjunto dos pontos de E que estão “mais próximos” de x_0 (com relação à métrica definida na Seção 1.1), do que qualquer outro ponto do reticulado L .

Exemplo 1.5.3. Em $(\mathbb{R}^2, \cdot)$, a Figura 1.2 ilustra uma região de Voronoi do reticulado L do Exemplo 1.2.9.

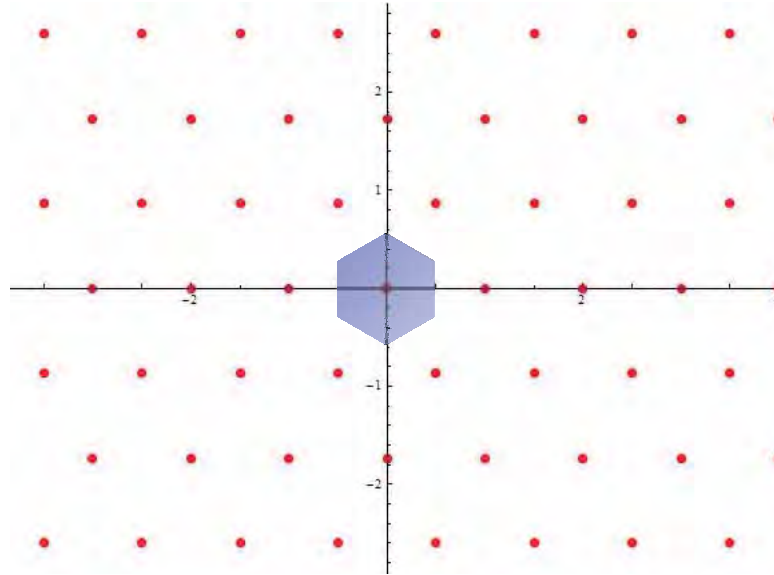


Figura 1.2: Região de Voronoi $V_L(0)$ do reticulado L .

O próximo resultado diz respeito a uma propriedade importante das regiões de Voronoi de um reticulado.

Proposição 1.5.4. Se L é um reticulado em E , então, para todo $x_0 \in L$, tem-se que

$$V_L(x_0) = x_0 + V_L(0) .$$

Demonstração: Se $x \in V_L(x_0)$, então

$$\|x - x_0\| \leq \|x - y\| , \text{ para todo } y \in L .$$

Em particular, como $x_0 + y \in L$, para todo $y \in L$, segue que

$$\|x - x_0\| \leq \|x - (x_0 + y)\| = \|(x - x_0) - y\| , \text{ para todo } y \in L ,$$

ou seja, $x - x_0 \in V_L(0)$ e, portanto, $x \in x_0 + V_L(0)$. Por outro lado, se $x \in x_0 + V_L(0)$, então $x - x_0 \in V_L(0)$ e daí

$$\|x - x_0\| \leq \|(x - x_0) - y\| , \text{ para todo } y \in L .$$

Como $y + x_0 \in L$, para todo $y \in L$, logo tem-se

$$\|x - x_0\| \leq \|(x - x_0) - y + x_0\| = \|x - y\| , \forall y \in L ,$$

e, portanto, $x \in V_L(x_0)$. ■

Observe que uma família de regiões de Voronoi $(V_L(x))_{x \in L}$ é uma cobertura de E .

Exemplo 1.5.5. A Figura 1.3 elucida o ladrilhamento de $\mathbb{R}^2$ pelas regiões de Voronoi do reticulado L do Exemplo 1.2.9.

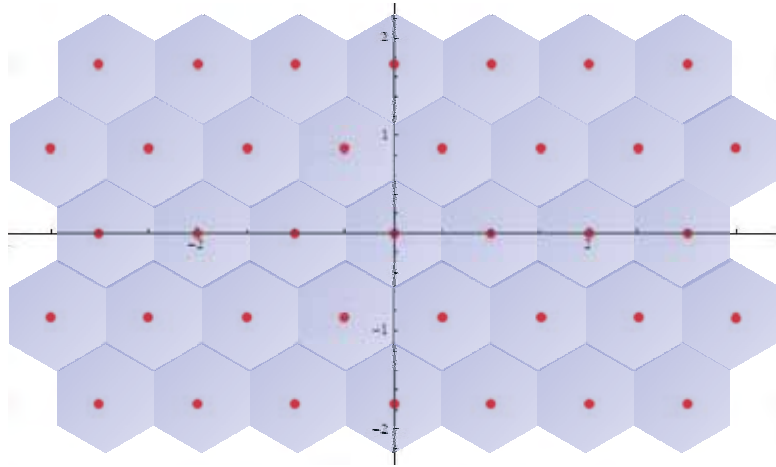


Figura 1.3: Ladrilhamento de $\mathbb{R}^2$.

Definição 1.5.6. Uma família de subconjuntos $\mathcal{P} = (K_i)_{i \in I}$ de E , onde I é um conjunto de índices, é dita ser um *empacotamento* de E se o interior de quaisquer dois subconjuntos K_i e K_j são disjuntos, sempre que $i \neq j$. Dado L um reticulado em E , um empacotamento $\mathcal{P}$ de E é dito um *empacotamento pelo reticulado L* , se $\mathcal{P} = (K + x)_{x \in L}$, para algum $K \subset E$.

Em especial, dado um reticulado L em E , tem-se sempre relacionado a E um empacotamento particular chamado *empacotamento esférico do reticulado L* , que é um empacotamento por reticulado $\mathcal{P} = (K + x)_{x \in L}$, onde K é a esfera n -dimensional $B[0, \rho_L]$, onde

$$\rho_L = \sup\{r \in \mathbb{R}_+ ; B[0, r] \subset V_L(0)\} .$$

Note que, neste caso, o empacotamento é dado por $\mathcal{P} = (B[x, \rho_L])_{x \in L}$.

Exemplo 1.5.7. O empacotamento esférico do reticulado L do Exemplo 1.2.9 está ilustrado na Figura 1.4.

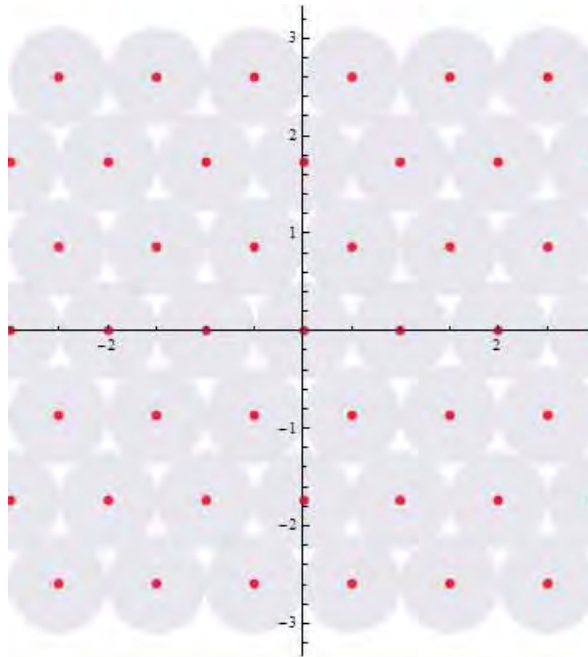


Figura 1.4: Empacotamento esférico do reticulado L .

O problema de empacotamento esférico por um reticulado visa avaliar “o quanto” de E é coberto pelas esferas de $\mathcal{P} = (B[x, \rho_L])_{x \in L}$. Para isto é necessário o conceito de região fundamental de um reticulado.

Definição 1.5.8. Seja L um reticulado em E . Um subconjunto fechado $F \subset E$ é dita uma *região fundamental de L* se $(F + x)_{x \in L}$ é uma cobertura de E e $(F + x)_{x \in L}$ é um empacotamento pelo reticulado L de E .

Exemplo 1.5.9. Dado um reticulado L com base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$, a região de Voronoi $V_L(0)$ e o conjunto

$$P_{\mathcal{B}} = \left\{ x = \sum_{i=1}^n \alpha_i v_i \in E ; 0 \leq \alpha_i \leq 1 \text{ para } i = 1, 2, \dots, n \right\}$$

são regiões fundamentais de L .

A seguir tem-se a principal propriedade de uma região fundamental de um reticulado. Omitiremos a demonstração deste resultado por fugir ao escopo deste texto.

Teorema 1.5.10. [11] *Seja L um reticulado em E . O volume de uma região fundamental de um reticulado é invariante.*

A seguinte definição refere-se ao invariante que mede o quão denso é o reticulado.

Definição 1.5.11. Seja L um reticulado em E . Definimos a *densidade* do empacotamento esférico $\mathcal{P}$ pelo reticulado L por

$$\Delta(L) = \frac{\mu(B[0, \rho_L])}{\mu(V_L(0))}.$$

Observe que tal invariante está bem definido uma vez que $(x + V_L(0))_{x \in L}$ é uma cobertura de E . Além disso, pela uniformidade com que está disposto o reticulado em E , tem-se $\Delta(L) = \frac{\mu(B[x_0, \rho_L])}{\mu(V_L(x_0))}$, para todo $x_0 \in L$, uma vez que $B[x_0, \rho_L] = x_0 + B[0, \rho_L]$ e $V_L(x_0) = x_0 + V_L(0)$. Com isso, estamos aptos a encontrar uma expressão para a densidade do empacotamento esférico de L com base nos seus invariantes.

Teorema 1.5.12. *Se L é um reticulado em E , então o empacotamento esférico pelo reticulado L tem densidade*

$$\Delta(L) = \omega_n \frac{\min(L)^{n/2}}{2^n \det(L)^{1/2}},$$

onde $\omega_n = \mu(B[0, 1])$.

Demonstração: Notemos inicialmente que $\rho_L = \frac{1}{2} \min(L)^{1/2}$ e

$$\mu(P_{\mathcal{B}}) = \int d\eta(v_1) d\eta(v_2) \dots d\eta(v_n) = \int |\det(\eta(v_i))| d\epsilon_1 d\epsilon_2 \dots d\epsilon_n = |\det(\eta(v_i))| = \det(L)^{1/2}.$$

Como $\mu(B[0, \rho_L]) = \rho_L^n \omega_n$, onde $\omega_n = \mu(B[0, 1])$ e, sendo $P_{\mathcal{B}}$ uma região fundamental de L , segue que $\mu(V_L(0)) = \mu(P_{\mathcal{B}})$. Assim,

$$\Delta(L) = \frac{\mu(B[0, \rho_L])}{\mu(V_L(0))} = \omega_n \frac{\min(L)^{n/2}}{2^n \det(L)^{1/2}},$$

o que prova o Teorema. ■

Definição 1.5.13. O *invariante de Hermite* do reticulado L é

$$\gamma(L) = \frac{\min(L)}{\det(L)^{1/n}}.$$

O invariante

$$\delta(L) = 2^{-n} \gamma(L)^{n/2} = \frac{\min(L)^{n/2}}{2^n \det(L)^{1/2}},$$

é chamado a *densidade de centro* de L .

1.6 Modularidade

Seja (E, b) um espaço euclidiano n -dimensional. Introduzimos a seguir a noção de modularidade para reticulados.

Definição 1.6.1. Um reticulado integral L em (E, b) é dito ser *modular* se $L \sim L^\#$.

De acordo com a definição, L ser modular implica na existência de uma similaridade σ de norma $\ell \in \mathbb{R}_+^\times$ em E tal que $\sigma(L^\#) = L$. Por isso é comum dizermos que L é ℓ -modular, onde ℓ é dito o *grau de modularidade* de L . No que segue, trataremos dos resultados que decorrem do conceito de modularidade para reticulados. A proposição a seguir fornece uma relação de inclusão com o reticulado dual.

Proposição 1.6.2. Se L em (E, b) é um reticulado ℓ -modular, então $\ell L^\# \subset L$.

Demonstração: Da hipótese, existe σ uma similaridade de norma ℓ de E tal que $\sigma(L^\#) = L$. Consideremos $x \in L^\#$. Para todo $y \in L^\#$ tem-se que

$$b(\ell x, y) = \ell b(x, y) = b(\sigma(x), \sigma(y)).$$

Como $\sigma(x), \sigma(y) \in L$ e L é integral, segue que $b(\ell x, y) \in \mathbb{Z}$, para todo $y \in L^\#$, ou seja, $\ell x \in (L^\#)^\# = L$. ■

Com base na Proposição 1.6.2, observamos que a noção introduzida na Definição 1.6.1 estende a noção de unimodularidade, que aqui é o caso modular de grau $\ell = 1$. Para seguirmos com nosso estudo, precisamos da seguinte proposição.

Proposição 1.6.3. Se L em (E, b) é um reticulado ℓ -modular, então $\ell \in \mathbb{Z}$.

Demonstração: De acordo com a Proposição 1.6.2 e a integralidade de L , tem-se que $\ell L^\# \subset L \subset L^\#$. Portanto, é necessário que $\ell \in \mathbb{Z}$, já que $\ell L^\# \subset L^\#$. ■

Exemplo 1.6.4. Um exemplo de reticulados modulares em $(\mathbb{R}^2, \cdot)$, são os do tipo $C_{(\ell)} = \mathbb{Z} \perp \sqrt{\ell} \mathbb{Z}$, para ℓ primo, onde $\mathbb{Z} \perp \sqrt{\ell} \mathbb{Z}$ representa o $\mathbb{Z}$ -módulo em (E, b) gerado pela base ortogonal $\mathcal{B} = \{\epsilon_1, \sqrt{\ell} \epsilon_2\}$ para $\{\epsilon_1, \epsilon_2\}$ a base canônica de $\mathbb{R}^2$. Com isso, tem-se que $\mathcal{B}^* = \{\epsilon_1, \frac{1}{\sqrt{\ell}} \epsilon_2\}$. Definindo $\sigma : C_{(\ell)} \rightarrow C_{(\ell)}^\#$ por $\epsilon_1 \xrightarrow{\sigma} \frac{1}{\sqrt{\ell}} \epsilon_2$ e $\sqrt{\ell} \epsilon_2 \xrightarrow{\sigma} \epsilon_1$, segue que se $x = x_1 \epsilon_1 + x_2 \sqrt{\ell} \epsilon_2 \in C_{(\ell)}$, então $\sigma(x) = x_2 \epsilon_1 + x_1 \frac{1}{\sqrt{\ell}} \epsilon_2 \in C_{(\ell)}^\#$ e, assim, se $x = x_1 \epsilon_1 + x_2 \sqrt{\ell} \epsilon_2$ e $y = y_1 \epsilon_1 + y_2 \sqrt{\ell} \epsilon_2$, então $x \cdot y = x_1 y_1 + \ell x_2 y_2$ e $\sigma(x) \cdot \sigma(y) = x_2 y_2 + \frac{1}{\ell} x_1 y_1$ e, portanto,

$$\sigma(x) \cdot \sigma(y) = \ell x \cdot y,$$

para todo $x, y \in C_{(\ell)}$. Logo, $C_{(\ell)}$ é modular de grau ℓ em E . Mais geralmente, para todo inteiro positivo ℓ , podemos considerar em $(\mathbb{R}^{d(\ell)}, \cdot)$, onde $d(\ell) = \sum_{d|\ell} 1$ é o número de divisores de ℓ , o reticulado ℓ -modular

$$C_{(\ell)} = \perp_{d|\ell} \sqrt{d} \mathbb{Z},$$

que representa o reticulado gerado pela base $\mathcal{B} = \{\sqrt{d_1} \epsilon_1, \sqrt{d_2} \epsilon_2, \dots, \sqrt{d_{d(\ell)}} \epsilon_{d(\ell)}\}$, onde $\{\epsilon_1, \epsilon_2, \dots, \epsilon_{d(\ell)}\}$ a base canônica de $\mathbb{R}^{d(\ell)}$.

Proposição 1.6.5. Se L em (E, b) é um reticulado ℓ -modular, então $L \simeq \sqrt{\ell} L^\#$.

Demonstração: Das Proposições 1.3.5 e 1.3.6 segue que $L \simeq {}^\ell L^\#$ e ${}^\ell L^\# \simeq \sqrt{\ell} L^\#$ e, portanto, $L \simeq \sqrt{\ell} L^\#$. ■

O determinante de um reticulado modular é unicamente determinado pelo grau de modularidade e pelo seu posto como veremos a seguir:

Proposição 1.6.6. Se L em (E, b) é um reticulado ℓ -modular, então

$$\det(L) = \ell^{n/2},$$

onde $n = \dim_{\mathbb{R}} E$.

Demonstração: Se $\{v_1, v_2, \dots, v_n\}$ é uma base de $L^\#$, então $\{\sqrt{\ell} v_1, \sqrt{\ell} v_2, \dots, \sqrt{\ell} v_n\}$ é uma base de $\sqrt{\ell} L^\#$. Logo, tem-se que

$$\begin{aligned} \det(\sqrt{\ell} L^\#) &= \det(b(\sqrt{\ell} v_i, \sqrt{\ell} v_j)_{n \times n}) = \det((\ell b(v_i, v_j))_{n \times n}) \\ &= \ell^n \det(b(v_i, v_j)_{n \times n}) = \ell^n \det(L^\#) \\ &= \ell^n \det(L)^{-1}, \end{aligned}$$

ou seja, $\det(L) \det(\sqrt{\ell} L^\#) = \ell^n$. Da Proposição 1.6.5, segue $\det(L) = \det(\sqrt{\ell} L^\#)$ e, portanto, $\det(L) = \ell^{n/2}$. ■

Observe na Proposição 1.6.6 que devemos ter $n \in 2\mathbb{Z}$ a menos que ℓ seja um quadrado perfeito. O resultado a seguir fornece uma cota superior para a norma de um reticulado modular com graus especiais. Omitiremos sua demonstração por tratar com técnicas e ferramentas que fogem ao propósito deste texto.

Teorema 1.6.7. [15] *Se L é um reticulado par e ℓ -modular com $\ell = 1$ ou um primo satisfazendo $(\ell + 1) \mid 24$, então tem-se*

$$\min(L) \leq 2 \left\lfloor \frac{(\ell + 1)n}{48} \right\rfloor .$$

Conclusão

Neste capítulo apresentamos o objeto central deste trabalho junto com suas principais propriedades. Estudamos seus invariantes, os conceitos de paridade e integralidade e como essas noções se relacionam com o reticulado dual, introduzido na Seção 1.3. Introduzimos também os empacotamentos por reticulados, onde vimos os parâmetros de densidade de um empacotamento deste tipo a partir dos invariantes do reticulado. Por último, apresentamos a definição de reticulado modular, que generaliza o conceito de reticulado unimodular, e também as consequências imediatas dessa noção nos invariantes do reticulado.

Capítulo 2

Theta séries e formas modulares

Neste capítulo, tratamos da exposição da teoria de theta série de um reticulado com certas propriedades num espaço euclidiano. Tal tratamento visa estabelecer a conexão da theta série de alguns reticulados com formas modulares para o grupo modular e, mais geralmente, para um de seus grupos de congruência. Com isso, formalizamos inicialmente a definição de theta série de um reticulado par bem como apresentamos algumas propriedades especialmente no que refere-se a relação entre a theta série de um reticulado e a theta série de seu reticulado dual. Na seção 2.1, introduzimos o conceito de formas modulares junto com seus principais resultados e mostramos que a theta série de reticulados unimodulares pares são formas modulares para o grupo modular. Finalizamos o capítulo apresentando a generalização da relação de theta séries de reticulados modulares pares com formas modulares.

2.1 Theta séries

Consideremos (E, b) um espaço euclidiano n -dimensional. A seguir definimos a transformada de Fourier de uma função de E com valores complexos. Tal conceito será usado adiante nos resultados relacionados à theta série de um reticulado.

Definição 2.1.1. Para uma função $f : E \longrightarrow \mathbb{C}$, definimos, sempre que houver sentido¹, a *transformada de Fourier de f* como sendo a função $\hat{f} : E \longrightarrow \mathbb{C}$ dada

¹Nos referimos à convergência da integral.

por

$$\widehat{f}(y) = \int_E f(x) e^{-2\pi \mathbf{i} \cdot b(x,y)} d\mu(x) ,$$

onde μ representa a medida de E definida na Seção 1.1 e $\mathbf{i} = \sqrt{-1}$.

Exemplo 2.1.2. A função $h(x) = e^{-\pi b(x,x)}$ satisfaz $\widehat{h} = h$. De fato, identificando (E, b) com $(\mathbb{R}^n, \cdot)$ através de uma isometria, a medida μ identifica-se com a medida de Lebesgue $dx = dx_1 dx_2 \dots dx_n$. Logo, é equivalente mostrarmos o resultado para a função $h(x) = e^{-\pi x \cdot x} = \prod_{i=1}^n e^{-\pi x_i^2}$, onde $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$. Assim, para $x = (x_1, x_2, \dots, x_n)$ e $y = (y_1, y_2, \dots, y_n)$ tem-se que $e^{-2\pi \mathbf{i} x \cdot y} = \prod_{i=1}^n e^{-2\pi \mathbf{i} x_i y_i}$ e daí

$$\widehat{h}(y) = \int_{\mathbb{R}^n} \prod_{i=1}^n e^{-\pi x_i^2} \prod_{i=1}^n e^{-2\pi \mathbf{i} x_i y_i} dx = \int_{\mathbb{R}^n} \prod_{i=1}^n e^{-\pi x_i^2} e^{-2\pi \mathbf{i} x_i y_i} dx .$$

Com isso, pelo Teorema de Fubini, segue que

$$\widehat{h}(y) = \int_{\mathbb{R}} \int_{\mathbb{R}} \dots \int_{\mathbb{R}} \prod_{i=1}^n e^{-\pi x_i^2} e^{-2\pi \mathbf{i} x_i y_i} dx = \prod_{i=1}^n \int_{\mathbb{R}} e^{-\pi x_i^2} e^{-2\pi \mathbf{i} x_i y_i} dx_i = \prod_{i=1}^n \widehat{e^{-\pi x_i^2}} .$$

Assim, basta mostrarmos o resultado para o caso em que $n = 1$. Seja, portanto, $h(x) = e^{-\pi x^2}$. Com isso, a transformada de h , para $y \in \mathbb{R}$, é dada por

$$\widehat{h}(y) = \int_{\mathbb{R}} e^{-\pi x^2} e^{-2\pi \mathbf{i} x y} dx ,$$

e derivando obtemos

$$\frac{d\widehat{h}}{dy}(y) = \int_{\mathbb{R}} e^{-\pi x^2} \frac{d}{dy} (e^{-2\pi \mathbf{i} x y}) dx = \mathbf{i} \int_{\mathbb{R}} -2\pi x e^{-\pi x^2} e^{-2\pi \mathbf{i} x y} dx .$$

Utilizando $u(x) = e^{-2\pi \mathbf{i} x y}$ e $v'(x) = -2\pi x e^{-\pi x^2}$ e fazendo uso de integração por partes na integral, segue que

$$\begin{aligned} \frac{d\widehat{h}}{dy}(y) &= \mathbf{i} \left(\underbrace{e^{-\pi x^2} e^{-2\pi \mathbf{i} x y}}_0 \Big|_{\mathbb{R}} - \int_{\mathbb{R}} -2\pi \mathbf{i} y e^{-\pi x^2} e^{-2\pi \mathbf{i} x y} dx \right) \\ &= 2\pi \mathbf{i}^2 y \int_{\mathbb{R}} e^{-\pi x^2} e^{-2\pi \mathbf{i} x y} dx , \end{aligned}$$

já que $e^{-2\pi \mathbf{i} x y}$ é limitada e $e^{-\pi x^2} \rightarrow 0$. Assim, $\frac{d\widehat{h}}{dy}(y) = -2\pi y \widehat{h}(y)$. Agora, utilizando a derivação de $g(y) = \widehat{h}(y)/e^{-\pi y^2}$, tem-se que $\frac{dg}{dy} = 0$ e, assim, $\widehat{h}(y) = C e^{-\pi y^2}$, para alguma constante C . Mas, sendo

$$\widehat{h}(0) = C = \int_{\mathbb{R}} e^{-\pi x^2} dx ,$$

segue que $C = 1$ e, portanto, $\widehat{h} = h$.

