Raffaela Raposo Palmieri

Diagonalização Da Forma Traço Sobre Alguns Anéis De Inteiros

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

Diagonalização Da Forma Traço Sobre Alguns Anéis De Inteiros

Raffaela Raposo Palmieri

Orientador: Prof. Dr. Clotilzio Moreira dos Santos

Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

São José do Rio Preto - SP
Março - 2005

Palmieri, Raffaela Raposo .
Diagonalização da forma traço sobre alguns anéis de inteiros / Raffaela Raposo Palmieri– São José do Rio Preto : [s.n.], 2005
46 f. ; 30 cm.

Orientador: Clotilzio Moreira dos Santos
Dissertação (mestrado) – Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas

1. Álgebra. 2. Forma quadrática . 3. Forma traço. 4. Corpos de números quadráticos. 5. Base integral ortogonal. 6. Anéis de inteiros. 7. I. Santos, Clotilzio Moreira dos. II. Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU – 511.23

À minha mãe,

Silvania,

e à minha irmã,

Manuela,

dedico.

Agradecimentos

Ao concluir este trabalho deixo aqui meus agradecimentos:

A Deus, pela saúde e por permitir a realização de mais um sonho.

À minha mãe e à minha irmã pela força, perseverança, união e pelo imenso amor.

Aos professores do Departamento de Matemática da FCT - UNESP (Câmpus de Presidente Prudente) pela amizade e pelo conhecimento transmitido. Especialmente ao Prof. Dr. José Roberto Nogueira pela credibilidade e amizade durante a graduação e principalmente durante o projeto de Iniciação Científica.

À banca examinadora.

Ao Prof. Dr. Clotílzio Moreira dos Santos pela paciência, amizade e valiosa orientação.

À amiga Janete do Prado pelo apoio e amizade.

À Dona Amélia, Sr. Pedro e às amigas do pensionato pela nova família.

Aos professores do Departamento de Matemática do IBILCE - UNESP pelo conhecimento transmitido.

À CAPES pelo apoio financeiro.

Resumo

Neste trabalho estamos interessados no problema da forma traço sobre corpos de números. Estudamos quando a forma traço pode ser diagonalizada, isto é, quando no anel de inteiros de um corpo de números quadrático existe uma base integral ortogonal com respeito ao traço. Também são dados exemplos de corpos de grau maior com a mesma propriedade.

Palavras-Chaves: Forma Traço, Corpos Quadráticos, Base Integral Ortogonal.

Abstract

In this work we are concerned with the problem of the study the trace form in the number fields. We study when the form trace can be diagonalized, i.e., when on the ring of integers of a quadratic number field there is an integral basis orthogonal with respect to the trace form. There are also given examples of fields of higher degree with the same property.

Keywords: Trace Form, Quadratic Fields, Orthogonal Integral Basis.

Índice de Símbolos

$\mathbb{Z}$: o conjunto do números inteiros

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

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

∂p : grau do polinômio p.

K : corpo de números

$[\mathrm{K} : \mathbb{Q}]$: grau de K sobre $\mathbb{Q}$

$Tr_{\mathrm{K}/\mathbb{Q}}$: traço em relação à extensão $\mathrm{K}/\mathbb{Q}$

$\mathbb{Q}(\sqrt{d})$: corpo quadrático

$\prod$: produtório

$\sum$: somatório

$N(\beta)$: norma de β

$Tr(\beta)$: traço de β

$\mathcal{D}_{\mathrm{K}}$: anel dos inteiros algébricos do corpo de números K

$\rho(\mathcal{D})$: posto de $\mathcal{D}$

(a_{ij}) : matriz

$det(a_{ij})$: determinante de (a_{ij})

$Adj(M)$: adjunta da matriz M

M^{-1} : inversa de M

M_{ST} : matriz de mudança da base S para a base T

δ_{ik} : delta de Kronecker

$\Delta[S]$ ou $\Delta[e_1, \ldots, e_n]$: discriminante da base $S = \{e_1, \ldots, e_n\}$