Consideremos o resultado a seguir para transformadas de Fourier:

Lema 2.1.3. *Seja uma função $f : E \longrightarrow \mathbb{C}$ tal que sua transformada de Fourier $\widehat{f} : E \longrightarrow \mathbb{C}$ esteja bem definida. Se $f_A(x) = f(Ax)$, para $A \in GL_n(\mathbb{R})$, então*

$$\widehat{f}_A(y) = |\det(A)|^{-1} \widehat{f}((A^t)^{-1}y) .$$

Demonstração: Tem-se que

$$\begin{aligned} \widehat{f}_A(y) &= \int_E f_A(x) \cdot e^{-2\pi i b(x,y)} d\mu(x) \\ &= \int_E f(Ax) e^{-2\pi i b(x,y)} d\mu(x) \\ &= \int_E f(x') e^{-2\pi i b(A^{-1}x',y)} |\det(A^{-1})| d\mu(x') \quad (x = A^{-1}x') \\ &= \int_E f(x') e^{-2\pi i b(A^{-1}x',y)} |\det(A)|^{-1} d\mu(x') \\ &= |\det(A)|^{-1} \int_E f(x') e^{-2\pi i b(x', (A^t)^{-1}y)} d\mu(x') \\ &= |\det(A)|^{-1} \widehat{f}((A^t)^{-1}y) , \end{aligned}$$

o que prova o lema. ■

Lema 2.1.4. [8] *Se $f : \mathbb{R}^n \longrightarrow \mathbb{C}$ é uma função satisfazendo*

1. $\int_{\mathbb{R}^n} |f(x)| dx < +\infty$;
 2. $\sum_{x \in \mathbb{Z}^n} |f(x+u)|$ converge uniformemente para $u \in K$, para todo $K \subseteq \mathbb{R}^n$ compacto;
 3. $\sum_{y \in \mathbb{Z}^n} |\widehat{f}(y)| < +\infty$,
- então vale

$$\sum_{u \in \mathbb{Z}^n} f(u) = \sum_{y \in \mathbb{Z}^n} \widehat{f}(y) .$$

O resultado a seguir generaliza o Lema 2.1.4 para qualquer reticulado e seu dual em espaços euclidianos.

Teorema 2.1.5. (Fórmula da Soma de Poisson) *Se L é um reticulado em (E, b) e $f : E \longrightarrow \mathbb{C}$ é uma função satisfazendo*

1. $\int_E |f(x)| d\mu < +\infty$;
 2. $\sum_{x \in L} |f(x+u)|$ converge uniformemente para $u \in K$, para todo $K \subseteq E$ compacto;
 3. $\sum_{y \in L^\#} |\widehat{f}(y)| < +\infty$,
- então

$$\sum_{x \in L} f(x) = \det(L)^{-1/2} \sum_{y \in L^\#} \widehat{f}(y) .$$

Demonstração: Identificando (E, b) com $(\mathbb{R}^n, \cdot)$ através de uma isometria, tem-se que $L = M\mathbb{Z}^n$ com $M \in \text{GL}_n(\mathbb{R})$ (note que M é uma matriz geradora de L). Assim, pelo Lema 2.1.4, segue que

$$\sum_{x \in L} f(x) = \sum_{u \in \mathbb{Z}^n} f(Mu) = \sum_{u \in \mathbb{Z}^n} f_M(u) = \sum_{y \in \mathbb{Z}^n} \widehat{f}_M(y) .$$

De acordo com o Lema 2.1.3, tem-se que $\widehat{f}_M(y) = |\det(M)|^{-1} \widehat{f}((M^t)^{-1}y)$ e, deste modo,

$$\sum_{y \in L} f(x) = |\det(M)|^{-1} \sum_{y \in \mathbb{Z}^n} \widehat{f}((M^t)^{-1}y) .$$

Mas, pela Proposição 1.4.7, segue que $L^\# = (M^t)^{-1}\mathbb{Z}^n$. Assim, sendo $|\det(M)| = \Delta_L = \det(L)^{1/2}$, segue que

$$\sum_{y \in L} f(x) = \det(L)^{-1/2} \sum_{y \in L^\#} \widehat{f}(y) ,$$

o que prova o teorema. ■

A seguir, apresentamos o conceito de theta série de reticulados pares e suas propriedades:

Definição 2.1.6. Seja L um reticulado par em (E, b) . Definimos a *theta série de L* por

$$\Theta_L(z) = \sum_{x \in L} q^{b(x,x)/2} ,$$

onde $q = e^{2\pi iz}$ e $z \in \mathbb{H} = \{z \in \mathbb{C} ; \text{Im}(z) > 0\}$.

Notemos que, de acordo com a Definição 2.1.6, podemos escrever

$$\Theta_L(q) = \sum_{k=0}^{+\infty} a_k q^k , \tag{2.1}$$

onde $a_k = \#\{x \in L ; b(x, x) = 2k\}$, ou seja, a_k fornece o número de elementos de L que pertencem à fronteira de $B[0, \sqrt{2k}]$, como é possível notar no exemplo a seguir:

Exemplo 2.1.7. A Figura 2.1 ilustra como são dados os coeficientes da theta série Θ_L para $L = \sqrt{2}\mathbb{Z}^2$, representados pelo número de pontos de L nos círculos coloridos. Com isso, tem-se que

$$\Theta_L(z) = \sum_{k=0}^{+\infty} a_k q^k = 1 + 4q + 4q^2 + 4q^4 + 8q^5 + 4q^8 + 4q^9 + \dots$$

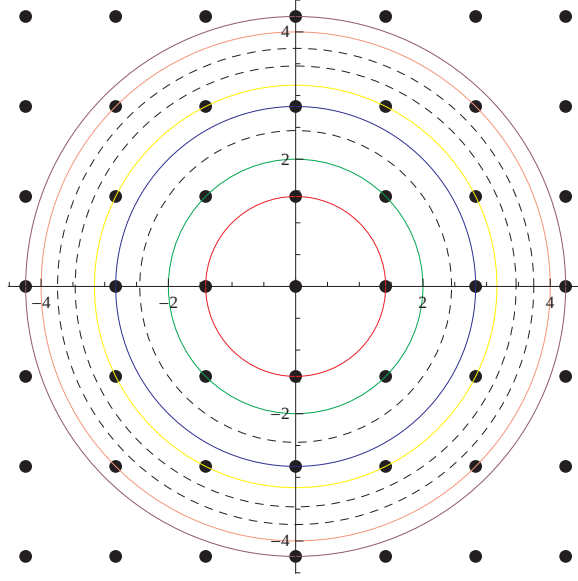


Figura 2.1: Reticulado $\sqrt{2}\mathbb{Z}^2$.

Agora, com a Equação (2.1), denotando para cada inteiro positivo k_0 a respectiva soma $N_{k_0} = \sum_{k=0}^{k_0} a_k$ que é o número de elementos de L em $B[0, \sqrt{2k}]$, segue que o número a_k é finito para todo inteiro k positivo, já que $a_k \leq N_k$ e N_k é finito pois L é discreto e $B[0, \sqrt{2k}]$ é limitado em E . Além disso, notemos que Θ_L está bem definida, pois quando $k \rightarrow \infty$, tem-se que N_k cresce proporcionalmente ao volume $\mu(B[0, \sqrt{2k}])$, uma vez que N_k é estimado por $\frac{\mu(B[0, \sqrt{2k}])}{\mu(V_L(0))}$ e $\mu(V_L(0))$ é invariante. Como $\mu(B[0, \sqrt{2k}])$ é da ordem de $k^{n/2}$, logo temos $N_k \leq Ck^{n/2}$, para k suficientemente grande e C uma constante adequada. Assim,

$$\lim_{k \rightarrow \infty} a_k^{1/k} \leq \lim_{k \rightarrow \infty} C^{1/k} k^{n/2k} = 1 ,$$

e, portanto, tem-se que o raio de convergência R de Θ_L é $R \geq 1$ e, em particular, Θ_L converge para $q \in \mathbb{C}$ com $|q| < 1$, o que equivale a $z \in \mathbb{H}$, pois

$$|e^{2\pi i(Re(z) + Im(z)i)}| = e^{-2\pi Im(z)} \underbrace{|\cos(2\pi Re(z)) + i \sin(2\pi Re(z))|}_1 = e^{-2\pi Im(z)} < 1 \Leftrightarrow Im(z) > 0 .$$

Com isso mostramos que Θ_L está bem definida. O resultado seguinte nos mostrará que Θ_L converge uniformemente nas partes compactas de $\mathbb{H}$, resultado que nos permitirá concluir sobre sua analiticidade (ou holomorfia) em $\mathbb{H}$.

Lema 2.1.8. *Se L é um reticulado em (E, b) , então $\Theta_L(z) = \sum_{x \in L} e^{\pi i z b(x, x)}$ converge uniformemente e absolutamente para todo $z \in \mathbb{C}$ com $Im(z) \geq v_0 > 0$.*

Demonstração: Identificamos o espaço E com $\mathbb{R}^n$ através de uma isometria que leva uma base ortonormal $\{\epsilon_1, \epsilon_2, \dots, \epsilon_n\}$ de $\mathbb{R}^n$ em uma ortonormal de E . Sejam

$L = M\mathbb{Z}^n$ onde $M \in \text{GL}_n(\mathbb{R})$ é a matriz geradora de L e

$$\epsilon = \inf_{\substack{u \in \mathbb{R}^n \\ \|u\|=1}} \{b(Mu, Mu)\} .$$

Com isso, tem-se que $\epsilon > 0$ e $b(Mu, Mu) \geq \epsilon u^2$ para todo $u \in \mathbb{R}^n$. Deste modo, considerando $\text{Im}(z) \geq v_0$, segue que

$$\begin{aligned} \sum_{x \in L} |e^{\pi i z b(x, x)}| &= \sum_{u \in \mathbb{Z}^n} |e^{\pi i z b(Mu, Mu)}| \\ &= \sum_{u \in \mathbb{Z}^n} e^{-\pi \text{Im}(z) b(Mu, Mu)} \\ &\leq \sum_{u \in \mathbb{Z}^n} e^{-\pi v_0 b(Mu, Mu)} \\ &\leq \sum_{u \in \mathbb{Z}^n} e^{-\pi v_0 \epsilon u^2} \\ &= \left(\sum_{r=-\infty}^{\infty} e^{-\pi v_0 \epsilon r^2} \right)^n < \infty , \end{aligned}$$

o que prova o resultado. ■

Desde que Θ_L pode ser escrita por uma série de funções $\sum_{k=1}^{\infty} f_k$ cujos termos $f_k(z) = a_k e^{\pi i z k}$ são holomorfos (são uma composição de funções holomorfas), segue, da convergência uniforme dada no Lema 2.1.8, que a Θ_L é holomorfa em $\mathbb{H}$.

Lema 2.1.9. *A transformada de Fourier da função $f(x) = e^{-\pi \frac{1}{t}(x+\rho)^2}$, onde $x, t, \rho \in \mathbb{R}$ com $t > 0$ é*

$$\widehat{f}(y) = \sqrt{t} e^{2\pi i \rho y} e^{-\pi t y^2} .$$

Demonstração: Tem-se que

$$\widehat{f}(y) = \int_{\mathbb{R}} e^{-\pi(\frac{1}{t})(x+\rho)^2} e^{-2\pi i x y} dx .$$

Utilizando a mudança de coordenadas $u = \frac{x+\rho}{\sqrt{t}}$, ou seja, com $x = \sqrt{t}u - \rho$, segue que

$$\widehat{f}(y) = \int_{\mathbb{R}} e^{-\pi u^2} e^{-2\pi i [u(\sqrt{t}y) - \rho y]} \sqrt{t} du = \sqrt{t} e^{2\pi i \rho y} \int_{\mathbb{R}} e^{-\pi u^2} e^{-2\pi i u(\sqrt{t}y)} du . \quad (2.2)$$

Como $\widehat{h}(y) = e^{-\pi y^2}$, para $h(x) = e^{-\pi x^2}$, segue da Equação (2.2) que

$$\widehat{f}(y) = \sqrt{t} e^{2\pi i \rho y} e^{-\pi(\sqrt{t}y)^2} = \sqrt{t} e^{2\pi i \rho y} e^{-\pi t y^2} ,$$

o que prova o lema. ■

Teorema 2.1.10. *Se L é um reticulado par em (E, b) , então*

$$\Theta_{L^\#}(z) = \det(L)^{1/2} (\mathbf{i}/z)^{n/2} \Theta_L(-1/z) . \quad (2.3)$$

Demonstração: Sendo ambos os lados da Equação (2.3) funções holomorfas em $\mathbb{H}$, pelo Teorema da Identidade², é suficiente provar tal identidade para $z = \mathbf{i}t$, onde $t \in \mathbb{R}$ com $t > 0$, desde que tal conjunto de pontos de $\mathbb{H}$ possui ponto de acumulação em $\mathbb{H}$. Com isso, considerando a função $g(x) = e^{-\pi(\frac{1}{t})b(x,x)}$ e tomando uma isometria de E com $\mathbb{R}^n$, segue que $\widehat{g}$ é obtida através do cálculo da Transformada de Fourier da função $e^{-\pi\frac{1}{t}x^2}$ para $x \in \mathbb{R}^n$. Mas, como feito no Exemplo 2.1.2, podemos nos restringir ao caso $n = 1$ e, portanto, ao cálculo de $\widehat{f}$ para $f(x) = e^{-\pi\frac{1}{t}x^2}$ onde $x \in \mathbb{R}$. Assim, pelo Lema 2.1.9, segue que $\widehat{f}(y) = \sqrt{t}e^{-\pi ty^2}$ de onde segue que $\widehat{g}(y) = t^{n/2}e^{-\pi tb(y,y)}$. Assim, pela Fórmula da Soma de Poisson (Teorema 2.1.5), tem-se que

$$\begin{aligned} \Theta_L(-\frac{1}{\mathbf{i}t}) &= \sum_{x \in L} e^{\pi \mathbf{i}(-\frac{1}{\mathbf{i}t})b(x,x)} \\ &= \sum_{x \in L} e^{-\pi(\frac{1}{t})b(x,x)} \\ &= \det(L)^{-1/2} \sum_{x \in L^\#} t^{n/2} e^{-\pi tb(y,y)} \\ &= t^{n/2} \det(L)^{-1/2} \sum_{x \in L^\#} e^{-\pi tb(y,y)} \\ &= t^{n/2} \det(L)^{-1/2} \sum_{x \in L^\#} e^{\pi \mathbf{i}(t\mathbf{i})b(y,y)} \\ &= t^{n/2} \det(L)^{-1/2} \Theta_{L^\#}(\mathbf{i}t) . \end{aligned}$$

Como $z = \mathbf{i}t$, segue que $t = z/\mathbf{i}$ e, portanto, temos o resultado. ■

2.2 Theta séries como formas modulares

Consideremos o semiplano superior $\mathbb{H}$ e Γ o subgrupo linear

$$\mathrm{SL}_2(\mathbb{Z}) = \{\lambda \in \mathrm{GL}_2(\mathbb{Z}) ; \det(\lambda) = 1\}$$

de $\mathrm{GL}_2(\mathbb{Z})$, o qual chamamos de *grupo modular completo*. Consideremos ainda, para cada $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, a transformação linear fracionária dada por

$$\lambda \longmapsto \lambda z = \frac{az + b}{cz + d} ,$$

²(**Teorema da Identidade**) [17] Sejam F e G funções holomorfas de uma região conexa $H \subseteq \mathbb{C}$ em $\mathbb{C}$. Então $F = G$ se, e somente se, o conjunto $\{z \in H ; F(z) = G(z)\}$ tem um ponto de acumulação em H .

para todo $z \in \mathbb{H}$. Assim, notando que se $z \in \mathbb{H}$, então $\lambda z \in \mathbb{H}$, pois

$$\operatorname{Im}(\lambda z) = \operatorname{Im} \left(\frac{(az + b)(c\bar{z} + d)}{|cz + d|^2} \right) = \frac{\operatorname{Im}(adz + bc\bar{z})}{|cz + d|^2}.$$

Deste modo, como $\operatorname{Im}(adz + bc\bar{z}) = \det(\lambda)\operatorname{Im}(z) = \operatorname{Im}(z)$, segue que

$$\operatorname{Im}(\lambda z) = \frac{\operatorname{Im}(z)}{|cz + d|^2} > 0.$$

Temos portanto definido uma ação de Γ em $\mathbb{H}$. Como $\{\pm I\} \subset \operatorname{SL}_2(\mathbb{Z})$ age trivialmente em $\mathbb{H}$, ou seja, $\pm Iz = z$, segue que podemos considerar

$$G = \operatorname{SL}_2(\mathbb{Z})/\{\pm I\},$$

que chamamos *grupo modular* e cujos os elementos serão denotados sem as barras. Desta forma, os elementos

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

de G , agem em $\mathbb{H}$, respectivamente, por

$$z \xrightarrow{S} \frac{-1}{z} \quad \text{e} \quad z \xrightarrow{T} z + 1.$$

O resultado a seguir caracteriza G através de seus geradores. Omitiremos sua demonstração por fugir dos propósitos deste texto.

Teorema 2.2.1. *O grupo modular G é gerado por S e T .*

Demonstração: Ver ([8], Cap. 2, §2). ■

Veremos a seguir o conceito de formas modulares que, a grosso modo, são funções sobre $\mathbb{H}$ que possuem bom comportamento com relação à ação do grupo modular completo Γ em $\mathbb{H}$.

Definição 2.2.2. Seja $k \in \mathbb{Z}$. Dizemos que uma função holomorfa $f : \mathbb{H} \rightarrow \mathbb{C}$ é uma *forma modular de peso k para Γ* e denotamos $f \in \mathcal{M}_k(\Gamma)$, se satisfaz:

- (i) $f(\lambda z) = (cz + d)^k f(z)$, para todo $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$;
- (ii) f é escrita como série de potência em $q = e^{2\pi iz}$.

Note que se k é ímpar, então toda forma modular de peso k para Γ é nula, visto que para $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, tem-se que $f(z) = (-1)^k f(z)$ e, portanto, $f(z) = 0$ para todo $z \in \mathbb{H}$. Portanto, podemos supor, sem perda de generalidade, que o inteiro k é par.

Proposição 2.2.3. *Se $f : \mathbb{H} \rightarrow \mathbb{C}$ é uma função holomorfa, então $f \in \mathcal{M}_k(\Gamma)$ se, e somente se, satisfaz $f(z+1) = f(z)$, $f(-1/z) = z^k f(z)$ para todo $z \in \mathbb{H}$ e f possui uma expansão em série de potências em $q = e^{2\pi iz}$.*

Demonstração: Se $f \in \mathcal{M}_k(\Gamma)$, então o resultado segue da Definição 2.2.2 e do Teorema 2.2.1. Reciprocamente, como

$$\frac{d(\lambda z)}{dz} = \frac{d}{dz} \left(\frac{az+b}{cz+d} \right) = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{ad-bc}{(cz+d)^2} = \frac{1}{(cz+d)^2},$$

segue que podemos escrever

$$f(\lambda z) = (cz+d)^k f(z) \quad (2.4)$$

como

$$f(\lambda z) \left(\frac{d(\lambda z)}{dz} \right)^{k/2} = f(z)$$

e daí segue que $f(\lambda z)d(\lambda z)^{k/2} = f(z)dz^{k/2}$. Assim, tem-se $f(z)dz^{k/2}$ invariante para multiplicação por λ , o que mostra que se a Equação (2.4) é satisfeita para $\lambda_1, \lambda_2 \in \Gamma$, então é válida também para $\lambda_1\lambda_2$. Desta forma, é suficiente analisá-la para T e S , uma vez G é gerado por tais elementos. Como

$$f(Tz) = f(z+1) = f(z) \quad \text{e} \quad f(Sz) = f(-1/z) = z^k f(z),$$

para todo $z \in \mathbb{H}$, tem-se provada a proposição. ■

Os próximos resultados permitem estabelecer uma relação entre theta séries de reticulados unimodulares pares com formas modulares para o grupo modular Γ .

Teorema 2.2.4. *Se L é um reticulado unimodular par em (E, b) , então*

$$n \equiv 0 \pmod{8}.$$

Demonstração: Suponhamos que $8 \nmid n$. Assim, sem perda de generalidade, podemos tomar $n \equiv 4 \pmod{8}$, já que caso contrário é possível substituir o reticulado L por $L \oplus L$ ou $L \oplus L \oplus L \oplus L$ que são ambos unimodulares e pares (basta notar que uma matriz Gram desses reticulados são formadas por blocos de alguma matriz Gram de L) de modo que o posto obtido seja cômputo a 4 módulo 8 e a aplicar a argumentação que segue. Como L é unimodular, segue que $L = L^\#$ e $\det(L) = 1$. Deste modo, pelo Teorema 2.1.10, tem-se, para todo $z \in \mathbb{H}$, que

$$\Theta_L(Sz) = \Theta_L(-1/z) = -z^{n/2} \Theta_L(z),$$

pois $n/2 \equiv 2 \pmod{4}$ e, com isso, $\mathbf{i}^{n/2} = -1$. Ainda, do fato de L ser par, segue, para todo $z \in \mathbb{H}$, que

$$\Theta(Tz) = \Theta_L(z+1) = \sum_{x \in L} e^{\pi \mathbf{i} z \cdot b(x,x)} e^{\pi \mathbf{i} \cdot b(x,x)} = \sum_{x \in L} e^{\pi \mathbf{i} z \cdot b(x,x)} = \Theta_L(z) . \quad (2.5)$$

Assim, tem-se que $\Theta_L((TS)z) = -z^{n/2}\Theta_L(z)$, para todo $z \in L$. Agora, notemos que $(TS)^3 = 1$ pois

$$z \xrightarrow{\text{S}} -\frac{1}{z} \xrightarrow{\text{T}} \frac{z-1}{z} \xrightarrow{\text{S}} -\frac{z}{z-1} \xrightarrow{\text{T}} -\frac{1}{z-1} \xrightarrow{\text{S}} z-1 \xrightarrow{\text{T}} z . \quad (2.6)$$

Assim,

$$\begin{aligned} \Theta_L(z) &= \Theta_L((TS)^3 z) \\ &= (-1)((TS)^2 z)^{n/2} \Theta_L((TS)^2 z) \\ &= (-1)((TS)^2 z)^{n/2} (-1)((TS)z)^{n/2} \Theta_L((TS)z) \\ &= (-1)((TS)^2 z)^{n/2} (-1)((TS)z)^{n/2} (-1)z^{n/2} \Theta_L(z) \\ &= (-1)((TS)^2 z)^{n/2} ((TS)z)^{n/2} z^{n/2} \Theta_L(z) . \end{aligned} \quad (2.7)$$

Pelas relações em (2.6), segue que

$$((TS)^2 z)^{n/2} ((TS)z)^{n/2} z^{n/2} = \left(\frac{-1}{z-1} \frac{z-1}{z} z \right)^{n/2} = (-1)^{n/2} .$$

Da Equação (2.7), segue que

$$\Theta_L(z) = (-1)(-1)^{n/2} \Theta_L(z) = -\Theta_L(z) ,$$

implicando que $\Theta_L = 0$ e, portanto, $L = \emptyset$ o que nos leva ao absurdo. ■

Com isso, temos o seguinte resultado para Θ_L , com L um reticulado unimodular par.

Teorema 2.2.5. *Se L é um reticulado unimodular par em (E, b) , então $\Theta_L(z) \in \mathcal{M}_k(\Gamma)$ para $k = n/2$.*

Demonstração: De acordo com a Proposição 2.2.3, é suficiente mostrar que

$$\Theta_L(z+1) = \Theta_L(z) \text{ e } \Theta_L(-1/z) = z^{n/2} \Theta_L(z) ,$$

uma vez que da Equação (2.1), segue que Θ_L pode ser escrita como uma série de potências em $q = e^{2\pi \mathbf{i} z}$. A primeira igualdade decorre da paridade de L como na Equação (2.5). Já a segunda, como $L = L^\#$ e $\det(L) = 1$, segue, pelo Teorema 2.1.10, que

$$\Theta_L(-1/z) = \det(L)^{-1/2} (z/\mathbf{i})^{n/2} \Theta_{L^\#}(z) = z^{n/2} \Theta_L(z) ,$$

já que $n \equiv 0 \pmod{8}$ implica que $n/2 \equiv 0 \pmod{4}$ e, com isso, $i^{n/2} = 1$. Portanto, tem-se que Θ_L é uma forma modular de peso $n/2$ para Γ . ■

Exemplo 2.2.6. Um exemplo de reticulado unimodular par é o reticulado E_8 definido por

$$E_8 = \{(\alpha_1, \alpha_2, \dots, \alpha_8) \in \mathbb{R}^8 ; \alpha_i \in \mathbb{Z} \text{ ou } \alpha_i \in \mathbb{Z} + 1/2 \text{ com } \sum \alpha_i \equiv 0 \pmod{2}\} .$$

Com o auxílio da estrutura de $\mathcal{M}_4(\Gamma)$ é possível mostrar que E_8 é, a menos de isomorfismos, o único reticulado unimodular par em dimensão 8 e que sua theta série é dada por

$$\Theta_{E_8} = 1 + 240(q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + \dots) .$$

2.3 Theta séries de reticulados modulares pares

Consideremos N um inteiro positivo. Chamamos de *subgrupo principal de congruência de grau N* o conjunto

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma ; a \equiv d \equiv 1 \pmod{N} \text{ e } b \equiv c \equiv 0 \pmod{N} \right\} .$$

É simples ver que $\Gamma(N)$ é um subgrupo de Γ e que, em particular, tem-se que $\Gamma(1) = \Gamma$. Dizemos que um subgrupo Γ' de Γ é um *subgrupo de congruência*, se existe $N \in \mathbb{N}$ tal que $\Gamma(N) \subset \Gamma'$. Neste caso, dizemos que Γ' é um subgrupo de congruência de grau N .

Os principais grupos de congruências de Γ são

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma ; c \equiv 0 \pmod{N} \right\}$$

e

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) ; a \equiv 1 \pmod{N} \right\} .$$

Observe que

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma .$$

Além disso, tem-se os seguintes isomorfismos de grupos

$$\Gamma_1(N)/\Gamma(N) \xrightarrow{\cong} \mathbb{Z}/N\mathbb{Z} \quad \text{e} \quad \Gamma_0(N)/\Gamma_1(N) \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^\times , \quad (2.8)$$

uma vez que considerando os homomorfismos sobrejetores de grupos

$$\Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z} \quad ; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto b \pmod{N}$$

e

$$\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \quad ; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto d \pmod{N}$$

tem-se $\Gamma(N)$ e $\Gamma_1(N)$ como seus respectivos núcleos e, com isso, obtém-se os isomorfismos de grupos.

Definição 2.3.1. Sejam $f : \mathbb{H} \longrightarrow \mathbb{C}$ uma função e $k \in \mathbb{Z}$. Para $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, definimos

$$(f|_k \lambda)(z) = (cz + d)^{-k} f(\lambda z) .$$

Notemos que o símbolo introduzido na Definição 2.3.1 satisfaz a seguinte propriedade:

$$(f|_k(\lambda_1 \lambda_2))(z) = ((f|_k \lambda_1)|_k \lambda_2)(z), \quad (2.9)$$

para quaisquer $\lambda_1, \lambda_2 \in \Gamma$. Agora, estamos aptos a definir o que são formas modulares para subgrupos de congruências.

Definição 2.3.2. Sejam $k \in \mathbb{Z}$, Γ' um subgrupo de congruência de grau N e ε um caracter³ de Γ' . Uma função holomorfa $f : \mathbb{H} \longrightarrow \mathbb{C}$ é dita uma *forma modular de peso k para Γ' com caracter ε* , denotada por $f \in \mathcal{M}_k(\Gamma', \varepsilon)$, se satisfaz:

- (i) $f|_k \lambda = \varepsilon(\lambda)f$, para todo $\lambda \in \Gamma'$;
- (ii) f é escrita como uma série de potências em $q_N = e^{\frac{2\pi iz}{N}}$.

De agora em diante, sejam L um reticulado par em um espaço euclidiano (E, b) n -dimensional com n par e $\rho \in E$. Aqui, substituiremos $b(x, y)$ por $\langle x, y \rangle$ para simplificar a notação.

Definição 2.3.3. Definimos para todo $z \in \mathbb{H}$ a série

$$\Theta_{\rho+L}(z) = \sum_{x \in \rho+L} e^{\pi i z \langle x, x \rangle} = \sum_{x \in L} e^{\pi i z \langle x+\rho, x+\rho \rangle} .$$

A proposição a seguir, cuja demonstração omitiremos por fugir do escopo deste trabalho, fornece uma expressão que nos permite relacionar formas modulares à theta séries de reticulados modulares e pares.

³Seja J um grupo. Chamamos de *caracter do grupo J* toda aplicação $\varepsilon : J \longrightarrow \mathbb{C}^\times$ que é um homomorfismo de grupos.

Proposição 2.3.4. [8] *Se L é um reticulado ℓ -modular e par, $\rho \in L^\#$ e $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$, então*

$$\Theta_{\rho+L}|_{n/2}\lambda = \varepsilon(\lambda)e^{\pi i ab \langle \rho, \rho \rangle} \Theta_{a\rho+L} ,$$

onde

$$\varepsilon(\lambda) = \begin{cases} \det(L)^{-1/2}(\mathbf{i}c)^{-n/2} \sum_{\bar{\gamma} \in L/cL} e^{\pi i \frac{a}{c} \langle \gamma, \gamma \rangle} & , \text{ para } c \neq 0 \\ d^{-n/2} & , \text{ para } c = 0 \end{cases} .$$

Em particular, se $\rho = 0$ na Proposição 2.3.4, então Θ_L satisfaz

$$\Theta_L|_{n/2}\lambda = \varepsilon(\lambda)\Theta_L , \text{ para todo } \lambda \in \Gamma_0(\ell) . \quad (2.10)$$

Como, da Equação 2.9, vale

$$\varepsilon(\lambda_1\lambda_2)\Theta_L(z) = (\Theta_L|_{n/2}\lambda_1\lambda_2)(z) = ((\Theta_L|_{n/2}\lambda_1)|_{n/2}\lambda_2)(z) = \varepsilon(\lambda_1)\varepsilon(\lambda_2)\Theta_L(z),$$

para quaisquer $\lambda_1, \lambda_2 \in \Gamma_0(\ell)$, segue que

$$\varepsilon(\lambda_1\lambda_2) = \varepsilon(\lambda_1)\varepsilon(\lambda_2)$$

e, portanto, ε é um caracter do subgrupo de congruência $\Gamma_0(\ell)$. O objetivo, a seguir, é explicitar uma forma simples para ε . Para isto, consideramos os próximos resultados:

Lema 2.3.5. *Se $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$ com $c \neq 0$, então, para todo $t \in \mathbb{Z}$, tem-se*

$$\varepsilon\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \varepsilon\left(\begin{pmatrix} a & b+ta \\ c & d+tc \end{pmatrix}\right) .$$

Demonstração: Segue da Proposição 2.3.4. ■

Lema 2.3.6. [8] *Se $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$ com $c, d \neq 0$, então*

$$\varepsilon(\lambda) = d^{-n/2} \sum_{\bar{\gamma} \in L/dL} e^{\pi i \frac{b}{d} \langle \gamma, \gamma \rangle} .$$

Agora, consideremos para $d \neq 0$, o número

$$G(b, d) = \sum_{\bar{\gamma} \in L/dL} e^{\pi i \frac{b}{d} \langle \gamma, \gamma \rangle} .$$

Lema 2.3.7. Se $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$ com $c, d \neq 0$, então $G(b, d) \in \mathbb{Q}$. Além disso, $G(b, d) = G(1, d)$.

Demonstração: Sendo L par, tem-se que $G(b, d) \in \mathbb{Q}(\zeta)$, onde $\zeta = e^{2\pi i/d}$, uma vez que $G(b, d) = \sum_{\bar{\gamma} \in L/dL} \zeta^{b \langle \gamma, \gamma \rangle / 2}$. Agora, da Proposição 2.3.4 e do Lema 2.3.6, segue, para todo $t \in \mathbb{Z}$, que

$$G(b, d) = d^{n/2} \varepsilon(A) = d^{n/2} (d + tc)^{-n/2} \sum_{\bar{\gamma} \in L/(d+tc)L} e^{\pi i \frac{b+ta}{d+tc} \langle \gamma, \gamma \rangle}.$$

Pelo mesmo raciocínio, concluímos que $G(b, d) \in \mathbb{Q}(\hat{\zeta})$, onde $\hat{\zeta} = e^{2\pi i/(d+tc)}$ para todo inteiro l . Mas, como $\det(\lambda) = ad - cb = 1$, segue que $\text{mdc}(c, d) = 1$ e, com isso, existe $t' \in \mathbb{Z}$ tal que $\text{mdc}(d, d + t'c) = 1$. Assim, tomando $\hat{\zeta} = e^{2\pi i/(d+t'c)}$, tem-se que $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\hat{\zeta}) = \mathbb{Q}$ e, portanto, $G(b, d) \in \mathbb{Q}$. Com isso, $G(b, d)$ é invariante por automorfismos de $\mathbb{Q}(\zeta)$. Tomando o automorfismo $\zeta \mapsto \zeta^b$ em $G(1, d)$, segue que $G(b, d) = G(1, d)$. ■

Lema 2.3.8. O caracter ε só depende de d .

Demonstração: Seja $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$. Pelo Lema 2.3.5 segue que $\varepsilon(\lambda) = \varepsilon\left(\begin{pmatrix} a & b+ta \\ c & d+t\ell \end{pmatrix}\right)$ para todo $t \in \mathbb{Z}$. Assim, se $\lambda \in \Gamma_1(\ell)$, então $d \equiv 1 \pmod{\ell}$ e, com isso, existe $t' \in \mathbb{Z}$ tal que $1 = d + t'\ell$. Deste modo, pela Lema 2.3.6, tem-se que $\varepsilon(\lambda) = \varepsilon\left(\begin{pmatrix} a & b+t'a \\ c & 1 \end{pmatrix}\right) = 1$. Portanto, o caracter $\varepsilon : \Gamma_0(\ell) \rightarrow \mathbb{C}^\times$ se fatora via um caracter de $\Gamma_0(\ell)/\Gamma_1(\ell)$. No entanto, das relações em (2.8), tem-se que $\Gamma_0(\ell)/\Gamma_1(\ell) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$ por $\lambda \mapsto \bar{d}$. Deste modo, ε se fatora via um caracter χ de $(\mathbb{Z}/\ell\mathbb{Z})^\times$ que só depende de $\bar{d}$. ■

O próximo lema faz uso do símbolo introduzido a seguir:

Definição 2.3.9. Sejam p e a números inteiros com p primo e $\text{mdc}(p, a) = 1$. Definimos o símbolo $\left(\frac{a}{p}\right) \in \{\pm 1\}$ pelo número

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}, \text{ se } p \text{ é ímpar}$$

e

$$\left(\frac{a}{p}\right) = (-1)^{(p^2-1)/8}, \text{ se } p = 2.$$

Note que quando p é ímpar, o símbolo acima é chamado *símbolo de Legendre*.

Lema 2.3.10. $\varepsilon(\lambda) = \chi(d) = \left(\frac{\Delta}{d}\right)$, onde $\Delta = (-1)^{n/2} \det(L)$ e $(\cdot)$ é o símbolo de Jacobi-Legendre.

Demonstração: Consideremos os primos $p \neq 2$ tal que $\text{mdc}(p, \ell) = 1$. Assim, existem $t, u \in \mathbb{Z}$ tal que $pt - \ell u = 1$. Deste modo, pela Proposição 2.3.4, com $\lambda = \begin{pmatrix} p & 1 \\ u\ell & t \end{pmatrix}$, tem-se que

$$\begin{aligned}
\chi(\bar{t}) \det(L)^{1/2} (\mathbf{i}u\ell)^{n/2} &= \sum_{\bar{\gamma} \in L/u\ell L} e^{\pi \mathbf{i} \frac{p}{\ell u} \langle \gamma, \gamma \rangle} \\
&= \sum_{\bar{\gamma} \in L/u\ell L} (e^{\frac{\pi \mathbf{i}}{\ell u} \langle \gamma, \gamma \rangle})^p \\
&\equiv \left(\sum_{\bar{\gamma} \in L/u\ell L} e^{\frac{\pi \mathbf{i}}{\ell u} \langle \gamma, \gamma \rangle} \right)^p \pmod{p} \\
&\equiv \left(\varepsilon \begin{pmatrix} 1 & 1 \\ u\ell & pt \end{pmatrix} \det(L)^{1/2} (\mathbf{i}u\ell)^{n/2} \right)^p \pmod{p}.
\end{aligned} \tag{2.11}$$

Agora, como $\varepsilon \begin{pmatrix} 1 & 1 \\ u\ell & pt \end{pmatrix} = 1$ pois $\begin{pmatrix} 1 & 1 \\ u\ell & pt \end{pmatrix} \in \Gamma_1(\ell)$, e $p \nmid \det(L) = \ell^{n/2}$, segue, por (2.11), que

$$\begin{aligned}
\chi(\bar{t}) &\equiv (\det(L)^{1/2} (\mathbf{i}u\ell)^{n/2})^{p-1} \pmod{p} \\
&\equiv (\det(L) (\mathbf{i}u\ell)^n)^{(p-1)/2} \pmod{p}.
\end{aligned} \tag{2.12}$$

Mas, sendo n par, tem-se que $\mathbf{i}^n = (-1)^{n/2}$, pois $4 \mid n$ ou $n \equiv 2 \pmod{4}$, o que equivale a $n/2$ par ou ímpar, respectivamente. Além disso, de $pt - \ell u = 1$, segue que $u\ell \equiv -1 \pmod{p}$ e, com isso, $(u\ell)^n \equiv 1 \pmod{p}$ já que n é par. Assim, de (2.12), tem-se que

$$\chi(\bar{t}) \equiv \Delta^{(p-1)/2} \pmod{p}, \tag{2.13}$$

onde $\Delta = (-1)^{n/2} \det(L)$. Portanto, de (2.13) e da Definição 2.3.9, tem-se

$$\chi(\bar{t}) = \left(\frac{\Delta}{p} \right).$$

Como $\overline{pt} = \bar{1}$ em $(\mathbb{Z}/\ell\mathbb{Z})^\times$, segue que $\chi(\bar{p})\chi(\bar{t}) = 1$, mas $\chi(\bar{p}), \chi(\bar{t}) \in \{\pm 1\}$, logo $\chi(\bar{p}) = \chi(\bar{t})$ e, deste modo, tem-se

$$\chi(\bar{t}) = \left(\frac{\Delta}{p} \right).$$

Assim, se $\bar{d} \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, então $d = p_1^{e_1} \cdots p_s^{e_s}$ com $\text{mdc}(p_i, \ell) = 1$, para $i = 1, \dots, s$. Com isso,

$$\chi(\bar{d}) = \chi(\bar{p}_1^{e_1} \cdots \bar{p}_s^{e_s}) = \left(\frac{\Delta}{p_1} \right)^{e_1} \cdots \left(\frac{\Delta}{p_s} \right)^{e_s},$$

o chamado símbolo de Jacobi-Legendre $(\frac{\Delta}{d})$, provando portanto o lema. ■

Teorema 2.3.11. *Seja L reticulado par e ℓ -modular em (E, b) com um espaço euclidiano de dimensão n par. Então Θ_L é uma forma modular de peso $n/2$ para $\Gamma_0(\ell)$ com caracter χ dado por $\chi(d) = \left(\frac{\Delta}{d}\right)$ (símbolo de Jacobi-Legendre) para $\Delta = (-1)^{n/2} \det(L)$.*

Demonstração: Sendo L um reticulado ℓ -modular, pela Proposição 1.6.5, segue que $L \simeq \sqrt{\ell}L^\#$, ou seja, existe uma isometria σ tal que $\sigma(L) = \sqrt{\ell}L^\#$. Com isso,

$$\Theta_L(z) = \sum_{x \in L} q^{\langle x, x \rangle / 2} = \sum_{x \in L} q^{\langle \sigma(x), \sigma(x) \rangle / 2} = \sum_{y \in L^\#} q^{\ell \langle y, y \rangle / 2} = \sum_{y \in L^\#} q_\ell^{\langle \ell y, \ell y \rangle / 2} = \sum_{y \in \ell L^\#} q_\ell^{\langle y, y \rangle / 2}.$$

Pela Equação (2.10) e pelo Lema 2.3.10, segue, para todo $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell)$ e todo $z \in \mathbb{H}$, que

$$\Theta_L|_{n/2}\lambda(z) = \chi(d)\Theta_L(z).$$

Portanto, temos Θ_L uma forma modular de peso $n/2$ para $\Gamma_0(\ell)$ com caracter $\chi(\lambda) = \chi(d) = \left(\frac{\Delta}{d}\right)$ para $\Delta = (-1)^{n/2} \det(L)$. ■

Conclusão

Neste capítulo apresentamos a noção de theta série de um reticulado par. Vimos algumas de suas propriedades e a identidade que relaciona a theta série de um reticulado com a theta série de seu reticulado dual. Com isso, estudamos a relação entre as theta séries de reticulados unimodulares pares com formas modulares para o grupo modular completo e, mais geralmente, o resultado que abrange esta relação para reticulados modulares, afirmando que as theta séries de reticulados modulares são formas modulares para um subgrupo de congruência do grupo modular completo.

Capítulo 3

Reticulados ideais

O presente capítulo é dedicado à apresentação de reticulados obtidos via técnicas algébricas, mais detalhadamente, através de ideais fracionários em corpos de números, os quais chamamos de reticulados ideais. Tais estruturas, cujos invariantes derivam da teoria dos números algébricos, fornecem algumas vantagens quando deseja-se obter construções com parâmetros específicos. A formalização dessas estruturas se deve, em grande parte, aos trabalhos [1] e [3] e tem sido usados sistematicamente em aplicações nos trabalhos [4] e [5]. Com isso, abordamos a formalização dos reticulados ideais bem como suas propriedades básicas. Seguindo, consideramos o estudo de modularidade em reticulados ideais via corpos ciclotômicos. Para isto, faremos uso de alguns tópicos em teoria dos números algébricos, cujo conteúdo encontra-se para consulta no Apêndice A ao final do texto.