$\Delta(\mathrm{K})$: discriminante de qualquer base integral de K

$\mathcal{D}^*$: grupo das unidades de K

$\{\sigma_1, \ldots, \sigma_n\}$: conjunto dos n monomorfismos de K em $\mathbb{C}$

W : grupo cíclico finito constituído das raízes da unidade contidas em K

$\overline{x}$: conjugado complexo do elemento x

$(\mathcal{D}, b)$: um espaço bilinear

$\{\beta_1, \beta_2\}$: uma $\mathbb{Z}$-base

ε : a unidade fundamental do anel de inteiros $\mathcal{D}$ de um corpo quadrático

$N\varepsilon$: norma da unidade fundamental

$\left(\frac{p}{q}\right) = 1$: p é um resíduo quadrático módulo q

Sumário

Introdução

O Capítulo 1 contém resultados básicos da Teoria Algébrica dos Números que servem de suporte para o Capítulo 2. Nele introduziremos conceitos importantes da Teoria Algébrica dos Números, tais como elementos algébricos sobre um corpo, corpo de números quadráticos e alguns de seus principais parâmetros, como: Anel dos Inteiros Algébricos, Discriminante, Base Integral, Norma e Traço de um elemento.

Demonstraremos o Teorema de Dirichlet para corpos quadráticos a menos de alguns resultados fortes sobre números, cuja demonstração é necessária à teoria analítica, obtendo assim resultados importantes sobre o grupo das unidades do anel de inteiros de um corpo quadrático. Finalizaremos o capítulo com o conceito de unidade fundamental (um gerador da parte livre do grupo das unidades) que tem papel central no Capítulo Dois em se tratando da existência de uma base integral ortogonal, ou seja, na diagonalização da forma traço.

O objetivo do Capítulo 2 e da dissertação é demonstrar para quais valores inteiros d não nulo e livre de quadrados existe uma base integral ortogonal para o anel de inteiros de um corpo de números quadrático $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ segundo as formas traços usuais $\mathcal{D} \times \mathcal{D} \longrightarrow \mathbb{Z}$ definidas por $(x, y) \longmapsto tr_{\mathrm{K}/\mathbb{Q}}(xy)$ e $tr_{\mathrm{K}/\mathbb{Q}}(x\overline{y})$. Em resumo, teremos os seguintes resultados:

Com relação à forma traço $tr_{\mathrm{K}/\mathbb{Q}}(xy)$, para $d \equiv 2, 3 (mod\ 4)$, temos que $\{1, \sqrt{d}\}$ é uma base integral ortogonal. Para o caso $d \equiv 1 (mod\ 4)$ não existe uma base integral ortogonal, se $d > 1$. Agora para $d < 0$ existe uma base

integral ortogonal se, e somente se, u é par, onde $\epsilon = u+v\sqrt{-d}$ é a unidade fundamental do corpo $\mathbb{Q}(\sqrt{-d})$ (Teorema 2.7). Em particular, o corpo $\mathbb{Q}(\sqrt{-p})$, onde $p \equiv 3(mod\ 4)$ é um número primo, tem uma base integral ortogonal.

Sejam p, q números primos positivos com $pq \equiv 3(mod\ 4)$. Então em $\mathbb{Q}(\sqrt{-pq})$ existe uma base integral ortogonal se, e somente se, p não é um resíduo quadrático módulo q. Para casos bem particulares de corpos quárticos provamos que existem bases integrais ortogonais. Finalizamos a dissertação exibindo vários exemplos.

Capítulo 1

Unidades em Anéis de Corpos Quadráticos

Neste capítulo introduzimos os conceitos de elemento algébrico, corpos de números, corpo quadrático, norma e traço de um elemento, inteiro algébrico, anel dos inteiros algébricos, base integral. Mostraremos que a partir de uma base integral de um dado corpo quadrático calculamos o seu discriminante (Teorema 1.8). Finalizaremos o capítulo demonstrando o Teorema de Dirichlet para corpos quadráticos, e provamos que o grupo das unidades do anel de inteiros possui um único gerador maior que 1 quando o corpo quadrático é real, (Teorema 1.17).