3.1 Caracterização

Consideremos K um corpo de números com grau $n = [K : \mathbb{Q}]$ e F seu subcorpo maximal real, ou seja,

$$F = K \cap \mathbb{R} = \{x \in K ; \bar{x} = x\} ,$$

onde $\bar{\cdot}$ denota a conjugação complexa. Assim, $[K : F] \leq 2$. A seguir veremos que um reticulado ideal é um ideal fracionário munido de uma forma bilinear satisfazendo

uma propriedade de invariância.

Definição 3.1.1. Um *reticulado ideal* é um par $(\mathfrak{a}, b)$, onde $\mathfrak{a}$ é um ideal fracionário de K e $b : \mathfrak{a} \times \mathfrak{a} \rightarrow \mathbb{Q}$ é uma forma $\mathbb{Z}$ -bilinear simétrica, positiva e não-degenerada satisfazendo a relação

$$b(\eta x, y) = b(x, \bar{\eta} y) , \quad (3.1)$$

para todo $\eta \in \mathcal{O}_K$ e para quaisquer $x, y \in \mathfrak{a}$.

Aqui observamos que, apesar de não explicitarmos o espaço euclidiano de ambiente do reticulado em questão, é sempre possível fazer a imersão de tal reticulado no espaço euclidiano $(K_{\mathbb{R}}, \tilde{b})$ por $(x \mapsto x \otimes 1)$, onde $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ e $\tilde{b}$ estende b por $\tilde{b}(x_1 \otimes r_1, x_2 \otimes r_2) = b(x_1, x_2)r_1r_2$.

Exemplo 3.1.2. Consideremos $p > 2$ um primo e $K = \mathbb{Q}(\zeta_p)$ o p -ésimo corpo ciclotômico. Tomando, conforme o Teorema A.6.1, $\mathfrak{p} = (1 - \zeta_p)$ o único ideal primo de $\mathcal{O}_K$ acima de p e, para $t \geq 1$ inteiro, a forma bilinear

$$\begin{aligned} b : \mathfrak{p}^t \times \mathfrak{p}^t &\longrightarrow \mathbb{Q} \\ (x, y) &\longmapsto \text{Tr}_{K|\mathbb{Q}}\left(\frac{1}{p}x\bar{y}\right) , \end{aligned}$$

obtem-se os reticulados de Craig $A_p^{(t)} = (\mathfrak{p}^t, b)$, que são reticulados ideais já que:

- b é não-degenerada, pois pela Proposição A.2.2, a forma bilinear $(x, y) \mapsto \text{Tr}_{K|\mathbb{Q}}(x\bar{y})$ é não-degenerada e, com isso, $b(x, y) = \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(x\bar{y})$ também é não-degenerada.
- b é simétrica, já que para quaisquer $x, y \in K$, tem-se que

$$b(x, y) = \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(x\bar{y}) = \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(\overline{\bar{x}y}) = \frac{1}{p}\overline{\text{Tr}_{K|\mathbb{Q}}(\bar{x}y)} = \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(\bar{x}y) = b(y, x) .$$

- b é positiva, uma vez que para $x \neq 0$, tem-se que

$$\begin{aligned} b(x, x) &= \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(x\bar{x}) = \frac{1}{p} \sum_{i=1}^n \sigma_i(x\bar{x}) \\ &= \frac{1}{p} \sum_{i=1}^n \sigma_i(x)\overline{\sigma_i(x)} = \frac{1}{p} \sum_{i=1}^n \underbrace{|\sigma_i(x)|^2}_{\geq 0} > 0 . \end{aligned}$$

- para todo $\eta \in \mathcal{O}_K$ e quaisquer $x, y \in K$, tem-se que b satisfaz

$$b(\eta x, y) = \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(\eta x\bar{y}) = \frac{1}{p}\text{Tr}_{K|\mathbb{Q}}(x\overline{\eta y}) = b(x, \bar{\eta} y) .$$

Definição 3.1.3. Um elemento $\alpha \in K$ é dito ser *totalmente positivo* se $\sigma_i(\alpha) > 0$ para todo $\sigma_i : K \longrightarrow \mathbb{C}$ monomorfismos de K .

O próximo resultado mostra a relação entre reticulados ideais com a forma traço. Mas antes é necessário notarmos que, para todo ideal fracionário $\mathfrak{a}$ de K , tem-se que $K = \mathfrak{a}\mathbb{Q}$ e, com isso, K pode ser escrito como

$$K = \left\{ \frac{x}{\gamma} ; x \in \mathfrak{a} \text{ e } \gamma \in \mathbb{Z} \setminus \{0\} \right\} . \quad (3.2)$$

Proposição 3.1.4. Se $\mathfrak{a}$ é um ideal fracionário de $\mathcal{O}_K$ e $b : \mathfrak{a} \times \mathfrak{a} \longrightarrow \mathbb{Q}$ é uma forma $\mathbb{Z}$ -bilinear simétrica, positiva e não-degenerada, então, $(\mathfrak{a}, b)$ é um reticulado ideal se, e somente se, existe $\alpha \in F^\times$ totalmente positivo tal que

$$b(x, y) = \text{Tr}_{K|\mathbb{Q}}(\alpha x \bar{y}) . \quad (3.3)$$

Demonstração: Se $(\mathfrak{a}, b)$ é um reticulado ideal, da relação (3.2), podemos estender a forma bilinear b de $\mathfrak{a}$ para K da seguinte forma

$$b\left(\frac{x}{\gamma}, \frac{x'}{\gamma'}\right) = \frac{b(x, x')}{\gamma\gamma'} ,$$

obtendo-se uma forma bilinear de K em $\mathbb{Q}$. Além disso, a extensão de b satisfaz

$$b(\eta x, y) = b(x, \bar{\eta} y) ,$$

para qualquer $\eta \in K$, pois para $\frac{x'}{\gamma'} \in K$, tem-se que

$$b\left(\frac{x'}{\gamma'} x, y\right) = \frac{1}{\gamma'} b(x' x, y) = \frac{1}{\gamma'} b(x, \bar{x}' y) = b\left(x, \frac{\bar{x}'}{\gamma'} y\right) = b\left(x, \overline{\left(\frac{x'}{\gamma'}\right)} y\right) .$$

Agora, sendo a forma bilinear $(x, y) \mapsto \text{Tr}_{K|\mathbb{Q}}(xy)$ de K em $\mathbb{Q}$ não-degenerada, segue do isomorfismo dado em (1.2) que, para $x, y \in K$, existe $h \in \text{End}_{\mathbb{Q}} K$ tal que

$$b(x, y) = \text{Tr}_{K|\mathbb{Q}}(xh(y)) .$$

Como $b(\eta x, y) = b(x, \bar{\eta} y)$, para todo $\eta \in K$, segue que

$$\text{Tr}_{K|\mathbb{Q}}(\eta x h(y)) = \text{Tr}_{K|\mathbb{Q}}(x h(\bar{\eta} y)), \text{ para todo } \eta \in K,$$

e, portanto, $h(\bar{\eta} y) = \eta h(y)$, para quaisquer $y, \eta \in K$. Seja $\alpha = h(1)$. Assim,

$$h(y) = \bar{y} h(1) = \alpha \bar{y} .$$

Ainda, como

$$b(x, y) = \text{Tr}_{K|\mathbb{Q}}(\alpha x \bar{y}) = \text{Tr}_{K|\mathbb{Q}}(\overline{\alpha x y}) = \underbrace{\overline{\text{Tr}_{K|\mathbb{Q}}(\alpha x y)}}_{\in \mathbb{Q}} = \text{Tr}_{K|\mathbb{Q}}(\overline{\alpha x y})$$

e

$$b(x, y) = b(y, x) = \text{Tr}_{K|\mathbb{Q}}(\alpha \bar{x} y) ,$$

segue que $\text{Tr}_{K|\mathbb{Q}}(\alpha \bar{x} y) = \text{Tr}_{K|\mathbb{Q}}(\overline{\alpha x y})$, para todo $y \in K$. Assim, $\bar{\alpha} = \alpha$ com $\alpha \neq 0$, visto que b é uma forma bilinear não-degenerada. Reciprocamente, se $b : \mathfrak{a} \times \mathfrak{a} \rightarrow \mathbb{Q}$ satisfaz a condição (3.3), então b satisfaz as condições da Definição 3.1.1 e, assim, $(\mathfrak{a}, b)$ é um reticulado ideal. ■

Em virtude da existência do elemento $\alpha \in F^\times$ assegurada na Proposição 3.1.4, passamos a denotar o reticulado ideal $(\mathfrak{a}, b)$ satisfazendo a condição (3.3) por $(\mathfrak{a}, \alpha)$.

Agora, para prosseguirmos com o estudo de dualidade para reticulados ideais, se faz necessário a seguinte ressalva: vale a seguinte igualdade de conjuntos

$$\{x \otimes 1 \in K_{\mathbb{R}} ; b(x, \mathfrak{a}) \subset \mathbb{Z}\} = \{x \otimes r \in K_{\mathbb{R}} ; \tilde{b}(x \otimes r, a \otimes 1) \in \mathbb{Z} , \forall a \in \mathfrak{a}\} .$$

De fato, se $x \in K$ com $b(x, a) \in \mathbb{Z}$, para todo $a \in \mathfrak{a}$, então $\tilde{b}(x \otimes 1, a \otimes 1) = b(x, a) \in \mathbb{Z}$, para todo $a \in \mathfrak{a}$. Por outro lado, se $x \otimes r \in K_{\mathbb{R}}$ com $\tilde{b}(x \otimes r, a \otimes 1) = b(x, a)r \in \mathbb{Z}$, para todo $a \in \mathfrak{a}$, então, como $b(x, a) \in \mathbb{Q}$, segue que $r \in \mathbb{Q}$ e, assim, $x \otimes r = (rx) \otimes 1$ satisfaz $b(rx, a) = b(x, a)r \in \mathbb{Z}$ para todo $a \in \mathfrak{a}$. Portanto, em posse desta igualdade, concluímos que o reticulado dual de um reticulado ideal $(\mathfrak{a}, b)$ é o conjunto

$$\mathfrak{a}^\# = \{x \in K ; b(x, \mathfrak{a}) \subset \mathbb{Z}\} .$$

Com isso, a próxima proposição explicita o reticulado dual de um reticulado ideal.

Proposição 3.1.5. *O reticulado dual de $(\mathfrak{a}, \alpha)$ é o reticulado ideal $(\mathfrak{a}^\#, \alpha)$, onde*

$$\mathfrak{a}^\# = \alpha^{-1} \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{a}}^{-1} .$$

Demonstração: Como

$$\text{Tr}_{K|\mathbb{Q}}(\alpha \alpha^{-1} \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{a}}^{-1} \bar{\mathfrak{a}}) = \text{Tr}_{K|\mathbb{Q}}(\mathcal{D}_{K|\mathbb{Q}}^{-1} \mathcal{O}_K) \subset \mathbb{Z},$$

segue que $\alpha^{-1} \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{a}}^{-1} \subset \mathfrak{a}^\#$. Por outro lado, como $\bar{\mathfrak{a}} \mathcal{O}_K = \bar{\mathfrak{a}}$, segue que

$$\text{Tr}_{K|\mathbb{Q}}(\alpha \mathfrak{a}^\# \bar{\mathfrak{a}} \mathcal{O}_K) = \text{Tr}_{K|\mathbb{Q}}(\alpha \mathfrak{a}^\# \bar{\mathfrak{a}}) \subset \mathbb{Z},$$

implicando que $\alpha \mathfrak{a}^\# \bar{\mathfrak{a}} \subset \mathcal{D}_{K|\mathbb{Q}}^{-1}$ e, deste modo, $\mathfrak{a}^\# \subset \alpha^{-1} \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{a}}^{-1}$. ■

Como consequência, tem-se uma condição necessária e suficiente para avaliar a integralidade em reticulados ideais:

Corolário 3.1.6. *Um reticulado ideal $(\mathfrak{a}, \alpha)$ é integral se, e somente se,*

$$\alpha \mathfrak{a} \bar{\mathfrak{a}} \subset \mathcal{D}_{K|\mathbb{Q}}^{-1} .$$

Demonstração: Pela Proposição 1.4.8, tem-se que $(\mathfrak{a}, \alpha)$ integral se, e somente se, $\mathfrak{a} \subset \mathfrak{a}^\# = \alpha^{-1} \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{a}}^{-1}$. ■

Note que essa explanação sobre reticulados ideais não tem nenhuma diferença com a observação dada após o Teorema 1.2.3, uma vez que o ideal fracionário $\mathfrak{a}$ de K , que é um $\mathbb{Z}$ -módulo livre de posto finito n , é visto como um reticulado imerso no espaço euclidiano $(\mathfrak{a}_{\mathbb{R}}, \tilde{b})$, onde $\mathfrak{a}_{\mathbb{R}} = \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{R}$ e $\tilde{b}(x_1 \otimes r_1, x_2 \otimes r_2) = b(x_1, x_2) r_1 r_2$. No entanto, tem-se que $K_{\mathbb{R}} \subseteq \mathfrak{a}_{\mathbb{R}}$, uma vez que $x \otimes r = a \otimes \frac{r}{\gamma} \in \mathfrak{a}_{\mathbb{R}}$, desde que, da forma de K dada em (3.2), podemos escrever $x = \frac{a}{\gamma}$, com $a \in \mathfrak{a}$ e $\gamma \in \mathbb{Z} \setminus \{0\}$.

Um outro invariante, dado explicitamente por ferramentas algébricas, é o determinante do reticulado ideal como podemos verificar no resultado a seguir:

Proposição 3.1.7. *Se $(\mathfrak{a}, \alpha)$ é um reticulado ideal, então*

$$\det(\mathfrak{a}) = N_{K|\mathbb{Q}}(\alpha) N(\mathfrak{a})^2 |d_K| . \quad (3.4)$$

Demonstração: Note inicialmente que se $\mathfrak{b}$ é um ideal inteiro, então o reticulado ideal $(\mathfrak{b}, \alpha)$ é integral, uma vez que $\mathfrak{b} \subset \mathcal{O}_K \subset \mathcal{D}_{K|\mathbb{Q}}^{-1}$ e daí $\mathfrak{b} \bar{\mathfrak{b}} \subset \bar{\mathfrak{b}} \subset \overline{\mathcal{O}_K} \subset \mathcal{O}_K \subset \mathcal{D}_{K|\mathbb{Q}}^{-1}$. Além disso, tem-se que $\alpha \mathfrak{b} \bar{\mathfrak{b}} \subset \mathfrak{b} \bar{\mathfrak{b}}$ pois $\mathfrak{b} \bar{\mathfrak{b}} \mid \alpha \mathfrak{b} \bar{\mathfrak{b}}$ (note que $\alpha \mathfrak{b} \bar{\mathfrak{b}} = (\alpha \mathcal{O}_K) \mathfrak{b} \bar{\mathfrak{b}}$). Agora, tomando o ideal fracionário $\mathfrak{a}$, segue que existe $c \in \mathbb{Z}$ não nulo tal que $c\mathfrak{a} \subset \mathcal{O}_K$ e

com isso, $(c\mathfrak{a}, \alpha)$ é integral. Assim,

$$\begin{aligned}
\det(c\mathfrak{a}) &\stackrel{(1.4.11)}{=} ((c\mathfrak{a})^\# : c\mathfrak{a}) \\
&\stackrel{(1.4.10)}{=} \chi((c\mathfrak{a})^\#, \mathcal{O}_K) \chi(\mathcal{O}_K, c\mathfrak{a}) \\
&\stackrel{(1.4.10)}{=} \chi(\mathcal{O}_K, (c\mathfrak{a})^\#)^{-1} \chi(\mathcal{O}_K, c\mathfrak{a}) \\
&= N((c\mathfrak{a})^\#)^{-1} N(c\mathfrak{a}) \\
&\stackrel{(1.4.5)}{=} N(c^{-1}\mathfrak{a}^\#)^{-1} N(c\mathfrak{a}) \\
&\stackrel{(A.5.1)}{=} N_{K|\mathbb{Q}}(c^{-1})^{-1} N(\mathfrak{a}^\#)^{-1} N_{K|\mathbb{Q}}(c) N(\mathfrak{a}) \\
&= N_{K|\mathbb{Q}}(c)^2 N(\mathfrak{a}\mathfrak{a}^{\#-1}) \\
&= N_{K|\mathbb{Q}}(c)^2 N(\alpha\mathfrak{a}\bar{\alpha}\mathcal{D}_{K|\mathbb{Q}}) \\
&= c^{2n} N_{K|\mathbb{Q}}(\alpha) N(\mathfrak{a}) N(\bar{\alpha}) N(\mathcal{D}_{K|\mathbb{Q}}) \\
&= c^{2n} N_{K|\mathbb{Q}}(\alpha) N(\mathfrak{a})^2 |d_K| .
\end{aligned}$$

Agora, se $\{x_1, x_2, \dots, x_n\}$ é uma $\mathbb{Z}$ -base de $\mathfrak{a}$, então

$$\det(c\mathfrak{a}) = \det(b(cx_i, cx_j)) = \det(c^2 b(x_i, x_j)) = c^{2n} \det(\mathfrak{a}) ,$$

o que conclui a demonstração. ■

Exemplo 3.1.8. De acordo com a Proposição 3.1.7, o determinante dos reticulados de Craig é dado por

$$\det(A_p^{(t)}) = N_{K|\mathbb{Q}}(1/p) N(\mathfrak{P})^{2t} |d_K| = (1/p)^{p-1} p^{2t} p^{p-2} = p^{2t-1}.$$

O próximo corolário fornece a densidade de centro do empacotamento esférico por um reticulado ideal.

Corolário 3.1.9. *Se $(\mathfrak{a}, \alpha)$ é um reticulado ideal, então sua densidade de centro é dada por*

$$\delta(\mathfrak{a}) = \frac{t_{\mathfrak{a}}^{n/2}}{2^n N(\mathfrak{a}) (N_{K|\mathbb{Q}}(\alpha) |d_K|)^{1/2}} ,$$

onde $t_{\mathfrak{a}} = \min\{ \text{Tr}_{K|\mathbb{Q}}(\alpha x \bar{x}) ; x \in \mathfrak{a}, x \neq 0 \}$.

Demonstração: Segue imediatamente do Teorema 1.5.12. ■

O próximo resultado fornece uma condição na extensão $K | F$ quando $[K : F] = 2$, suficiente para que os reticulados ideais integrais em K sejam pares.

Proposição 3.1.10. *Seja $(\mathfrak{a}, \alpha)$ um reticulado ideal integral. Se 2 não ramifica em $K | F$, onde $[K : F] = 2$, então o reticulado ideal $(\mathfrak{a}, \alpha)$ é par.*

Demonstração: Como $[K : F] = 2$ e 2 não ramifica em $K \mid F$, segue da Proposição A.3.7 que a extensão $K \mid F$ é moderadamente ramificada e, com isso, da Proposição A.3.8, tem-se $\text{Tr}_{K|F}(\mathcal{O}_K) = \mathcal{O}_F$. Assim, existe $y \in \mathcal{O}_K$ tal que $\text{Tr}_{K|F}(y) = y + \bar{y} = 1$. Deste modo, tem-se que

$$\begin{aligned} \text{Tr}_{K|\mathbb{Q}}(\alpha x \bar{x}) &= \text{Tr}_{K|\mathbb{Q}}(\alpha(y + \bar{y})x \bar{x}) \\ &= \text{Tr}_{K|\mathbb{Q}}(\alpha y x \bar{x}) + \text{Tr}_{K|\mathbb{Q}}(\alpha \bar{y} x \bar{x}) \\ &= \text{Tr}_{K|\mathbb{Q}}(\alpha y x \bar{x}) + \text{Tr}_{K|\mathbb{Q}}(\overline{\alpha y x \bar{x}}) \\ &= \text{Tr}_{K|\mathbb{Q}}(\alpha y x \bar{x}) + \overline{\text{Tr}_{K|\mathbb{Q}}(\alpha y x \bar{x})} \\ &= 2\text{Tr}_{K|\mathbb{Q}}(\alpha y x \bar{x}) \in 2\mathbb{Z} , \end{aligned}$$

pois, sendo $(\mathfrak{a}, \alpha)$ integral, segue que $\alpha \mathfrak{a} \bar{\mathfrak{a}} \subset \mathcal{D}_{K|\mathbb{Q}}^{-1}$ e, deste modo,

$$\text{Tr}_{K|\mathbb{Q}}(\alpha y x \bar{x}) \in \mathbb{Z},$$

o que prova a proposição. ■

Dizemos que um reticulado ideal $(\mathfrak{a}, \alpha)$ é *do tipo traço* se $\alpha = 1$. A seguir, veremos a existência desses reticulados com determinante pré-definidos.

Proposição 3.1.11. *Seja d um inteiro positivo. Existe um $(\mathfrak{a}, 1)$ reticulado ideal integral com $\det(\mathfrak{a}) = d$ em K se, e somente se, existem $\mathfrak{Q}$ e $\mathfrak{J}$ ideais fracionários de K tais que $N(\mathfrak{Q}) = d$ e $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{Q}\mathfrak{J}\bar{\mathfrak{J}}$.*

Demonstração: Se existe um $(\mathfrak{a}, 1)$ reticulado ideal integral do tipo traço em K com $\det(\mathfrak{a}) = d$, então $\mathfrak{a} \subset \mathfrak{a}^\# = \bar{\mathfrak{a}}^{-1}\mathcal{D}_{K|\mathbb{Q}}^{-1}$ e, com isso, $\mathcal{D}_{K|\mathbb{Q}} \subset \mathfrak{a}^{-1}\bar{\mathfrak{a}}^{-1}$, ou seja, $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{a}^{-1}\bar{\mathfrak{a}}^{-1}\mathfrak{Q}$, para algum ideal fracionário $\mathfrak{Q}$. Portanto, tomando $\mathfrak{J} = \mathfrak{a}^{-1}$ e notando que

$$d = \det(\mathfrak{a}) = N(\mathfrak{a})^2 |d_K| = N(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K|\mathbb{Q}}) = N(\mathfrak{J}^{-1}\bar{\mathfrak{J}}^{-1}\mathfrak{Q}\mathfrak{J}\bar{\mathfrak{J}}) = N(\mathfrak{Q}) ,$$

segue resultado. Reciprocamente, considerando o reticulado ideal $(\mathfrak{a}, 1)$ onde $\mathfrak{a} = \mathfrak{J}^{-1}$, tem-se que

$$\mathfrak{a} = \mathfrak{J}^{-1} \subset \bar{\mathfrak{J}}\mathcal{D}_{K|\mathbb{Q}}^{-1} = \bar{\mathfrak{a}}^{-1}\mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{a}^\# ,$$

uma vez que $\mathcal{D}_{K|\mathbb{Q}} \subset \mathfrak{J}\bar{\mathfrak{J}}$. Portanto, $(\mathfrak{a}, 1)$ é integral. Além disso, tem-se que

$$\det(\mathfrak{a}) = N(\mathfrak{a})^2 |d_K| = N(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K|\mathbb{Q}}) = N(\mathfrak{J}^{-1}\bar{\mathfrak{J}}^{-1}\mathfrak{Q}\mathfrak{J}\bar{\mathfrak{J}}) = N(\mathfrak{Q}) = d ,$$

o que prova o resultado. ■

Corolário 3.1.12. *Existe um reticulado ideal do tipo traço e unimodular em K se, e somente se, existe $\mathfrak{J}$ ideal fracionário de K tal que $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{J}\bar{\mathfrak{J}}$.*

Demonstração: Segue imediatamente da Proposição 3.1.11. ■

No que segue, introduzimos um conceito de equivalência para reticulados ideais. Essa noção nos permitirá analisar uma classe especial de reticulados ideais modulares através de condições de existência.