1.1 Norma, Traço e Bases Integrais

Um número complexo α é dito *número algébrico* se ele é raiz de um polinômio não nulo com coeficientes em $\mathbb{Q}$. Em todo o texto K será um *corpo de números*, isto é, uma extensão finita de $\mathbb{Q}$ contida em $\mathbb{C}$. Pelo Teorema do Elemento Primitivo tem-se que $K = \mathbb{Q}(\theta)$, onde θ é um número algébrico. Neste caso, se $p(X)$ é o polinômio minimal (= polinômio irredutível) de θ sobre $\mathbb{Q}$ então o grau

de $p(X)$ é igual ao grau da extensão $\mathrm{K} \supseteq \mathbb{Q}$. Em símbolos: $\partial p(X) = [\mathrm{K} : \mathbb{Q}]$.

Um *corpo quadrático* é uma extensão $\mathrm{K} \supseteq \mathbb{Q}$ de grau 2. É imediata a demonstração de que todo corpo quadrático é uma *extensão radical*, ou seja, é da forma $\mathbb{Q}(\sqrt{d})$, para algum $d \in \mathbb{Z}$ *livre de quadrados*. Um número inteiro racional não nulo $d \neq 1$ é dito *livre de quadrados* se qualquer que seja o número primo $p \in \mathbb{Z}$, p^2 não é um fator de d.

Um corpo quadrático $\mathbb{Q}(\sqrt{d})$ é dito *real* se $d > 0$, isto é, $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ e se $d < 0$, $\mathbb{Q}(\sqrt{d})$ é dito *imaginário*.

Seja $\mathrm{K} = \mathbb{Q}(\theta)$ um corpo de número de grau n. Então existem exatamente n monomorfismos $\sigma_i : \mathrm{K} \longrightarrow \mathbb{C}$. Os elementos $\sigma_i(\theta) = \theta_i$ são exatamente as raízes do polinômio minimal de θ sobre $\mathbb{Q}$. Para um elemento qualquer $\beta \in \mathrm{K}$ definimos a *Norma* e o *Traço* de β, respectivamente, por:

$$N(\beta) = \prod_{i=1}^{n} \sigma_i(\beta),$$

$$Tr(\beta) = \sum_{i=1}^{n} \sigma_i(\beta).$$

Para todo $\beta \in \mathrm{K}$ tem-se que $N(\beta)$ e $Tr(\beta)$ são números racionais. Além disso $N : \mathrm{K} \to \mathbb{Q}$ é uma funçaõ multiplicativa e $Tr : \mathrm{K} \to \mathbb{Q}$ é uma função $\mathbb{Q}$-linear.

No caso em que $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados os monomorfismos de K em $\mathbb{C}$ são a identidade e a conjugação dada por $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$, onde $a,\ b \in \mathbb{Q}$. Assim $N(a + b\sqrt{d}) = a^2 - db^2$ e $Tr(a + b\sqrt{d}) = 2a$.

Um número complexo α é dito *inteiro algébrico* se ele é raiz de um polinômio mônico não nulo com coeficientes em $\mathbb{Z}$. Seja K um corpo de números e $\mathcal{D}_{\mathrm{K}}$ o conjunto de todos os inteiros algébricos de K. Então $\mathcal{D}_{\mathrm{K}}$ é um anel, dito *anel de inteiros de* K. Quando não houver possibilidade de confusão escreveremos apenas $\mathcal{D}$ para o anel de inteiros de um corpo de números K.

Como $\mathcal{D} \subseteq \mathbb{C}$ é claro que $\mathcal{D}$ é um grupo abeliano, logo um $\mathbb{Z}$-módulo. É possível demonstrar que $\mathcal{D}$ é um $\mathbb{Z}$-módulo de *posto* finito (denotamos *posto*

de $\mathcal{D}$ por $\rho(\mathcal{D})$) e $\rho(\mathcal{D}) = [K : \mathbb{Q}]$.

Definição 1.1. Seja $\mathcal{D}$ o anel de inteiros de um corpo de números. Uma $\mathbb{Z}$-base de $\mathcal{D}$ é dita uma *base integral.*

Observação 1.2. Desde que o $\rho(\mathcal{D})$ é igual a $[K : \mathbb{Q}]$ toda base integral é uma $\mathbb{Q}$-base para K.

Uma matriz quadrada de ordem n com entradas $a_{ij} \in \mathbb{Z}$ é dita *unimodular* se ela é inversível no anel das matrizes quadradas de ordem n com entradas inteiras racionais, equivalentemente, se seu determinante é 1 ou -1. Com isto podemos enunciar o seguinte teorema.

Teorema 1.3. [ST] Sejam $\mathcal{D}$ o anel de inteiros de um corpo de números K, com base $\{e_1, \ldots, e_n\}$ e $a_{ij} \in \mathbb{Z}$, $i, j = 1, \ldots, n$. Então $\{c_i = \sum_{j=1}^{n} a_{ij}e_j$, $i = 1, 2, \ldots, n\}$ é base de $\mathcal{D}$ se, e somente se, a matriz $M = (a_{ij})$ é unimodular.

Demonstração:

Suponhamos que $\{c_1, \ldots, c_n\}$ é uma $\mathbb{Z}$ base de $\mathcal{D}$ e seja $e_j = \sum_{k=1}^{n} b_{jk}c_k$, com $b_{jk} \in \mathbb{Z}$. Substituindo os valores de e_j temos:
$c_i = \sum_{j=1}^{n} a_{ij}e_j = \sum_{j=1}^{n} a_{ij}(\sum_{k=1}^{n} b_{jk}c_k) = \sum_{j=1}^{n}(\sum_{k=1}^{n} a_{ij}b_{jk}c_k) = \sum_{k=1}^{n}(\sum_{j=1}^{n} a_{ij}b_{jk})c_k$. Isto implica que

$$(\sum_{j=1}^{n} a_{ij}b_{jk}) = (\delta_{ik}),$$

onde δ_{ik} é o delta de Kronecker. Logo $(a_{ij})(b_{jk}) = I_n$. Calculando o determinante temos que $det(a_{ij}).det(b_{jk}) = 1$. Como os determinantes destas matrizes são números inteiros racionais temos que $det(a_{ij}) = det(b_{jk}) = \pm 1$.

Reciprocamente, se a matriz M é unimodular, desde que $M^{-1} := \frac{Adj(M)}{det(M)} = \pm(Adj(M))$, temos que M^{-1} é uma matriz com entradas inteiras racionais. Denote por N^t a matriz transposta da matriz N. Multiplicando

$$(c_1 \cdots c_n)^t = M.(e_1 \cdots e_n)^t$$

à esquerda por M^{-1} temos

$$M^{-1}(c_1 \cdots c_n)^t = M^{-1}M(e_1 \ldots e_n)^t = (e_1 \ldots e_n)^t.$$

Seja $M^{-1} := (b_{ij})$. Da igualdade acima podemos escrever $e_i = \sum_{j=1}^{n} b_{ij}c_j$. Disto segue que $c_1, \ldots, c_n$ geram $\mathcal{D}$ (pois $\{e_i, i = 1, \ldots, n\}$ gera $\mathcal{D}$), e como $detM$ é não nulo, $\{c_1, \ldots, c_n\}$ também é linearmente independente. Logo uma base para $\mathcal{D}$. □

Já temos definido a norma e o traço de elementos de um corpo de números K e sabemos que para cada elemento de K seu traço e sua norma são números racionais. Agora consideremos novamente $K = \mathbb{Q}(\theta)$ um corpo de números de grau n e $S = \{e_1, \ldots, e_n\}$ uma base de K como $\mathbb{Q}$ espaço vetorial. Considere também $\sigma_i : K \to \mathbb{C}$ os n monomorfismos de K em $\mathbb{C}$. O *discriminante da base* S é denotado por $\Delta[S]$ ou $\Delta[e_1, \ldots, e_n]$ e é definido por

$$\Delta[S] := det(\sigma_i(e_j))^2.$$

Se escolhermos outra $\mathbb{Q}$-base T para K temos que

$$\Delta[T] = det(M_{ST})^2\Delta[S],$$

onde M_{ST} é a matriz de mudança da base S para a base T.