Definição 3.1.13. Dizemos que dois reticulados ideais $(\mathfrak{a}, \alpha)$ e $(\mathfrak{a}', \alpha')$ em K são *Arakelov-equivalentes*, se existe $\beta \in K^\times$ tal que $\mathfrak{a}' = \beta\mathfrak{a}$ e $\alpha' = (\beta\bar{\beta})^{-1}\alpha$.

Exemplo 3.1.14. Considere $K = \mathbb{Q}(\zeta_{p^r})$, com p um número primo tal que $p \not\equiv 1 \pmod{4}$ e $r \geq 1$. Seja $\mathfrak{p}$ o único ideal de $\mathcal{O}_K$ acima de p , então os reticulados ideais $(\mathfrak{p}^s, 1)$ e $(\mathfrak{p}^{-(a+s)}, p)$, onde $a = p^{r-1}(pr - r - 1)$ e $s = \frac{\phi(p^r) - 2a}{4}$, são Arakelov-equivalentes, pois existe $\beta = \frac{1}{\sqrt{-p}} \in K^\times$, tal que $\mathfrak{p}^{-(a+s)} = \frac{1}{\sqrt{-p}}\mathfrak{p}^s$, uma vez que sendo $\phi(p^r)/2 = s + 2a$ e $\sqrt{-p}\mathcal{O}_K = \mathfrak{p}^{\frac{\phi(p^r)}{2}}$, tem-se

$$\sqrt{-p} \mathfrak{p}^{-(a+s)} = \mathfrak{p}^s ,$$

com $p = (\beta\bar{\beta})^{-1}$.

Definição 3.1.15. Um reticulado ideal $(\mathfrak{a}, \alpha)$ sobre K é dito ser *Arakelov-modular de grau $\ell \in \mathbb{Z}$* se $(\mathfrak{a}, \alpha)$ e $(\mathfrak{a}^\#, \ell\alpha)$ são Arakelov-equivalentes. Chamamos um reticulado ideal $(\mathfrak{a}, \alpha)$ de *Arakelov-modular*, se existe $\ell \in \mathbb{Z}$ tal que $(\mathfrak{a}, \alpha)$ seja Arakelov-modular de grau ℓ .

Notemos que reticulados Arakelov-modulares são reticulados modulares, onde a similaridade é dada por $(x \mapsto \beta x)$, para $\beta \in K^\times$ garantido na definição. Com isso, tem-se o seguinte resultado para a existência de reticulados Arakelov-modulares.

Proposição 3.1.16. *Seja ℓ um inteiro positivo. Existe um reticulado ideal $(\mathfrak{a}, \alpha)$ Arakelov-modular de grau ℓ em K se, e somente se, existe $\lambda \in K^\times$ com $\ell = \lambda\bar{\lambda}$ tal que*

$$\lambda\mathcal{O}_K = \alpha\mathfrak{a}\bar{\alpha}\mathcal{D}_{K|\mathbb{Q}} .$$

Demonstração: Se $(\mathfrak{a}, \alpha)$ é um reticulado ideal Arakelov-modular de grau ℓ em K , então, por definição, existe $\beta \in K^\times$ tal que $\mathfrak{a} = \beta\mathfrak{a}^\#$ e $\alpha = \ell\alpha(\beta\bar{\beta})^{-1}$. Tomando $\lambda = \beta$, como $\mathfrak{a}^\# = \alpha^{-1}\mathcal{D}_{K|\mathbb{Q}}^{-1}\bar{\alpha}^{-1}$, segue que

$$\mathfrak{a} = \lambda\mathfrak{a}^\# = \lambda\alpha^{-1}\mathcal{D}_{K|\mathbb{Q}}^{-1}\bar{\alpha}^{-1} \implies \lambda\mathcal{O}_K = \alpha\mathfrak{a}\bar{\alpha}\mathcal{D}_{K|\mathbb{Q}} .$$

Reciprocamente, considerando as existências do ideal fracionário $\mathfrak{a}$ e do elemento λ de K nas condições do enunciado, tem-se que $\lambda\mathcal{O}_K = (\mathfrak{a}^\#)^{-1}\mathfrak{a}$ e, desse modo,

$\mathfrak{a} = \lambda \mathfrak{a}^\#$ com $\ell = \lambda \bar{\lambda}$. Finalmente, mostremos que $(\mathfrak{a}, \alpha)$ é integral. Para isto, seja $\mathfrak{P}$ um ideal primo de $\mathcal{O}_K$. Como $\lambda \mathcal{O}_K = \alpha \mathfrak{a} \bar{\mathfrak{a}} \mathcal{D}_{K|\mathbb{Q}} = \bar{\lambda} \mathcal{O}_K$, uma vez que $\mathcal{D}_{K|\mathbb{Q}} \subset \mathcal{O}_K$ e $\overline{\mathcal{O}_K} = \mathcal{O}_K$, segue que $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(\bar{\lambda})$ e, portanto,

$$\nu_{\mathfrak{P}}(\ell) = \nu_{\mathfrak{P}}(\lambda \bar{\lambda}) = \nu_{\mathfrak{P}}(\lambda) + \nu_{\mathfrak{P}}(\bar{\lambda}) = 2\nu_{\mathfrak{P}}(\lambda) .$$

Agora, como $\ell \in \mathbb{Z} \subset \mathcal{O}_K$, segue que $\ell \mathcal{O}_K$ é um ideal de $\mathcal{O}_K$ e, com isso, $\nu_{\mathfrak{P}}(\ell) \geq 0$ uma vez que $\mathcal{O}_K \subset \mathcal{O}_{\mathfrak{P}} = \{x \in K ; \nu_{\mathfrak{P}}(x) \geq 0\}$. Assim, $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(\ell)/2 \geq 0$ para todo ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$ e, portanto, $\lambda \mathcal{O}_K \subset \mathcal{O}_K$. Assim, $\lambda \in \lambda \mathcal{O}_K \subset \mathcal{O}_K$. Deste modo, $\mathfrak{a} = \lambda \mathfrak{a}^\# \subseteq \mathfrak{a}^\#$ já que $\mathfrak{a}^\#$ é um ideal fracionário de K (um $\mathcal{O}_K$ -módulo). ■

Exemplo 3.1.17. Note que nas condições do Exemplo 3.1.14, sendo $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}^a$ e considerando $\mathfrak{a} = \mathfrak{p}^s$, como $\mathfrak{a} = \bar{\mathfrak{a}}$, podemos escrever

$$\sqrt{-p} \mathcal{O}_K = \mathfrak{a} \bar{\mathfrak{a}} \mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{p}^s \mathfrak{p}^s \mathfrak{p}^a = \mathfrak{p}^{a+2s} = \mathfrak{p}^{\phi(p^r)/2} .$$

Portanto, pelo Teorema 3.1.16, segue que existe um reticulado Arakelov-modular de grau $\ell = \sqrt{-p} \sqrt{-p} = p$ em $K = \mathbb{Q}(\zeta_{p^r})$. De fato, o reticulado dual de $(\mathfrak{p}^s, 1)$ é $(\mathfrak{p}^s)^\# = \mathfrak{p}^{-(a+s)}$. Assim, como $(\mathfrak{p}^s, 1)$ e $(\mathfrak{p}^{-(a+s)}, p)$ são ideais Arakelov-equivalentes com $p = \sqrt{-p} \cdot \sqrt{-p}$, segue que o reticulado ideal $(\mathfrak{p}^s, 1)$ é Arakelov-modular de grau p .

O seguinte resultado nos diz que podemos considerar apenas reticulados ideais Arakelov-modulares de graus livres de quadrados.

Proposição 3.1.18. *Seja ℓ um inteiro positivo. Se existe um reticulado ideal $(\mathfrak{a}, \alpha)$ Arakelov-modular de grau ℓ com $\ell = \ell_1 \ell_2^2$ para ℓ_1 livre de quadrados, então o reticulado ideal reescalado $(\mathfrak{a}, \ell_2^{-1} \alpha)$ é Arakelov-modular de grau ℓ_1 .*

Demonstração: Seja $\lambda \in K^\times$ tal que $\ell = \lambda \bar{\lambda}$ e $\mathfrak{a} = \lambda \mathfrak{a}^\#$. Considerando $\lambda_1 = \lambda/\ell_2$, tem-se que $\lambda_1 \bar{\lambda}_1 = \ell_1$ e $\lambda_1 \mathcal{O}_K = \ell_2^{-1} \alpha \mathfrak{a} \bar{\mathfrak{a}} \mathcal{D}_{K|\mathbb{Q}}$. Assim, pela Proposição 3.1.16, segue que $(\mathfrak{a}, \ell_2^{-1} \alpha)$ é um reticulado ideal Arakelov-modular de grau ℓ_1 . ■

3.2 Modularidade em corpos ciclotômicos

Nesta seção, tratamos de obter condições para a existência de reticulados ideais Arakelov-modulares do tipo traço em corpos ciclotômicos e também da caracterização de reticulados ideais do tipo traço que são Arakelov-modulares para graus primos em corpos ciclotômicos. Para isto, consideremos m um inteiro positivo

ímpar ou divisível por 4, $K = \mathbb{Q}(\zeta_m)$ o m -ésimo corpo ciclotômico e $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ seu subcorpo real maximal. Precisamos da noção de norma dada pela seguinte definição.

Definição 3.2.1. Sejam p um primo e m um natural tal que $p \nmid m$. Dizemos que p é uma *norma de m* se $\mathfrak{P} \neq \bar{\mathfrak{P}}$, para todo ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$ acima de p , para $K = \mathbb{Q}(\zeta_m)$.

Outro conceito necessário é o de bom divisor.

Definição 3.2.2. Sejam p primo com $p \mid m$. Dizemos que p é um *bom divisor de m* se o diferente $\mathcal{D}_{K|\mathbb{Q}}$ da extensão $K|\mathbb{Q}$, para $K = \mathbb{Q}(\zeta_m)$, pode ser escrito como $\mathfrak{Q}\mathfrak{I}\bar{\mathfrak{I}}$, onde $\mathfrak{I}$ é um ideal de $\mathcal{O}_K$ sobre p e $\mathfrak{Q}$ um ideal relativamente primo a p . Um inteiro m' é dito ser *bom divisor de m* se seus divisores primos são bons divisores de m .

Exemplo 3.2.3. Note que 2 é um bom divisor para todo m , pois como $4 \mid m$, segue que $m = 2^r m'$ para $r \geq 2$ e m' ímpar. Assim, seja $\mathfrak{p}$ o único ideal de $\mathbb{Q}(\zeta_{2^r})$ acima de 2. Como $\mathcal{D}_{\mathbb{Q}(\zeta_{2^r})|\mathbb{Q}} = \mathfrak{p}^a$ com $\mathfrak{p} = \bar{\mathfrak{p}}$, onde $a = 2^{r-1}(r-1)$, segue que

$$\mathcal{D}_{\mathbb{Q}(\zeta_{2^r})|\mathbb{Q}} = \mathfrak{p}^{2^{r-2}(r-1)} \bar{\mathfrak{p}}^{2^{r-2}(r-1)}.$$

Portanto, como $\mathcal{D}_{K|\mathbb{Q}} = \mathcal{D}_{K|\mathbb{Q}(\zeta_{2^r})}(\mathcal{D}_{\mathbb{Q}(\zeta_{2^r})|\mathbb{Q}}\mathcal{O}_K)$, segue que 2 é um bom divisor de m .

Note que tomando um ideal fracionário $\mathfrak{a}$ de K satisfazendo $\lambda\mathcal{O}_K = \alpha\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K|\mathbb{Q}}$, sendo $\alpha \in F$, tem-se que $\lambda\mathcal{O}_K = \bar{\lambda}\mathcal{O}_K$ ou, equivalentemente, $(\lambda/\bar{\lambda})\mathcal{O}_K = \mathcal{O}_K$ e, portanto, $\lambda/\bar{\lambda}$ é uma unidade de $\mathcal{O}_K$. Se ℓ é um inteiro positivo que satisfaz $\ell = \lambda\bar{\lambda}$, então podemos escrever $\lambda^2 = u\ell$, onde u é uma unidade de $\mathcal{O}_K$. Consideremos, portanto, que ocorra a seguinte situação: ℓ é um inteiro positivo livre de quadrados tal que todos os seus divisores primos ramifiquem em K e $\lambda \in K^\times$ com $\lambda^2 = u\ell$ para $u \in \{\pm 1, \pm i\}$ satisfazendo $\ell = \ell_1\ell_2$, onde ℓ_1 é o produto dos divisores primos p de ℓ tais que $p \equiv 1 \pmod{4}$ caso m seja ímpar ou m divisível por 8, e ℓ_2 é o produto dos divisores primos p de ℓ tais que $p \equiv 3 \pmod{4}$ caso $m \equiv 4 \pmod{8}$. Com isso tem-se o seguinte:

Lema 3.2.4. *Seja p um divisor primo de m . Se todo ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$ acima de p satisfaz $\mathfrak{P} \neq \bar{\mathfrak{P}}$, então p é um bom divisor de m .*

Demonstração: Como $p \mid m$, segue que p ramifica em K e, se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}_K$ acima de p que ramifica, do fato que $p\mathcal{O}_K = (\prod \sigma(\mathfrak{P}))^{\phi(p^r)}$, segue que $\bar{\mathfrak{P}}$ também ramifica. Em particular, $\mathfrak{P}$ e $\bar{\mathfrak{P}}$ aparecem na fatoração de $\mathcal{D}_{K|\mathbb{Q}}$ com expoente

$p^{r-1}(pr - r - 1)$. Considerando $\mathfrak{J}\bar{\mathfrak{J}}$ o produto dos ideais primos $\mathfrak{P}$ acima de p em $\mathcal{O}_K$ que ramificam com expoente $p^{r-1}(pr - r - 1)$, tem-se que $\mathfrak{J}\bar{\mathfrak{J}}$ divide $\mathcal{D}_{K|\mathbb{Q}}$ e, com isso, $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{J}_1\mathfrak{J}\bar{\mathfrak{J}}$, onde $\mathfrak{J}_1$ é o produto de ideais primos de $\mathcal{O}_K$ que ramificam para primos diferentes de p . Com isso, $\mathfrak{J}_1$ é primo com p no sentido de que $\mathfrak{J}_1 \cap \mathbb{Z} \neq p\mathbb{Z}$. Portanto, tem-se que $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{J}_1\mathfrak{J}\bar{\mathfrak{J}}$, onde $\mathfrak{J}_1$ é primo com p e $\mathfrak{J}$ está acima de p , ou seja, p é um bom divisor de m . ■

Lema 3.2.5. *Se uma decomposição do tipo $\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{a}\bar{\mathfrak{a}}$ existe para algum ideal fracionário $\mathfrak{a}$ de K e algum $\lambda \in K^\times$, então $\nu_{\mathfrak{P}}(\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1})$ é par para todo $\mathfrak{P}$ ideal primo de $\mathcal{O}_K$ satisfazendo $\mathfrak{P} = \bar{\mathfrak{P}}$.*

Demonstração: Se $\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{a}\bar{\mathfrak{a}}$ com $\nu_{\mathfrak{P}}(\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1})$ ímpar para algum $\mathfrak{P}$ tal que $\mathfrak{P} = \bar{\mathfrak{P}}$, então tem-se que $\nu_{\mathfrak{P}}(\mathfrak{a}) \neq \nu_{\mathfrak{P}}(\bar{\mathfrak{a}})$, pois caso contrário $\nu_{\mathfrak{P}}(\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1})$ seria par. Isto implica que $\mathfrak{P} \neq \bar{\mathfrak{P}}$, o que é uma contradição. ■

Com base nas suposições e lemas anteriores, tem-se o seguinte resultado fornecendo condições para a existência de reticulados ideais do tipo traço e Arakelov-modulares:

Teorema 3.2.6. *Existe um reticulado ideal Arakelov-modular de grau ℓ do tipo traço em K se, e somente se, as seguintes condições são satisfeitas:*

1. $\ell \mid m$;
2. ℓ e m' são bons divisores de m (onde $m = \ell^s m'$ com $\text{mdc}(\ell, m') = 1$);
3. 2 é norma de $m/4$ se ℓ_1 é par.

Demonstração: Suponhamos a existência de um reticulado ideal Arakelov-modular de grau ℓ do tipo traço em K . Pela Proposição 3.1.16, segue que existem $\lambda \in K$ com $\ell = \lambda\bar{\lambda}$ e $\mathfrak{a}$ um ideal fracionário de K satisfazendo $\lambda\mathcal{O}_K = \mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K|\mathbb{Q}}$. Mostremos que $\ell \mid m$. Como os divisores primos de ℓ ramificam em K e ℓ é livre de quadrados, segue que $\ell \mid m$. Agora, mostremos que $\ell_1 m'$ é um bom divisor de m (e, portanto, ℓ_1 e m' o são). Consideremos p um divisor de $\ell_1 m'$ e $\mathfrak{P}$ um ideal primo de $\mathcal{O}_K$ acima de p . Se p divide ℓ_1 , então caso p seja ímpar, tem-se que $p \equiv 1 \pmod{4}$ e daí sendo ℓ livre de quadrados, segue que $\nu_{\mathfrak{P}}(\ell) = \nu_{\mathfrak{P}}(p) = p^{r-1}(p-1) \equiv 0 \pmod{4}$ e, com isso, $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(\ell)/2 \equiv 0 \pmod{2}$, ou seja, $\nu_{\mathfrak{P}}(\lambda)$ é par com $\nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}}) = p^{r-1}(pr - r - 1)$ ímpar. Assim, $\nu_{\mathfrak{P}}(\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1}) = \nu_{\mathfrak{P}}(\lambda) - \nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}})$ é ímpar. Se $p = 2$, então $n \equiv 4 \pmod{8}$, ou seja, $n = 4k'$ com k' ímpar. Novamente, como $\nu_{\mathfrak{P}}(\ell) = \nu_{\mathfrak{P}}(p) = 2$, segue que $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(\ell)/2 = 1$ com $\nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}}) = 2$. Assim, $\nu_{\mathfrak{P}}(\lambda\mathcal{D}_{K|\mathbb{Q}}^{-1})$ é ímpar. Agora, se p divide m' , então podemos considerar p ímpar, já que 2 já é um bom divisor para m . Com isso, como $\text{mdc}(\ell, m') = 1$, segue que $\nu_{\mathfrak{P}}(\lambda) = 0$ com $\nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}}) = p^{r-1}(pr - r - 1)$ ímpar e,

portanto, $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1})$ é ímpar. Deste modo, para todo ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$ dividindo $\ell_1 m' \mathcal{O}_K$, segue que $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1})$ é ímpar. Agora, da hipótese, tem-se que $\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{a}\bar{\mathfrak{a}}$ e, com isso, tem-se $\nu_{\mathfrak{P}}(\mathfrak{a}) \neq \nu_{\mathfrak{P}}(\bar{\mathfrak{a}})$, pois caso contrário $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1})$ seria par. Logo $\mathfrak{P} \neq \bar{\mathfrak{P}}$, senão teríamos $\nu_{\mathfrak{P}}(\mathfrak{a}) = \nu_{\mathfrak{P}}(\bar{\mathfrak{a}})$. Portanto, com esses fatos, concluímos pelo Lemma 3.2.4, que ℓ_1 e m' são bons divisores de m . Ainda, considerando ℓ_1 par, estamos no caso em que $m \equiv 4 \pmod{8}$, ou seja, $m = 4k$ com k ímpar. Assim, com o mesmo raciocínio, mostramos que $\mathfrak{P} \neq \bar{\mathfrak{P}}$ para todo ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$ acima de 2. Logo, tem-se que $\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Q}(\zeta_{m/4}) \neq \bar{\mathfrak{P}}'$, já que 2 é totalmente ramificado em $K|\mathbb{Q}(\zeta_{m/4})$. Portanto, tem-se que $\mathfrak{P} \neq \bar{\mathfrak{P}}'$ para todo ideal primo $\mathfrak{P}'$ de $\mathcal{O}_{\mathbb{Q}(\zeta_{m/4})}$ acima de 2, ou seja, 2 é norma de $m/4$. Reciprocamente, notemos que, da Proposição 3.1.16, mostrar a existência de um reticulado ideal Arakelov-modular de grau ℓ do tipo traço em K é equivalente a encontrar uma decomposição do tipo $\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{a}\bar{\mathfrak{a}}$, para algum ideal fracionário $\mathfrak{a}$ de K e $\lambda \in K^\times$ com $\ell = \lambda\bar{\lambda}$. No entanto, pelo Lema 3.2.5, se tal decomposição existe, então $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1})$ é par sempre que $\mathfrak{P} = \bar{\mathfrak{P}}$, onde $\mathfrak{P}$ é um ideal primo de $\mathcal{O}_K$. Agora, se possível, tomemos $\mathfrak{P}$ um ideal primo de $\mathcal{O}_K$ com $\mathfrak{P} = \bar{\mathfrak{P}}$ e $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1})$ ímpar, onde $\lambda^2 = u\ell$ para $u \in \{\pm 1, \pm i\}$ e, portanto, estamos assumindo que não existe reticulado ideal nas condições desejadas. Como $\ell \mid m$, segue que $\mathfrak{P}$ divide $m\mathcal{O}_K$ pois sendo $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1})$ ímpar e, assim, não nulo, tem-se que $\mathfrak{P}$ divide $\lambda\mathcal{O}_K$ e daí como $\ell\mathcal{O}_K = \lambda^2\mathcal{O}_K$, segue que $\mathfrak{P}$ divide $\ell\mathcal{O}_K$ que divide $m\mathcal{O}_K$. Além disso, tem-se que $\mathfrak{P}$ não divide $\ell_1 m' \mathcal{O}_K$, pois caso contrário, considerando p um primo abaixo de $\mathfrak{P}$ e, assim, divisor de $\ell_1 m'$, que é norma para k' onde $k' = m/p^{r_p}$ caso p seja primo ímpar, que segue do fato que $\ell_1 m'$ é um bom divisor de m e $k' = m/4$ caso $p = 2$ que segue da hipótese que 2 é norma de $m/4$. Assim, teríamos que p é norma de k' que implicaria que