Pode-se demonstrar (Veja Teorema 2.6 de [ST]) que o discriminante de uma base é um número racional não nulo. Portanto pela igualdade acima o discriminante de duas bases diferem por um fator racional quadrático. Quando as bases são integrais seus discriminantes são números inteiros racionais bem definidos como mostra o teorema seguinte. Para a sua demonstração vamos precisar do seguinte lema devido a Gauss.

Lema 1.4. [ST] Seja $p(X)$ um polinômio com coeficientes inteiros e suponhamos que $p(X) = g(X).h(X)$, $g(X)$, $h(X) \in \mathbb{Q}[X]$. Então existe $\lambda \in \mathbb{Q}$, $\lambda \neq 0$ tal que $\lambda g(X)$, $\lambda^{-1}h(X) \in \mathbb{Z}[X]$.

Demonstração:

Ver [ST, Lemma 1.4]. □

Teorema 1.5. [ST] Sejam K $= \mathbb{Q}(\theta)$ um corpo de números de grau n e $S = \{e_1, \ldots, e_n\}$ uma base integral de K. Se $T = \{c_1, \ldots, c_n\}$ é outra base integral de K então $\Delta[T] = \Delta[S] \in \mathbb{Z}$.

Demonstração:

Considere $M_{ST} = (a_{ij})$ a matriz de mudança de base, da base S para a base T. Como vimos acima temos que $\Delta[T] = (det(a_{ij}))^2.\Delta[S]$. Por outro lado como T é uma $\mathbb{Z}$ base para $\mathcal{D}$ temos que $a_{ij} \in \mathbb{Z}$ para todos $i,\ j = 1, \ldots, n$. Assim pelo Teorema 1.3 $det(a_{ij}) = \pm 1$. Logo $\Delta[T] = (\pm 1)^2.\Delta[S] = \Delta[S]$. Resta demonstrar que $\Delta[S]$ é um número inteiro racional. Já sabemos que $\Delta[S]$ é um número racional não nulo. Como cada e_j é um inteiro algébrico e $\sigma_i(e_j)$ é raiz do mesmo polinômio minimal de e_j então cada entrada da matriz $(\sigma_i(e_j))$ é um inteiro algébrico. Logo $\Delta[S]$ é um inteiro algébrico. Ou seja $\Delta[S] \in \mathcal{D} \cap \mathbb{Q}$. Portanto o polinômio minimal de $\Delta[S]$ sobre $\mathbb{Q}$ é $g(X) = X - \Delta[S]$. Mas como $\Delta[S]$ é raiz de um polinômio mônico $p(X)$ com coeficientes em $\mathbb{Z}$, temos que $g(X)$ divide $p(X)$ em $\mathbb{Q}[X]$. Logo existe $h(X) \in \mathbb{Q}[X]$ tal que $p(X) = g(X).h(X)$. Pelo Lema 1.4 existe $\lambda \in \mathbb{Q} - \{0\}$ tal que $p(X) = (\lambda g(X))(\lambda^{-1}h(X))$, com $\lambda g(X),\ \lambda^{-1}h(X) \in \mathbb{Z}[X]$. Assim $\lambda g(X)$ divide $p(X)$ em $\mathbb{Z}[X]$. Como $p(X)$ é mônico $\lambda = 1$ (ou -1). Logo $g(X) = X - \Delta[S] \in \mathbb{Z}[X]$, ou seja $\Delta[S] \in \mathbb{Z}$. □

Como o discriminante de duas bases integrais quaisquer são iguais ele é um invariante do corpo de números K podemos definir o seguinte

Definição 1.6. Seja K um corpo de números. O *discriminante de* K será denotado por δ(K) e é definido como sendo o discriminante de qualquer base integral de K.

Vamos fechar esta subseção calculando uma base integral para cada corpo quadrático e a partir dela o discriminante do respectivo corpo quadrático.