$$\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Q}(\zeta_{k'}) \neq \bar{\mathfrak{P}}',$$

o que é um absurdo, pois como $\mathfrak{P} = \bar{\mathfrak{P}}$, segue que $\mathfrak{P} \cap \mathbb{Q}(\zeta_{k'}) = \bar{\mathfrak{P}} \cap \overline{\mathbb{Q}(\zeta_{k'})} = \bar{\mathfrak{P}} \cap \mathbb{Q}(\zeta_{k'})$. Portanto, $\mathfrak{P}$ divide $m\mathcal{O}_K$ e não divide $\ell_1 m' \mathcal{O}_K$ e, com isso, $\mathfrak{P}$ divide $\ell_2 \mathcal{O}_K$. Considerando p um primo abaixo de $\mathfrak{P}$, então se p é ímpar, então $p \equiv 3 \pmod{4}$ e daí $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(p) = p^{r-1}(p-1) \equiv 2p^{r-1} \pmod{4}$ e, portanto, $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(\ell)/2 \equiv p^{r-1} \pmod{2}$. Como p^{r-1} é ímpar, segue que $\nu_{\mathfrak{P}}(\lambda)$ é ímpar com $\nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}}) = p^{r-1}(pr-r-1)$ ímpar e, deste modo, $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1}) = \nu_{\mathfrak{P}}(\lambda) - \nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}})$ seria par. Se $p = 2$, então, das condições assumidas, $8 \mid m$ e logo $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(p) = 2^{r-1}$, com $r \geq 3$ pois $8 \mid m$. Assim, $\nu_{\mathfrak{P}}(\lambda) = \nu_{\mathfrak{P}}(\ell)/2 = 2^{r-2}$ e, portanto, $\nu_{\mathfrak{P}}(\lambda)$ é par com $\nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}}) = 2^{r-1}(r-1)$ também par, implicando em $\nu_{\mathfrak{P}}(\lambda \mathcal{D}_{K|\mathbb{Q}}^{-1}) = \nu_{\mathfrak{P}}(\lambda) - \nu_{\mathfrak{P}}(\mathcal{D}_{K|\mathbb{Q}})$ ser par, o que nos leva ao absurdo. ■

Nos resultados a seguir, buscamos formas de simplificar o Teorema 3.2.6 no intuito de sistematizar a busca por corpos ciclotômicos que possuam um reticulado ideal Arakelov-modular.

Proposição 3.2.7. *Se p é um primo ímpar tal que $p \mid m$ com $m = p^r m'$ e $\text{mdc}(p, m') = 1$, então p é um bom divisor de m se, e somente se, p é norma de m' .*

Demonstração: Se p é norma de m' , então $\mathfrak{P} \neq \bar{\mathfrak{P}}$ para todo ideal primo $\mathfrak{P}$ de $K' = \mathbb{Q}(\zeta_{m'})$ acima de p . Com isso, como $p \nmid m'$, segue que $p\mathcal{O}_{K'} = \prod \mathfrak{P}_i \prod \bar{\mathfrak{P}}_i$. Logo, $p\mathcal{O}_K = (\prod \mathfrak{p}_i \prod \bar{\mathfrak{p}}_i)^{\phi(p^r)}$, onde $\mathfrak{p}_i^{\phi(p^r)} = \mathfrak{P}_i \mathcal{O}_K$. Assim, $\mathfrak{p}_i$ e $\bar{\mathfrak{p}}_i$ dividem $\mathcal{D}_{K|\mathbb{Q}}$ e, portanto, tem-se que p um bom divisor de m . Reciprocamente, se p é bom divisor de m , então $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{Q}\mathfrak{J}\bar{\mathfrak{J}}$, para $\mathfrak{J}$ acima de p e $\mathfrak{Q}$ primo com p . Tomando $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ acima de p , então tem-se que

$$a = p^r(pr - r - 1) = \nu_{\mathfrak{p}}(\mathcal{D}_{K|\mathbb{Q}}) = \nu_{\mathfrak{p}}(\mathfrak{Q}) + \nu_{\mathfrak{p}}(\mathfrak{J}\bar{\mathfrak{J}}) = \nu_{\mathfrak{p}}(\mathfrak{J}\bar{\mathfrak{J}})$$

é ímpar e, portanto, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, pois caso contrário, teríamos $\mathfrak{p}$ na fatoração de $\mathfrak{J}$ e $\bar{\mathfrak{J}}$, e assim o expoente de $\mathfrak{p}$ em $\mathfrak{J}\bar{\mathfrak{J}}$ seria par. Considerando $\mathfrak{P} = \mathfrak{p} \cap K'$, como $\mathfrak{p}$ é totalmente ramificado em $K|K'$, segue que existe um único primo acima de $\mathfrak{P}$ em K que é $\mathfrak{p}$. Portanto, $\mathfrak{P} \neq \bar{\mathfrak{P}}$, ou seja, p é norma de m' . ■

Proposição 3.2.8. *Seja p um primo tal que $p \nmid m'$. Então, p é uma norma de m' se, e somente se, $f_p = \min\{f' ; p^{f'} \equiv 1 \pmod{m'}\}$ satisfaz uma das situações:*

1. *é ímpar;*
2. *é par com $p^{f_p/2} \not\equiv -1 \pmod{m'}$.*

Demonstração: Para $K' = \mathbb{Q}(\zeta_{m'})$ e $F' = \mathbb{Q}(\zeta_{m'} + \zeta_{m'}^{-1})$, sejam $\mathfrak{P}$ um ideal primo de $\mathcal{O}_{K'}$ acima de p e consideremos $G_{\mathfrak{P}}$ o grupo de decomposição de $\mathfrak{P}$ sobre K' . Vejamos se a conjugação pertence a $G_{\mathfrak{P}}$. Como $p \nmid m'$, segue que $\mathfrak{P}$ não ramifica em $K'|\mathbb{Q}$ e, com isso, tem-se que $G_{\mathfrak{P}}$ é cíclico gerado pelo elemento de Frobenius $\sigma_{\mathfrak{P}}$ tal que $\sigma_{\mathfrak{P}}(\zeta_{m'}) = \zeta_{m'}^p$. Agora, caso f_p seja ímpar, então $G_{\mathfrak{P}}$ não contém nenhum elemento de ordem 2 e, em particular, a conjugação complexa não pertence a $G_{\mathfrak{P}}$. Agora, se f_p é par, então o único elemento de ordem 2 em $G_{\mathfrak{P}}$ é $\sigma_{\mathfrak{P}}^{f_p/2}$. Com isso, p não é norma de $K'|F'$ se, e somente se, $\sigma_{\mathfrak{P}}^{f_p/2}$ é a conjugação complexa, ou seja,

$$\zeta_{m'}^{p^{f_p/2}} = \sigma_{\mathfrak{P}}^{f_p/2}(\zeta_{m'}) = \bar{\zeta}_{m'} = \zeta_{m'}^{-1} \iff p^{f_p/2} \equiv -1 \pmod{m'},$$

o que prova a proposição. ■

Corolário 3.2.9. *Seja p um primo ímpar tal que $m = p^r m'$ com $\text{mdc}(p, m') = 1$. Então, p é um bom divisor de m se, e somente se, ou f_p é ímpar ou f_p é par e $p^{f_p/2} \not\equiv -1 \pmod{m'}$.*

Agora, para todo inteiro positivo m e todo número primo p , seja m_p o maior divisor de m relativamente primo a p , ou seja, m_p é dado escrevendo $m = p^r m_p$ com $\text{mdc}(p, m_p) = 1$. Ainda, consideremos $f_p = \min\{f' ; p^{f'} \equiv 1 \pmod{m_p}\}$. Assim, com base nos resultados anteriores, obtem-se o seguinte resultado:

Teorema 3.2.10. *Seja ℓ um inteiro positivo livre de quadrados dividindo m . Assim, existe um reticulado ideal Arakelov-modular de grau ℓ do tipo traço em K se, e somente se, as seguintes condições são satisfeitas:*

1. *Para todo divisor primo p de ℓ tal que $p \equiv 1 \pmod{4}$, tem-se que f_p é ímpar ou*

$$p^{f_p/2} \not\equiv -1 \pmod{m_p};$$

2. *Para todo divisor primo p de m com $p \nmid \ell$, tem-se que $p = 2$, f_p é ímpar ou*

$$p^{f_p/2} \not\equiv -1 \pmod{m_p};$$

3. *Se ℓ é par e $m \equiv 4 \pmod{8}$, então f_2 é ímpar ou $2^{f_2/2} \not\equiv -1 \pmod{m_2}$.*

Exemplo 3.2.11. Consideremos os exemplos:

- Sejam $m = 21$ e $\ell = 3$. Como $m = 3 \cdot 7$, o único divisor primo de ℓ é $3 \not\equiv 1 \pmod{4}$, segue que a condição (1) do Teorema 3.2.10 é satisfeita. Além disso, sendo $f_7 = 1$, pois $7 \equiv 1 \pmod{3}$, tem-se que a condição (2) também é válida. Portanto, pelo Teorema 3.2.10, existe um reticulado ideal do tipo traço e Arakelov-modular de grau 3 em $\mathbb{Q}(\zeta_{21})$ e, com isso, tal reticulado é par com posto $\phi(m) = 12$ e determinante 3^6 .
- Consideremos $m = 40$ e $\ell = 2$. Escrevendo $m = 8 \cdot 5$, segue que o único divisor primo de ℓ é $2 \not\equiv 1 \pmod{4}$. Mais ainda, tem-se que $f_5 = 2$ já que $5^2 \equiv 1 \pmod{8}$ e satisfazendo $5 \equiv -3 \not\equiv -1 \pmod{8}$. Assim, como $m \equiv 0 \pmod{8}$, segue, pelo Teorema 3.2.10, que existe um reticulado ideal do tipo traço e Arakelov-modular de grau 2 em $\mathbb{Q}(\zeta_{40})$. Este reticulado é par de posto $\phi(m) = 16$ e determinante 2^8 .
- Não existe reticulado ideal do tipo traço Arakelov-modular de grau $\ell = 2$ em $\mathbb{Q}(\zeta_m)$ para $m = 36$, pois escrevendo $m = 4 \cdot 9$, tem-se que ℓ é par e $m \equiv 4 \pmod{8}$. Além disso, $f_2 = 6$ é par com $2^3 = 8 \equiv -1 \pmod{9}$, não satisfazendo a condição (3) do Teorema 3.2.10.

Para o caso de reticulados ideais do tipo traço e unimodulares, as condições do Teorema 3.2.10 se resumem ao seguinte:

Corolário 3.2.12. *Existe um reticulado ideal unimodular do tipo traço em K se, e somente se, para todo divisor primo p de m , tem-se que $p = 2$, f_p é ímpar ou $p^{f_p/2} \not\equiv -1 \pmod{m_p}$.*

Exemplo 3.2.13. É impossível obter um reticulado ideal 24-dimensional do tipo traço e unimodular em $\mathbb{Q}(\zeta_{35})$, já que sendo $m = 7 \cdot 5$, tem-se que $f_7 = 4$ é par e $7^2 \equiv -1 \pmod{5}$. No entanto, existe reticulado ideal 24-dimensional do tipo traço e unimodular em $K = \mathbb{Q}(\zeta_{39})$, pois como $m = 39 = 3 \cdot 13$, segue que $f_3 = 3$ e $f_{13} = 1$. Com base no Corolário 3.1.12, façamos a construção desse reticulado unimodular. Sendo 3 e 13 os únicos primos que ramificam em K já que dividem $m = 39$, segue que o número de ideais primos na decomposição de $3\mathcal{O}_K$ e $13\mathcal{O}_K$ são, respectivamente, $s_3 = \phi(13)/f_3 = 4$ e $s_{13} = \phi(3)/f_{13} = 2$. Assim, $3\mathcal{O}_K = (\mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2\bar{\mathfrak{p}}_2)^2$ e $13\mathcal{O}_K = (\mathfrak{q}\bar{\mathfrak{q}})^{12}$ (note que os conjugados estão na decomposição pois f_3 e f_{13} são ímpares). Com isso, $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}_1^i\bar{\mathfrak{p}}_1^i\mathfrak{p}_2^j\bar{\mathfrak{p}}_2^j\mathfrak{q}^k\bar{\mathfrak{q}}^k$. Agora, como

$$3^{24} = N_{K|\mathbb{Q}}(3) = N(\mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2\bar{\mathfrak{p}}_2)^2 = N(\mathfrak{p}_1)^2N(\bar{\mathfrak{p}}_1)^2N(\mathfrak{p}_2)^2N(\bar{\mathfrak{p}}_2)^2 = N(\mathfrak{p}_1)^4N(\mathfrak{p}_2)^4$$

e

$$13^{24} = N_{K|\mathbb{Q}}(13) = N(\mathfrak{q}\bar{\mathfrak{q}})^{12} = N(\mathfrak{q})^{12}N(\bar{\mathfrak{q}})^{12} = N(\mathfrak{q})^{24},$$

segue que $N(\mathfrak{p}_1) = N(\bar{\mathfrak{p}}_1) = 3^3 = N(\mathfrak{p}_2) = N(\bar{\mathfrak{p}}_2)$ e $N(\mathfrak{q}) = N(\bar{\mathfrak{q}}) = 13$. Dessa forma, sendo $|d_K| = 3^{12} \cdot 13^{22}$, segue que

$$3^{12} \cdot 13^{22} = |d_K| = N(\mathcal{D}_{K|\mathbb{Q}}) = N(\mathfrak{p}_1)^iN(\bar{\mathfrak{p}}_1)^iN(\mathfrak{p}_2)^jN(\bar{\mathfrak{p}}_2)^jN(\mathfrak{q})^kN(\bar{\mathfrak{q}})^k = 3^{12i} \cdot 13^{2k},$$

e portanto, $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{q}^{11}\bar{\mathfrak{q}}^{11} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}^{11}\overline{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}^{11}}$. Assim, como na demonstração da Proposição 3.1.11, segue que o reticulado ideal $(\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\mathfrak{q}^{-11}, 1)$ é um reticulado ideal do tipo traço e unimodular de posto 24. Note, além disso, que esse reticulado é par em virtude de que 2 não ramifica em $K|F$.

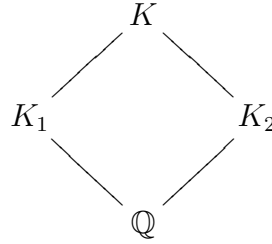
No que segue, faremos uma construção de reticulados ideais do tipo traço e Arakelov-modulares que estende o Exemplo 3.1.17 e mostramos que esses são os únicos reticulados ideais do tipo traço e Arakelov-modulares para os graus especificados.

Como no início da seção, considere m um inteiro positivo ímpar ou divisível por 4, $K = \mathbb{Q}(\zeta_m)$ o m -ésimo corpo ciclotômico e $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ seu subcorpo real maximal. Seja $\ell = p$ um número primo com $p \not\equiv 1 \pmod{4}$ satisfazendo $m = p^r m'$

onde $\text{mdc}(p, m') = 1$, para $r \geq 3$ se $p = 2$ e $r \geq 1$ para p ímpar. Supondo m' um bom divisor de m , então podemos escrever

$$\mathcal{D}_{K|\mathbb{Q}}^{-1} = \mathfrak{Q}\mathfrak{I}\tilde{\mathfrak{I}} ,$$

onde $\mathfrak{Q}$ está acima de p e $\mathfrak{I}$ é um ideal primo com p . Denotando $K_1 = \mathbb{Q}(\zeta_{p^r})$ e $K_2 = \mathbb{Q}(\zeta_{m'})$ e sendo p e m' primos entre si, segue que $K_1 \cap K_2 = \mathbb{Q}$ e $K_1 K_2 = K$. Consideremos, portanto, o seguinte diagrama de corpos:



Seja $\mathfrak{p}$ o único ideal primo de $\mathcal{O}_{K_1}$ acima de p . Tomando $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$ a extensão de $\mathfrak{p}$ em $\mathcal{O}_K$, segue que

$$\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{P}^a \mathfrak{I}\tilde{\mathfrak{I}} \quad (3.5)$$

com $a = p^{r-1}(pr - r - 1)$, já que $\mathcal{D}_{K|\mathbb{Q}} = \mathcal{D}_{K|K_1}(\mathcal{D}_{K_1|\mathbb{Q}}\mathcal{O}_K)$. Se $s = \frac{\phi(p^r) - 2a}{4}$, então temos o seguinte reticulado ideal Arakelov-modular:

Proposição 3.2.14. *O reticulado ideal $(\mathfrak{a}, 1)$, onde $\mathfrak{a} = \mathfrak{P}^s \mathfrak{I}^{-1}$, é Arakelov-modular de grau p em K . Mais ainda, se m não é uma potência de 2, então o reticulado é par.*

Demonstração: O reticulado ideal dual $(\mathfrak{a}^\#, 1)$ de $(\mathfrak{a}, 1)$ para $\mathfrak{a} = \mathfrak{P}^s \mathfrak{I}^{-1}$ é

$$\mathfrak{a}^\# = \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{P}}^{-s} \tilde{\mathfrak{I}} .$$

Mostremos que $(\mathfrak{a}, 1)$ e $(\mathfrak{a}^\#, p)$ são Arakelov-equivalentes. De fato, existe $\sqrt{-p} \in K$ que satisfaz $p = \sqrt{-p}\overline{\sqrt{-p}}$. Como já verificado no Exemplo 3.1.14, tem-se que o único ideal primo $\mathfrak{p}$ de $\mathcal{O}_{K_1}$ satisfazendo $\sqrt{-p} \mathfrak{p}^{-(s+a)} = \mathfrak{p}^s$ e, portanto, vale a igualdade $\sqrt{-p} \bar{\mathfrak{P}}^{-(s+a)} = \mathfrak{P}^s$, já que $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$. Assim, como $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{P}^a \mathfrak{I}\tilde{\mathfrak{I}}$, segue que

$$\mathfrak{a}^\# = \mathcal{D}_{K|\mathbb{Q}}^{-1} \bar{\mathfrak{P}}^{-s} \tilde{\mathfrak{I}} = \mathfrak{P}^{-a} \mathfrak{I}^{-1} \tilde{\mathfrak{I}}^{-1} \mathfrak{P}^{-s} \tilde{\mathfrak{I}} = \mathfrak{P}^{-(a+s)} \mathfrak{I}^{-1} = \frac{1}{\sqrt{-p}} \mathfrak{P}^s \mathfrak{I}^{-1} = \frac{1}{\sqrt{-p}} \mathfrak{a} .$$

Com isso, o reticulado ideal $(\mathfrak{a}, 1)$ é Arakelov-modular de grau p . Além disso, se m não é uma potência de 2, então 2 não ramifica em $K|F$ e, pela Proposição 3.1.10,

segue que o reticulado é par. ■

Observamos que na construção da Proposição 3.2.14, a condição restritiva $p \not\equiv 1 \pmod{4}$ se faz necessária pois não existe reticulado ideal do tipo traço e Arakelov-modular com $m = p^r$, para $r \geq 1$ e $p \equiv 1 \pmod{4}$. Supondo a existência de um reticulado ideal $(\mathfrak{a}, 1)$ com tais propriedades, teríamos que $\det(\mathfrak{a}) = \ell^{(p-1)/2}$, para algum ℓ inteiro. Como $(p-1)/2$ é par, segue que $\det(\mathfrak{a})$ é um quadrado perfeito. No entanto, sendo $\det(\mathfrak{a}) = N(\mathfrak{a})^2 |d_K|$ e pelo Teorema A.6.1, como $|d_K| = p^a$ para $a = p^{r-1}(pr - r - 1)$, segue que a é ímpar e, portanto, $\det(\mathfrak{a})$ não é um quadrado perfeito, o que nos leva ao absurdo. Abaixo, veremos a caracterização dos reticulados ideais do tipo traço e Arakelov-modulares para graus primos.