Teorema 1.7. [ST] Seja $d \in \mathbb{Z}$ livre de quadrados. Então o anel de inteiros de $K = \mathbb{Q}(\sqrt{d})$ é:

1. $\mathbb{Z}[\sqrt{d}]$, se $d \equiv 2, 3 (mod\ 4)$;
2. $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$, se $d \equiv 1 (mod\ 4)$.

Demonstração:

Todo elemento $\alpha \in \mathbb{Q}(\sqrt{d})$ é da forma $\alpha = r + s\sqrt{d}; r, s \in \mathbb{Q}$. Assim podemos escrever $\alpha = \dfrac{a + b\sqrt{d}}{c}, a, b, c \in \mathbb{Z}, c > 0$ e a, b e c relativamente primos, isto é, nenhum primo divide a, b e c ao mesmo tempo.

Agora, α é um inteiro algébrico se, e somente se, os coeficientes do polinômio minimal $\left(t - (\dfrac{a + b\sqrt{d}}{c})\right)\left(t - (\dfrac{a - b\sqrt{d}}{c})\right)$ são inteiros racionais. Assim se $\alpha \in \mathcal{D}$ então

$$N(\alpha) = \frac{a^2 - db^2}{c^2} \in \mathbb{Z} \qquad (1)$$

Logo $\dfrac{a^2 - db^2}{c^2} = m \in \mathbb{Z}$ e então

$$a^2 - c^2 m = b^2 d \qquad (1')$$

e

$$T(\alpha) = \frac{2a}{c} \in \mathbb{Z} \qquad (2)$$

(i) Se p é um primo tal que $p|a$ e $p|c$ então $p^2|a^2$ e $p^2|c^2$. Como d é livre de quadrados por (1') implica que $p|b^2$ e como p é primo $p|b$ (absurdo pois a, b e c são relativamente primos). Logo a e c são relativamente primos e de (2) temos que $c = 1$ ou $c = 2$.

• Se $c = 1$ então $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ e neste caso $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{D}_K$.

• Se $c = 2$, vejamos que $\dfrac{a + b\sqrt{d}}{2}$ é um inteiro $\iff a, b$ são ímpares e $d \equiv 1 (mod\ 4)$. De fato, por (1) a tem que ser ímpar. E se $b = 2r$ par segue de (1') que $2|a^2$. Logo $2|a$, absurdo. Portanto a e b são ímpares. Sejam $a = 2s + 1$, $b = 2r + 1; r, s \in \mathbb{Z}$ e provemos que $d \equiv 1 (mod\ 4)$. Substituindo os valores

de a e b em (1) encontramos $N(\alpha) = \dfrac{(2s+1)^2 - d(2r+1)^2}{4} = m \in \mathbb{Z}$. Assim $4(s^2+s)+1-d(4(r^2+r)+1) = 4m \equiv 0(mod\ 4)$, o que nos dá $d \equiv 1(mod\ 4)$.

Reciprocamente se $d \equiv 1(mod\ 4)$, então $\alpha = \dfrac{a+b\sqrt{d}}{2}$ com a, b ímpares também é inteiro pois é raiz do polinômio mônico $x^2 - ax + \dfrac{a^2-db^2}{4} \in \mathbb{Z}[X]$. Se $a = 2s+1, b = 2r+1$ então $\alpha = (s+r).1+1.(\frac{1}{2}+\frac{1}{2}\sqrt{d}) \in \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right] \subseteq \mathcal{D}$. Logo $\mathcal{D} = \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$ se, e somente se, $d \equiv 1(mod\ 4)$, e se $d \equiv 2, 3(mod\ 4)$ então $\mathcal{D} = \mathbb{Z}[\sqrt{d}]$. □

Teorema 1.8. [ST] Seja $K = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ livre de quadrados. Então:

(1). Se $d \not\equiv 1(mod\ 4)$ então $\beta = \{1, \sqrt{d}\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$ e $\delta(K) = 4d$.

(2). Se $d \equiv 1(mod\ 4)$ então $\gamma = \left\{1, \frac{1}{2}+\frac{1}{2}\sqrt{d}\right\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$ e $\delta(K) = d$.