Teorema 3.2.15. *Todo reticulado ideal do tipo traço e Arakelov-modular de grau p em K é obtido através da Proposição 3.2.14.*

Demonstração: Seja $(\mathfrak{a}, 1)$ um reticulado ideal Arakelov-modular de grau p em K . Pela Proposição 1.6.6, segue que $\det(\mathfrak{a}) = p^{\phi(m)/2}$. Assim, pela Proposição 3.1.11, segue que existem $\mathfrak{Q}$ e $\mathfrak{J}$ ideais fracionários de K com $N(\mathfrak{Q}) = p^{\phi(m)/2}$ e $\mathfrak{J}_1 = \mathfrak{a}^{-1}$ tal que $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{Q}\mathfrak{J}_1\bar{\mathfrak{J}}_1$. Agora, sendo $(\mathfrak{a}, 1)$ Arakelov-modular de grau p , pela Proposição 3.1.16, segue que existe $\lambda \in K$ tal que $p = \lambda\bar{\lambda}$ satisfazendo

$$\lambda\mathcal{O}_K = \mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{J}_1^{-1}\bar{\mathfrak{J}}_1^{-1}\mathfrak{Q}\mathfrak{J}_1\bar{\mathfrak{J}}_1 = \mathfrak{Q}.$$

Sendo $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$ onde $\mathfrak{p}$ é o único ideal primo de $\mathcal{O}_{K_1}$ acima de p onde $K_1 = \mathbb{Q}(\zeta_{p^r})$, e como $\lambda\mathcal{O}_K = \bar{\lambda}\mathcal{O}_K$, segue que

$$\mathfrak{P}^{\phi(p^r)} = p\mathcal{O}_K = (\lambda\mathcal{O}_K)(\bar{\lambda}\mathcal{O}_K) = \mathfrak{Q}^2$$

e, portanto, $\mathfrak{Q} = \mathfrak{P}^{\phi(p^r)/2} = \mathfrak{P}^{a+2s}$. De (3.5), segue que

$$\mathfrak{P}^a\mathfrak{J}\bar{\mathfrak{J}} = \mathcal{D}_{K|\mathbb{Q}} = \mathfrak{Q}\mathfrak{J}_1\bar{\mathfrak{J}}_1 = \mathfrak{P}^{a+2s}\mathfrak{J}_1\bar{\mathfrak{J}}_1,$$

e, assim, $\mathfrak{J}_1 = \mathfrak{P}^{-s}\mathfrak{J}$. Portanto, $\mathfrak{a} = \mathfrak{J}_1^{-1} = \mathfrak{P}^s\mathfrak{J}^{-1}$. ■

No que segue, apresentamos alguns construções explícitas de reticulados ideais do tipo traço e Arakelov-modulares.

Exemplo 3.2.16. Consideremos as construções:

- Pelo Exemplo 3.2.11, existe um reticulado ideal do tipo traço e Arakelov-modular de grau 3 em $K = \mathbb{Q}(\zeta_{21})$. Vejamos uma construção desse reticulado.

Para isso, encontremos a decomposição de $\mathcal{D}_{K|\mathbb{Q}}$. Como os únicos primos que ramificam em K são 3 e 7 (pois dividem m), segue que na decomposição de $3\mathcal{O}_K$ existem $s_3 = \phi(7)/f_3$ ideais primos. Sendo $f_3 = 6$, segue que $s_3 = 1$, ou seja, $3\mathcal{O}_K = \mathfrak{p}^2$. Ainda, o número de ideais primos na decomposição de $7\mathcal{O}_K$ é $s_7 = \phi(3)/f_7$. Como $f_7 = 1$, segue que $s_7 = 2$ e, portanto, $7\mathcal{O}_K = \mathfrak{q}^6\bar{\mathfrak{q}}^6$ (lembre que sendo $K|\mathbb{Q}$ uma extensão de Galois, como f_7 é ímpar, segue que seu conjugado complexo de ideais que ramificam também ramificam). Agora,

$$3^{12} = |\mathrm{N}_{K|\mathbb{Q}}(3)| = \mathrm{N}(3\mathcal{O}_K) = \mathrm{N}(\mathfrak{p})^2$$

e

$$7^{12} = |\mathrm{N}_{K|\mathbb{Q}}(7)| = \mathrm{N}(7\mathcal{O}_K) = \mathrm{N}(\mathfrak{q})^6\mathrm{N}(\bar{\mathfrak{q}})^6 = \mathrm{N}(\mathfrak{q})^{12}$$

e, assim, tem-se que $\mathrm{N}(\mathfrak{p}) = 3^6$ e $\mathrm{N}(\mathfrak{q}) = \mathrm{N}(\bar{\mathfrak{q}}) = 7$. Sendo $|d_K| = 3^6 \cdot 7^{10}$ e escrevendo $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}^i\mathfrak{q}^j\bar{\mathfrak{q}}^j$, segue que

$$3^6 \cdot 7^{10} = |d_K| = \mathrm{N}(\mathcal{D}_{K|\mathbb{Q}}) = \mathrm{N}(\mathfrak{p})^i\mathrm{N}(\mathfrak{q})^{2j} = 3^{6i} \cdot 7^{2j}.$$

Com isso, tem-se que $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p} \cdot \mathfrak{q}^5 \cdot \bar{\mathfrak{p}}^5$. Notando que $s = \frac{\phi(p^r)-2a}{4} = 0$, pela Proposição 3.2.14, o reticulado ideal $(\mathfrak{q}^{-5}, 1)$ é Arakelov-modular de grau 3 em K com determinante 3^6 . Além disso, é par, já que 2 não ramifica em $K|F$.

- Pelo Exemplo 3.2.11, existe um reticulado ideal do tipo traço e Arakelov-modular de grau 2 em $K = \mathbb{Q}(\zeta_{40})$. Os únicos primos que ramificam em K são 2 e 5 já que $m = 40 = 2^3 \cdot 5$, assim, sendo $f_2 = 4$ e $f_5 = 2$, segue que $s_2 = \phi(5)/f_2 = 1$ e $s_5 = \phi(8)/f_5 = 2$ e daí tem-se as seguintes decomposições: $2\mathcal{O}_K = \mathfrak{p}^4$ e $5\mathcal{O}_K = (\mathfrak{q}\bar{\mathfrak{q}})^4$, já que $\phi(8) = 4$ e $\phi(5) = 4$ (note que o conjugado complexo do ideal $\mathfrak{q}$ ramifica pois $5^{f_5/2} \not\equiv -1 \pmod{8}$) e, com isso, $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}^i\mathfrak{q}^j\bar{\mathfrak{q}}^j$. Agora, como

$$2^{16} = \mathrm{N}_{K|\mathbb{Q}}(2) = \mathrm{N}(\mathfrak{p})^4$$

e

$$5^{16} = \mathrm{N}_{K|\mathbb{Q}}(5) = \mathrm{N}(\mathfrak{q})^4\mathrm{N}(\bar{\mathfrak{q}})^4 = \mathrm{N}(\mathfrak{q})^8,$$

segue que $\mathrm{N}(\mathfrak{p}) = 2^4$ e $\mathrm{N}(\mathfrak{q}) = \mathrm{N}(\bar{\mathfrak{q}}) = 5^2$. Assim, sendo $|d_K| = 2^{32} \cdot 5^{12}$, tem-se que

$$2^{32} \cdot 5^{12} = |d_K| = \mathrm{N}(\mathcal{D}_{K|\mathbb{Q}}) = \mathrm{N}(\mathfrak{p})^i\mathrm{N}(\mathfrak{q})^j\mathrm{N}(\bar{\mathfrak{q}})^j = 2^{4i} \cdot 5^{2j} \cdot 5^{2j} = 2^{4i} \cdot 5^{4j}$$

implicando que $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}^8 \cdot \mathfrak{q}^3 \cdot \bar{\mathfrak{q}}^3$. Desse modo, como $s = \frac{\phi(8)-2 \cdot 8}{4} = -3$, segue, pela Proposição 3.2.14, que o reticulado ideal $(\mathfrak{p}^{-3}\mathfrak{q}^{-3}, 1)$ é par e Arakelov-modular de grau 2 em K com determinante 2^8 .

Conclusão

Neste capítulo apresentamos um estudo sobre a teoria de reticulados ideais, em que estudamos os invariantes desses reticulados e as principais propriedades envolvidas com o conceito. Finalizando, estudamos resultados que garantem, sob certas hipóteses, a existência de reticulados ideais modulares do tipo traço em corpos ciclotômicos, fornecendo condições sobre alguns invariantes numéricos do corpo estudado. Em posse dessas condições, estudamos a construção e a caracterização de reticulados ideais modulares para graus especiais de modularidade em corpos ciclotômicos com as propriedades requeridas.

Conclusões

Finalizando, apresentamos nesta seção uma análise do que foi desenvolvido em cada parte deste texto, expondo também nossas conclusões sobre os assuntos apresentados.

O Capítulo 1 foi dedicado à apresentação dos resultados da teoria de reticulados. Embora seja comum na literatura o desenvolvimento do tema para o espaço euclidiano usual $\mathbb{R}^n$, notamos que as propriedades são estendidas de forma natural a espaços euclidianos abstratos. Isto nos permite, dentre outras coisas, compreender a natureza geral dos reticulados nas suas diversas abordagens.

Com o estudo da dualidade feito na Seção 1.3, vimos as relações entre os invariantes de um reticulado com os invariantes de seu reticulado dual, bem como as caracterizações de reticulados integrais e unimodulares expressas pelo reticulado dual através de inclusões. Além disso, provamos a expressão para o determinante de um reticulado integral dada na Proposição 1.4.11. Estes resultados foram de grande utilidade para a obtenção e o cálculo de determinantes de reticulados ideais feitos no Capítulo 3.

Na Seção 1.5, vimos os conceitos e resultados relacionados aos empacotamentos esféricos de um espaço euclidiano dados por reticulados. Com esta abordagem, vimos a generalização do problema de empacotamento esférico para espaços euclidianos quaisquer e também expressões para densidade e densidade de centro obtidas a partir dos invariantes dos reticulados.

Apresentamos ainda os resultados que decorrem do conceito de reticulado modular, introduzido na Seção 1.6, onde vimos que um reticulado similar ao seu dual possui o determinante pré-determinado pela norma da similaridade, a qual chamamos de grau de modularidade do reticulado modular, que foi mostrado ser

sempre um inteiro positivo, e também as relações de inclusões com seu reticulado dual.

No Capítulo 2, apresentamos uma introdução à teoria das theta séries de reticulados pares, onde o foco dado foi nas propriedades que permitissem estabelecer uma conexão entre as theta séries de reticulados modulares pares com formas modulares.

Com isso, na Seção 2.1 do capítulo, vimos algumas propriedades importantes das theta séries de reticulados pares que culminam com a identidade do Teorema 2.1.10.

O objetivo principal da Seção 2.2 foi mostrar que a theta série de um reticulado unimodular par é uma forma modular para o grupo modular completo. Para isto introduzimos o conceito de forma modular e suas principais propriedades chegando ao resultado desejado.

Na Seção 2.3, estabelecemos o resultado que generaliza a relação entre reticulados unimodulares e formas modulares para reticulados com graus de modularidade quaisquer. A importância dessa conexão é que permite, dentre outras coisas, resultados de classificação para reticulados.

No Capítulo 3, o tema principal foi a teoria de reticulados ideais, onde o enfoque dado foi a formalização do conceito e o desenvolvimento dos invariantes destes reticulados bem como o estudo de reticulados ideais modulares do tipo traço em corpos ciclotômicos.

A Seção 3.1 visou o desenvolvimento do tema de acordo com o tratamento do Capítulo 1 para espaços euclidianos abstratos. Com isso, obtemos, com base na Teoria dos Números Algébricos, a caracterização dos reticulados ideais pela forma traço. Isto permitiu a busca de diversos invariantes como o reticulado dual, o determinante de reticulados ideais e condições para integralidade e paridade para essas estruturas, baseadas apenas em propriedades do corpo de números. Além disso, vimos condições suficientes para a existência de reticulados ideais do tipo traço com determinante determinado e de reticulados Arakelov-modulares em um corpo de números.

Na Seção 3.2, estudamos os resultados de existência de reticulados ideais modulares do tipo traço em corpos ciclotômicos, que foram obtidos através da caracterização de existência de reticulados Arakelov-modulares fornecida na Proposição 3.1.16, cujas condições são dadas no corpo de números. Com isso, simplificamos os resultados através de condições numéricas obtidas desenvolvendo o conceito de norma e de bom divisor. Deste modo, construímos alguns reticulados modulares através de reticulados ideais e, mais ainda, fornecemos uma construção de reticulado ideal Arakelov-modular para graus primos e mostramos que estes são

os únicos reticulados ideais modulares com esta propriedade no corpo abordado, estabelecendo assim uma caracterização para reticulados ideais modulares de graus primos em corpos ciclotômicos.

Com tais construções feitas nos exemplos, temos a importância da caracterização das condições de existência para reticulados ideais em corpos ciclotômicos com parâmetros pré-estabelecidos. Tal abordagem permite que as construções desejadas sejam direcionadas às propriedades numéricas do corpo, o que facilita a busca e também a caracterização dos reticulados ideais obtidos através dos corpos com tais propriedades.

Desta forma, fica a perspectiva de sistematizar a busca de $\mathbb{Z}$ -bases para tais construções de modo que, quando imergidos em $\mathbb{R}^n$ através do homomorfismo de Minkowski e seus homomorfismos torcidos, possam ser utilizados para alguns canais de comunicação, especialmente, no Gaussiano, visto que a densidade de centro de reticulados modulares são, em geral, boas. Mais ainda, uma expectativa mais arrojada seria, se possível, a mesma análise de caracterização das condições de existência para reticulados ideais modulares em corpos maximais reais de corpos ciclotômicos, uma vez que em canais Rayleigh Fading são necessários construções via corpos totalmente reais para a maximização da diversidade do reticulado.

Referências Bibliográficas

- [1] BAYER-FLUCKIGER, E. Lattices and number fields. *Algebraic geometry: Hirzebruch 70 (Warsaw, 1998)*, *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1999, pp. 69–84.
- [2] BAYER-FLUCKIGER, E. Cyclotomic modular lattices. *J. Théor. Nombres Bordeaux* 12, 2 (2000), 273–280. Colloque International de Théorie des Nombres (Talence, 1999).
- [3] BAYER-FLUCKIGER, E. Ideal lattices. *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*. Cambridge Univ. Press, Cambridge, 2002, pp. 168–184.
- [4] BAYER-FLUCKIGER, E., OGGIER, F., VITERBO, E. New algebraic constructions of rotated $\mathbf{Z}^n$ -lattice constellations for the Rayleigh fading channel. *IEEE Trans. Inform. Theory* 50, 4 (2004), 702–714.
- [5] BAYER-FLUCKIGER, E., OGGIER, F., VITERBO, E. Algebraic lattice constellations: bounds on performance. *IEEE Trans. Inform. Theory* 52, 1 (2006), 319–327.
- [6] BAYER-FLUCKIGER, E., SUAREZ, I. Modular lattices over cyclotomic fields. *J. Number Theory* 114, 2 (2005), 394–411.
- [7] CONWAY, J. H., SLOANE, N. J. A. *Sphere packings, lattices and groups*, Springer-Verlag, New York, 1999.
- [8] EBELING, W. *Lattices and codes*, Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 2002. A course partially based on lectures by F. Hirzebruch.
- [9] KOBLITZ, N. *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, 1993.

- [10] LANG, S. *Algebra*, Springer-Verlag, New York, 2002.
- [11] LAVOR, C. C., ALVES, M. M. S., SIQUEIRA, R. M., AND COSTA, S. I. R. Uma introdução à teoria de códigos. *XXIX Congresso Nacional de Matemática Aplicada e Computacional*. SBMAC, São Carlos, 2006.
- [12] MARTINET, J. *Perfect lattices in Euclidean spaces*, Springer-Verlag, Berlin, 2003.
- [13] NARKIEWICZ, W. *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Berlin, 2004.
- [14] NEUKIRCH, J. *Algebraic number theory*, Springer-Verlag, Berlin, 1999.
- [15] QUEBBEMANN, H.-G. Modular lattices in Euclidean spaces. *J. Number Theory* 54, 2 (1995), 190–202.
- [16] QUEBBEMANN, H.-G. Atkin-Lehner eigenforms and strongly modular lattices. *Enseign. Math. (2)* 43, 1-2 (1997), 55–65.
- [17] REMMERT, R. *Theory of complex functions*, Springer-Verlag, New York, 1991.
- [18] SAMUEL, P. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.
- [19] SERRE, J.-P. *A course in arithmetic*. Springer-Verlag, New York, 1973.
- [20] WASHINGTON, L. C. *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1997.

Apêndice A

Apêndice: Tópicos em teoria dos números algébricos

Neste apêndice, selecionamos os principais conceitos e resultados da teoria dos números algébricos para uma breve explanação dos tópicos que foram utilizados ao longo da dissertação. Nosso intuito, com isso, é tornar o texto auto-contido desses pré-requisitos e, por isso, omitimos as demonstrações para não tornar tal parte demasiadamente longa. Para uma exposição mais detalhada, sugerimos ao leitor as referências [18] e [14].

A.1 Domínios de Dedekind

Consideremos $\mathfrak{o}$ um domínio de Dedekind¹ com corpo de frações K . Dados ideais $\mathfrak{a}$ e $\mathfrak{b}$ de $\mathfrak{o}$, dizemos $\mathfrak{a}$ divide $\mathfrak{b}$ e denotamos $\mathfrak{a} \mid \mathfrak{b}$ se $\mathfrak{b} \subseteq \mathfrak{a}$. Com isso temos o seguinte resultado:

Proposição A.1.1. *Todo ideal próprio $\mathfrak{a} \neq 0$ de $\mathfrak{o}$ admite, a menos da ordem dos*

¹Um domínio de Dedekind é um domínio integralmente fechado, noetheriano e tal que todo ideal primo não nulo seja um ideal maximal.

fatores, uma única fatoração

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}} ,$$

em ideais primos $\mathfrak{p}$ de $\mathfrak{o}$ com $\nu_{\mathfrak{p}} \in \mathbb{N}$ e $\nu_{\mathfrak{p}} = 0$ para quase todo $\mathfrak{p}$.

Demonstração: Ver ([14], cap. I, § 3). ■

Chamamos de *ideal fracionário* de K , todo $\mathfrak{o}$ -submódulo $\mathfrak{a} \neq 0$ de K finitamente gerado. Note que um ideal $\mathfrak{a} \subseteq \mathfrak{o}$ é um ideal fracionário e, por isso, por distinção o chamamos de *ideal inteiro*. É fácil notar que um $\mathfrak{o}$ -submódulo $\mathfrak{a} \neq 0$ de K é um ideal fracionário se, e somente se, existe $c \in \mathfrak{o}$ não nulo tal que $c\mathfrak{a} \subseteq \mathfrak{o}$. Dessa forma, munido do produto usual de submódulos, o conjunto dos ideais fracionários possuem a propriedade enunciada abaixo:

Proposição A.1.2. *O conjunto dos ideais fracionários de K formam um grupo abeliano cujo elemento neutro é $\mathfrak{o}$ e o inverso de um ideal fracionário $\mathfrak{a}$ é dado por*

$$\mathfrak{a}^{-1} = \{x \in K ; x\mathfrak{a} \subseteq \mathfrak{o}\} .$$

Demonstração: Ver ([14], cap. I, § 3). ■

Corolário A.1.3. *Todo ideal fracionário $\mathfrak{a} \neq 0$ de K admite, a menos da ordem dos fatores, uma única fatoração*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}} ,$$

em ideais primos $\mathfrak{p}$ de $\mathfrak{o}$ com $\nu_{\mathfrak{p}} \in \mathbb{Z}$ e $\nu_{\mathfrak{p}} = 0$ para quase todo $\mathfrak{p}$.

Demonstração: Ver ([14], cap. I, § 3). ■

Observe que na fatoração do ideal fracionário

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

de K , o inteiro $\nu_{\mathfrak{p}}$ é o maior expoente, em módulo, do ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ na decomposição

$$\mathfrak{a} = \mathfrak{p}^{\nu_{\mathfrak{p}}} \mathfrak{b} ,$$

com $\mathfrak{p} \nmid \mathfrak{b}$. Com isso, o valor $\nu_{\mathfrak{p}} = \nu_{\mathfrak{p}}(\mathfrak{a})$ é chamada a *valorização $\mathfrak{p}$ -ádica* de $\mathfrak{a}$ que satisfaz

$$\nu_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = \nu_{\mathfrak{p}}(\mathfrak{a}) + \nu_{\mathfrak{p}}(\mathfrak{b}) \quad \text{e} \quad \nu_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) \geq \min\{\nu_{\mathfrak{p}}(\mathfrak{a}), \nu_{\mathfrak{p}}(\mathfrak{b})\} ,$$

para dois ideais fracionários $\mathfrak{a}$ e $\mathfrak{b}$ de K . Para $a \in K$, definimos a *valorização $\mathfrak{p}$ -ádica* de a por $\nu_{\mathfrak{p}}(a) = \nu_{\mathfrak{p}}((a))$, para (a) o ideal principal $a\mathfrak{o}$ de $\mathfrak{o}$.

A.2 Traços, normas e elementos integrais

Consideremos $L|K$ uma extensão de corpos. Definimos o *traço* e a *norma* de um elemento $x \in L$, respectivamente, pelo traço e determinante do endomorfismo de K -espaço vetorial $T_x : L \rightarrow L$ dado por $T_x(y) = xy$, onde $y \in L$, denotados, respectivamente, por $\text{Tr}_{L|K}(x)$ e $N_{L|K}(x)$.

Proposição A.2.1. *Se $L|K$ é uma extensão separável de corpos com grau $[L : K] = n < \infty$ e munida dos monomorfismos $\sigma_i : L \rightarrow \overline{K}$, para $i = 1, 2, \dots, n$, onde $\overline{K}$ denota o fecho algébrico de K , então vale*

$$\text{Tr}_{L|K}(x) = \sum_{i=1}^n \sigma_i(x) \quad \text{e} \quad N_{L|K}(x) = \prod_{i=1}^n \sigma_i(x) .$$

Demonstração: Ver ([14], cap. I, § 2). ■

Observamos que numa torre de extensões finitas de corpos $F \subset K \subset L$, vale

$$\text{Tr}_{L|F} = \text{Tr}_{K|F} \circ \text{Tr}_{L|K} \quad \text{e} \quad N_{L|F} = N_{K|F} \circ N_{L|K} .$$

Para uma extensão $L|K$ de corpos, definimos o *discriminante* de uma K -base $\{x_1, x_2, \dots, x_n\}$ de L por

$$d(x_1, \dots, x_n) = \det(\text{Tr}_{L|K}(x_i x_j)) .$$

Proposição A.2.2. *Se $L|K$ é uma extensão separável de corpos com base $\{x_1, x_2, \dots, x_n\}$ e munida dos monomorfismos $\sigma_i : L \rightarrow \overline{K}$, para $i = 1, 2, \dots, n$, onde $\overline{K}$ denota o fecho algébrico de K , então*

$$d(x_1, \dots, x_n) = \det((\sigma_i(x_j)))^2 \neq 0 .$$

Além disso, a forma bilinear $(x, y) \mapsto \text{Tr}_{L|K}(xy)$ de L em K é não-degenerada.

Demonstração: Ver ([14], cap. I, § 2). ■

Seja $\mathfrak{o} \subseteq \mathcal{O}$ uma extensão de anéis. Dizemos que um elemento $b \in \mathcal{O}$ é *inteiro* sobre $\mathfrak{o}$, se existe um polinômio $f \in \mathfrak{o}[x]$ mônico e não nulo tal que $f(b) = 0$. No caso em que todos os elementos de $\mathcal{O}$ são inteiros sobre $\mathfrak{o}$, dizemos que $\mathcal{O}$ é *inteiro sobre $\mathfrak{o}$* . O conjunto

$$\overline{\mathfrak{o}} = \{b \in \mathcal{O} ; b \text{ é inteiro sobre } \mathfrak{o}\}$$

é um anel, chamado *fecho inteiro de $\mathfrak{o}$ em $\mathcal{O}$* . Quando $\mathfrak{o} = \overline{\mathfrak{o}}$, dizemos que $\mathfrak{o}$ é *integralmente fechado em $\mathcal{O}$* .

Consideremos a partir de agora, a seguinte situação: $\mathfrak{o}$ um domínio integralmente fechado em seu corpo de frações K , $L|K$ uma extensão finita de corpos e $\mathcal{O}$ o fêcho inteiro de $\mathfrak{o}$ em L .

Proposição A.2.3. *Seja $L|K$ uma extensão separável de corpos. Se $x \in \mathcal{O}$, então $\text{Tr}_{L|K}(x), N_{L|K}(x) \in \mathfrak{o}$.*

Demonstração: Ver ([14], cap. I, § 2). ■

Ainda, consideremos $\mathcal{O}$ um domínio principal. Podemos afirmar a seguinte propriedade para os $\mathcal{O}$ -módulos finitamente gerados.

Proposição A.2.4. *Se $L|K$ é uma extensão separável de corpos com $\mathfrak{o}$ um domínio principal, então todo $\mathcal{O}$ -módulo M finitamente gerado e não nulo de L é um $\mathfrak{o}$ -módulo livre com posto igual a $[L : K]$.*

Demonstração: Ver ([14], cap. I, § 2). ■

A.3 Ramificação de ideais primos

Nesta seção, consideremos $\mathfrak{o}$ um domínio de Dedekind integralmente fechado em seu corpo de frações K , $L|K$ uma extensão finita e $\mathcal{O}$ o fêcho integral de $\mathfrak{o}$ em L .

Teorema A.3.1. *O anel $\mathcal{O}$ é um domínio de Dedekind.*

Demonstração: Ver ([14], Cap. I, § 8). ■

Assim, para todo ideal primo $\mathfrak{p}$ de $\mathfrak{o}$, tem-se que $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$. Logo, existe uma fatoração em ideais primos $\mathfrak{P}_i$ de $\mathcal{O}$ dada por

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r} . \quad (\text{A.1})$$

Neste caso, dizemos que os ideais $\mathfrak{P}_i$ que dividem $\mathfrak{p}\mathcal{O}$ estão *acima* de $\mathfrak{p}$ e que o ideal $\mathfrak{p}$ está *abaixo* dos $\mathfrak{P}_i$. O resultado abaixo justica tal terminologia.

Lema A.3.2. *Um ideal primo $\mathfrak{P}_i$ de $\mathcal{O}$ está acima de $\mathfrak{p}$ se, e somente se, $\mathfrak{P}_i \cap \mathfrak{o} = \mathfrak{p}$.*

Demonstração: Ver ([14], Cap. I, § 8). ■

Agora, sendo $\mathfrak{P}_i$ e $\mathfrak{p}$ ideais maximais, respectivamente, em $\mathcal{O}$ e $\mathfrak{o}$, segue que $\mathcal{O}/\mathfrak{P}_i$ e $\mathfrak{o}/\mathfrak{p}$ são corpos e do fato de $\mathcal{O}$ ser um $\mathfrak{o}$ -módulo finitamente gerado, segue

que $[\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}] < \infty$. Assim, dada uma fatoração de $\mathfrak{p}\mathcal{O}$ como dada em (A.1), chamamos os expoentes e_i de *índice de ramificação de $\mathfrak{P}_i$ sobre $\mathfrak{p}$* e $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}]$ de *grau de inércia de $\mathfrak{P}_i$ sobre $\mathfrak{p}$* . Tais números estão relacionados pelo seguinte resultado.

Teorema A.3.3. (Igualdade fundamental) *Se $L|K$ é extensão separável, então*

$$n = \sum_{i=1}^r e_i f_i .$$

Demonstração: Ver ([14], Cap. I, § 8). ■

Se $L|K$ é uma extensão separável, então $L = K(\theta)$, para algum $\theta \in L$. Definimos o condutor $\mathfrak{F}$ de $\mathfrak{o}[\theta]$ como sendo o maior ideal de $\mathcal{O}$ contido em $\mathfrak{o}[\theta]$, ou seja,

$$\mathfrak{F} = \{x \in \mathcal{O} ; x\mathcal{O} \subseteq \mathfrak{o}[\theta]\} .$$

Teorema A.3.4. *Se $\mathfrak{p}$ é um ideal primo de $\mathfrak{o}$ relativamente primo com $\mathfrak{F}$ e*

$$\bar{f}(x) = \bar{f}_1(x)^{e_1} \cdots \bar{f}_r(x)^{e_r}$$

é a fatoração do polinômio minimal f de θ sobre $\mathfrak{o}/\mathfrak{p}$ em polinômios irredutíveis $\bar{f}_i$ sobre $\mathfrak{o}/\mathfrak{p}$, então

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r} ,$$

onde

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + f_i(\theta)\mathcal{O} = (\mathfrak{p}, f_i(\theta))$$

são os ideais de $\mathcal{O}$ acima de $\mathfrak{p}$ com grau de inércia $f_i = \partial(\bar{f}_i)$, que é o grau do polinômio $\bar{f}_i$.

Demonstração: Ver ([14], Cap. I, § 8). ■

Um ideal primo $\mathfrak{P}_i$ de $\mathcal{O}$ na fatoração dada em (A.1) é dito *não-ramificado em K* se $e_i = 1$. Caso contrário, dizemos que $\mathfrak{P}_i$ é *ramificado em K* . Um ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ é dito ser *não-ramificado em L* , se todos os $\mathfrak{P}_i$ na fatoração dada em (A.1) são não-ramificados. Caso contrário, $\mathfrak{p}$ é dito ser *ramificado em L* . Se, ainda, $r = 1$ e $f = 1$, dizemos que $\mathfrak{p}$ é *totalmente ramificado em L* . A extensão $L|K$ é dita *não-ramificada* se todo ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ é não-ramificado em L . Caso exista algum ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ que seja ramificado (ou totalmente ramificado) em L , dizemos que a extensão $L|K$ é *ramificada* (ou *totalmente ramificada*). Dizemos que um ideal primo $\mathfrak{P}_i$ de $\mathcal{O}$ ramificado em K é *moderadamente ramificado em*

K , se $\text{mdc}(e_i, \text{car}(\mathfrak{o}/\mathfrak{p})) = 1$, onde $\text{car}(\mathfrak{o}/\mathfrak{p})$ é a característica do corpo $\mathfrak{o}/\mathfrak{p}$. Um ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ é dito *moderadamente ramificado* em L se todos os ideais primos acima de $\mathfrak{p}$ são moderadamente ramificados. Mais ainda, uma extensão $L|K$ é dita *moderadamente ramificada* se todos os ideais primos $\mathfrak{p}$ de $\mathfrak{o}$ são não-ramificados ou moderadamente ramificados.

A seguir, veremos exatamente quais ideais primos de $\mathfrak{o}$ que ramificam em L . Para isto, é necessário a noção de *ideal discriminante da extensão* $L|K$, denotado por $\mathfrak{d}_{L|K}$, como sendo o ideal gerado pelo discriminante $d(x_1, x_2, \dots, x_n)$, onde $\{x_1, x_2, \dots, x_n\}$ uma K -base de L .

Teorema A.3.5. *Um ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ ramifica em L se, e somente se, $\mathfrak{d}_{L|K} \subset \mathfrak{p}$, ou seja, $\mathfrak{p}$ divide $\mathfrak{d}_{L|K}$.*

Demonstração: Ver ([14], Cap. III, § 2). ■

É possível fazer uma caracterização semelhante para os ideais primos $\mathfrak{P}$ de $\mathcal{O}$ que ramificam em K . Para isto, definimos o *codiferente* de $L|K$ como sendo o ideal fracionário

$$\mathcal{D}_{L|K}^{-1} = \{x \in L ; \text{Tr}_{L|K}(x\mathcal{O}) \subseteq \mathfrak{o}\} .$$

O ideal fracionário inverso $\mathcal{D}_{L|K}$ de $\mathcal{D}_{L|K}^{-1}$ é chamado *diferente* de $L|K$. Observemos que numa torre de extensão $F \subset K \subset L$, o diferente satisfaz

$$\mathcal{D}_{L|F} = \mathcal{D}_{L|K}(\mathcal{D}_{K|F}\mathcal{O}) .$$

O ideal inteiro $\mathcal{D}_{L|K} \subset \mathcal{O}$ de L caracteriza a ramificação dos ideais primos de $\mathcal{O}$ conforme o seguinte teorema.

Teorema A.3.6. *Um ideal $\mathfrak{P}$ de $\mathcal{O}_L$ ramifica em L se, e somente se, $\mathcal{D}_{L|K} \subset \mathfrak{P}$, ou seja, $\mathfrak{P}$ divide $\mathcal{D}_{L|K}$. Mais ainda, se $\mathfrak{P}$ é moderadamente ramificado, então a maior potência de $\mathfrak{P}$ que divide $\mathcal{D}_{L|K}$ é $\mathfrak{P}^{e-1}$.*

Demonstração: Ver ([14], Cap. III, § 2). ■

Proposição A.3.7. [1] *Seja $L|K$ uma extensão com $[L : K] = 2$. Se 2 não ramifica em $L|K$, então $L|K$ é moderadamente ramificada.*

Proposição A.3.8. *Se $L|K$ é uma extensão moderadamente ramificada, então a restrição do traço $\text{Tr}_{L|K} : \mathcal{O} \longrightarrow \mathfrak{o}$ é sobrejetora.*

Demonstração: Ver ([13], Cap. IV, § 2). ■

A.4 Ramificação em extensões de Galois

Nesta seção, consideremos o caso particular em que $\mathfrak{o}$ é um domínio de Dedekind integralmente fechado com corpo de frações K , $L|K$ é uma extensão de Galois, $\mathcal{O}$ o fecho inteiro de $\mathfrak{o}$ em L e $G = \text{Gal}(L, K)$ como sendo o grupo de Galois da extensão $L|K$. Assim, se $b \in \mathcal{O}$, então $\sigma(b) \in \mathcal{O}$, para todo $\sigma \in G$ e, com isso, o grupo de Galois G age em $\mathcal{O}$. Com isso, se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}$ acima de $\mathfrak{p}$, então $\sigma(\mathfrak{P})$ também está acima de $\mathfrak{p}$ já que

$$\sigma(\mathfrak{P}) \cap \mathfrak{o} = \sigma(\mathfrak{P} \cap \mathfrak{o}) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

Os ideais $\sigma(\mathfrak{P})$, para $\sigma \in G$, são ditos conjugados de ideais primos conjugados de $\mathfrak{P}$.

Proposição A.4.1. *O grupo de Galois G age transitivamente sobre o conjunto de ideais primos de $\mathcal{O}$ que estão acima de $\mathfrak{p}$, ou seja, os primos acima de $\mathfrak{p}$ são todos conjugados um do outro.*

Demonstração: Ver ([14], Cap. I, § 9). ■

Seja $\mathfrak{P}$ um ideal de $\mathcal{O}$. Definimos o grupo de decomposição de $\mathfrak{P}$ por

$$G_{\mathfrak{P}} = \{\sigma \in G ; \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Tal grupo tem papel fundamental na decomposição de ideal primos.

Teorema A.4.2. *A decomposição de um ideal primo $\mathfrak{p}$ de $\mathfrak{o}$ é da forma*

$$\mathfrak{p}\mathcal{O} = \left(\prod_{\sigma} \sigma(\mathfrak{P}) \right)^e,$$

onde σ varia em $G/G_{\mathfrak{P}}$. Além disso, os índices de ramificação e graus de inércia independem de i na fatoração dada em (A.1) e são todos iguais, respectivamente, e e f . Vale ainda que $n = efr$.

Demonstração: Ver ([14], Cap. I, § 9). ■

O resultado a seguir, diz respeito ao gerador do grupo de decomposição de um ideal que não ramifica em K .

Teorema A.4.3. *Se $\mathfrak{P}$ é um ideal de $\mathcal{O}$ que não ramifica em K , então existe $\sigma_{\mathfrak{P}} \in G$ tal que para todo $a \in \mathcal{O}$ tem-se que*

$$\sigma_{\mathfrak{P}}(a) \equiv a^q \pmod{\mathfrak{P}},$$

onde $q = [\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p}]$. Além disso, $G_{\mathfrak{P}}$ é cíclico de ordem f com $\sigma_{\mathfrak{P}}$ um gerador. O automorfismo $\sigma_{\mathfrak{P}}$ é dito elemento de Frobenius.

Demonstração: Ver ([14], Cap. I, § 9). ■

A.5 Corpos de números e seus anéis de inteiros

Consideremos, nesta seção, K um corpo de números, ou seja, uma extensão $K|\mathbb{Q}$ finita. Com isso, sendo $\mathbb{Z}$ um anel integralmente fechado em seu corpo de frações $\mathbb{Q}$, consideremos o fêcho inteiro $\mathcal{O}_K$ de $\mathbb{Z}$ em K , chamado *anel de inteiros de K* . Desde que $\mathbb{Z}$ é um domínio de Dedekind ($\mathbb{Z}$ é domínio principal), segue, pelo Teorema A.3.1, que $\mathcal{O}_K$ é um domínio de Dedekind. Desse modo, pelo Corolário A.1.3, segue que todo ideal fracionário $\mathfrak{a}$ de K possui uma fatoração

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}} ,$$

em ideais primos $\mathfrak{p}$ de $\mathcal{O}$ com $\nu_{\mathfrak{p}} \in \mathbb{Z}$ e $\nu_{\mathfrak{p}} = 0$ para quase todo $\mathfrak{p}$.

Agora, com base na Proposição A.2.4, todo ideal fracionário $\mathfrak{a} \neq 0$ admite uma $\mathbb{Z}$ -base $\{x_1, x_2, \dots, x_n\}$ com $n = [K : \mathbb{Q}]$ sendo o grau do corpo de números. O discriminante de tais bases são invariantes do ideal fracionário $\mathfrak{a}$ e por isso denotamos por

$$d(\mathfrak{a}) = d(x_1, \dots, x_n) ,$$

uma vez que duas bases são combinações inteiras uma das outras de modo que o determinante da matriz de mudança de base entre elas seja ± 1 . No caso particular onde $\mathfrak{a} = \mathcal{O}_K$, chamamos o discriminante de uma $\mathbb{Z}$ -base de $\mathcal{O}_K$ de o *discriminante do corpo de números K* , denotado por d_K .

Outro fato importante a considerar é que, conforme o Teorema A.3.5, um ideal primo de $\mathbb{Z}$ (e portanto um número primo p) ramifica em K se, e somente se, divide $\mathfrak{d}_{K|\mathbb{Q}}$, que é gerado pelos discriminantes das $\mathbb{Q}$ -bases de K . No entanto, tais discriminantes são invariantes de K e, portanto, $\mathfrak{d}_{K|\mathbb{Q}}$ é um ideal principal gerado por d_K . Com isso, um número primo p ramifica em K se, e somente se, $p \mid d_K$.

Consideremos agora, $\mathfrak{a}$ e $\mathfrak{b}$ ideais fracionários de K com suas respectivas $\mathbb{Z}$ -bases $\mathcal{B}_{\mathfrak{a}}$ e $\mathcal{B}_{\mathfrak{b}}$. Definimos o *invariante relativo*² de $\mathfrak{a}$ e $\mathfrak{b}$ por

$$\chi(\mathfrak{a}, \mathfrak{b}) = |\det(M_{\mathcal{B}_{\mathfrak{b}}, \mathcal{B}_{\mathfrak{a}}})| ,$$

²Note a semelhança com a Definição 1.4.9.

onde $M_{\mathcal{B}_b, \mathcal{B}_a} \in \text{GL}_n(\mathbb{Q})$ é a matriz de mudança de base de $\mathcal{B}_b$ para $\mathcal{B}_a$. Note que este invariante satisfaz

- $\chi(\mathfrak{a}, \mathfrak{b}) \in \mathbb{Q}_+^\times$;
- $\chi(\mathfrak{a}, \mathfrak{b}) = \chi(\mathfrak{b}, \mathfrak{a})^{-1}$;
- $\chi(\mathfrak{a}, \mathfrak{c}) = \chi(\mathfrak{a}, \mathfrak{b})\chi(\mathfrak{b}, \mathfrak{c})$;
- se $\mathfrak{b} \subseteq \mathfrak{a}$, então $\chi(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a} : \mathfrak{b})$, onde $(\mathfrak{a} : \mathfrak{b})$ denota o índice de grupos de $\mathfrak{b}$ em $\mathfrak{a}$.

Assim, definimos a *norma do ideal fracionário* $\mathfrak{a}$ de K por

$$N(\mathfrak{a}) = \chi(\mathcal{O}_K, \mathfrak{a}) .$$

Observe que quando $\mathfrak{a}$ é um ideal inteiro, tem-se que $N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$. Observamos que tal definição estende a noção de norma de um elemento uma vez que dado $\alpha \in \mathcal{O}_K$, o ideal principal $(\alpha) = \alpha\mathcal{O}_K$, possui norma $N((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$. Além disso, tem-se o seguinte resultado.

Proposição A.5.1. *Se $\mathfrak{a}$ é um ideal inteiro de K e $a \in \mathbb{K}$, então*

$$N(\lambda\mathfrak{a}) = |N_{K|\mathbb{Q}}(a)|N(\mathfrak{a}) .$$

Demonstração: Ver ([14], Cap. I, § 6). ■

Proposição A.5.2. *Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais fracionários de K , então*

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}) .$$

Demonstração: Ver ([14], Cap. I, § 6). ■

Proposição A.5.3. *Se K é um corpo de números K , então*

$$N(\mathcal{D}_{K|\mathbb{Q}}) = |d_K| .$$

Demonstração: Ver ([14], Cap. III, § 2). ■

A.6 Corpos ciclotômicos

Dizemos que um elemento $\zeta \in \mathbb{C}$ é uma raiz m -ésima da unidade se $\zeta^m = 1$ com $\zeta \neq 1$ e m um inteiro positivo. Uma raiz m -ésima da unidade é dita ser *primitiva*, se $\zeta^d \neq 1$, para todo $0 < d < m$. As raízes m -ésimas da unidade são da forma $e^{2\pi ii/m}$, para $0 \leq i \leq m$. Para F um corpo de números, a extensão $K = F(\zeta_m)$ para ζ_m uma raiz m -ésima primitiva da unidade, é dita ser a m -ésima extensão ciclotômica de F . No caso específico onde $K = \mathbb{Q}(\zeta_m)$, para alguma raiz m -ésima primitiva da unidade de $\mathbb{C}$, K é chamado o m -ésimo corpo ciclotômico. Com base nas noções e resultados das seções anteriores, tem-se os seguintes resultados.

Teorema A.6.1. *Se ζ é uma raiz p^r -ésima primitiva da unidade e $K = \mathbb{Q}(\zeta)$, então:*

- (a) *O grau de K sobre $\mathbb{Q}$ é $\phi(p^r) = p^{r-1}(p-1)$.*
- (b) *O anel de inteiros de K é $\mathbb{Z}[\zeta]$.*
- (c) *O elemento $\pi = 1 - \zeta$ é um primo de $\mathcal{O}_K$ satisfazendo $p\mathcal{O}_K = \mathfrak{p}^{\phi(p^r)}$, onde $\mathfrak{p} = \pi\mathcal{O}_K$.*
- (d) *$|d_K| = p^a$, onde $a = p^{r-1}(pr - r - 1)$ e, portanto, p é o único primo que ramifica em $\mathcal{O}_K$. Além disso, $\mathcal{D}_{K|\mathbb{Q}} = \mathfrak{p}^a$.*
- (e) *O subcorpo maximal real $F = K \cap \mathbb{R}$ é $F = \mathbb{Q}(\zeta + \zeta^{-1})$ e possui anel de inteiros dado por $\mathcal{O}_F = \mathbb{Z}[\zeta + \zeta^{-1}]$. Além disso, o ideal primo acima de p é o único que ramifica em $K|F$.*

Demonstração: Ver ([20], Cap. 2). ■

Teorema A.6.2. *Se ζ é uma raiz m -ésima primitiva da unidade e $K = \mathbb{Q}(\zeta)$, então:*

- (a) *O grau de K sobre $\mathbb{Q}$ é $\phi(m)$.*
- (b) *O anel de inteiros de K é $\mathbb{Z}[\zeta]$.*
- (c) *Um primo p ramifica em K se, e somente se, $p \mid m$. Mais ainda, se $m = p^r m'$, com $\text{mdc}(p, m') = 1$, então*

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_{s_p})^{\phi(p^r)}$$

em $\mathcal{O}_K$, com $\mathfrak{p}_i$ ideais primos distintos de $\mathcal{O}_K$ e com grau de inércia dado por

$$f_p = \min\{f' \in \mathbb{N} ; p^{f'} \equiv 1 \pmod{m'}\}.$$

Além disso, tem-se que $s_p = \phi(m')/f_p$.

- (d) *O discriminante de K é*

$$d_K = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

(e) O subcorpo maximal real $F = K \cap \mathbb{R}$ é $F = \mathbb{Q}(\zeta + \zeta^{-1})$ e possui anel de inteiros dado por $\mathcal{O}_F = \mathbb{Z}[\zeta + \zeta^{-1}]$. Além disso, a extensão $K|F$ é não-ramificada.

Demonstração: Ver ([20], Cap. 2). ■