Demonstração:

(1) Pelo Teorema 1.7 segue que $\beta = \{1, \sqrt{d}\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$. Logo

$$\delta(K) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

(2) Pelo Teorema 1.7 segue que $\gamma = \{1, \frac{1}{2}+\frac{1}{2}\sqrt{d}\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$. Portanto

$$\delta(K) = \begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d})^2 = d.$$

□

1.2 Unidades fundamentais

Seja $\mathcal{D}$ o anel de inteiros de um corpo de número K. Um elemento $x \in \mathcal{D}$ é chamado de uma *unidade* se existe $x' \in \mathcal{D}$ tal que $xx' = 1$. O conjunto de todas unidades de $\mathcal{D}$ é um grupo multiplicativo e usualmente é denotado por $\mathcal{D}^*$. Também se diz que $\mathcal{D}^*$ é o grupo das unidades de K.

Sejam $K = \mathbb{Q}(\theta)$ um corpo de número de grau n, onde θ é um inteiro algébrico e $\{\sigma_1, \ldots, \sigma_n\}$ o conjunto de todos os monomorfismos de K em $\mathbb{C}$. Se $\sigma_i(K) \subseteq \mathbb{R}$, que ocorre se, e somente se, $\sigma_i(\theta) \in \mathbb{R}$, dizemos que σ_i é *real*. Caso contrário, dizemos que σ_i é *complexo*. Definimos a *conjugação complexa* de σ_i, $\overline{\sigma_i} : K \to \mathbb{C}$ por $\overline{\sigma_i}(\alpha) := \overline{\sigma_i(\alpha)}$, $\alpha \in K$. Segue-se que para qualquer monomorfismo σ_i de K em $\mathbb{C}$, $\overline{\overline{\sigma_i}} = \sigma_i$; e $\overline{\sigma_i} = \sigma_i$ se, e somente se, σ_i é real. Com isto temos que os monomorfismos complexos ocorrem aos pares conjugados. Seja $2r_2$ o *número de monomorfismos complexos*, e r_1 o *número de monomorfismos reais* de K em $\mathbb{C}$. Com isto tem-se que $n = r_1 + 2r_2$.

Sejam K um corpo de número de grau n e r_1 e r_2 como definidos acima. Seja $r = r_1 + r_2 - 1$. O Teorema de Dirichlet afirma que o grupo $\mathcal{D}^*$ das unidades de K é isomorfo a $W \times \mathbb{Z}^r$, onde W é um grupo cíclico finito constituído das raízes da unidade contidas em K. Portanto existem $r(= r_1 + r_2 - 1)$ unidades (u_i) de K tal que qualquer unidade u de K pode ser expressa de modo único na forma $u = zu_1^{\eta_1} \ldots u_r^{\eta_r}$ com $\eta_i \in \mathbb{Z}$ e z uma raiz da unidade. O conjunto (u_i), $i = 1, \ldots, r$ é chamado *sistema de unidades fundamentais* de K. Vamos demonstrar o Teorema de Dirichlet no caso em que K é um corpo quadrático, separando nos casos em que K é um corpo real ou um corpo imaginário. A seguinte proposição vai nos auxiliar bastante.

Proposição 1.9. [ST] Seja $\mathcal{D}$ o anel de inteiros de um corpo de número K e seja $x \in \mathcal{D}$. Então x é uma unidade de K (ou de $\mathcal{D}$) se, e somente se, $N(x) = \pm 1$.

Demonstração:

Se existe $y \in \mathcal{D}$ tal que $xy = 1$, então $N(xy) = 1$. Como a norma é uma

função multiplicativa temos que $N(x)N(y) = 1 \in \mathbb{Z}$. Logo $N(x) = \pm 1$.

Reciprocamente se $N(x) = \prod_{i=1}^{n} \sigma_i(x) = \pm 1$, então $x[(\pm 1).\sigma_2(x) \dots \sigma_n(x)] = 1$, (onde $\sigma_1(x) = x$). Com x e $\sigma_i(x) \in \mathcal{D}, x$ é uma unidade de $\mathcal{D}$. □

1.2.1 Teorema de Dirichlet em corpos quadráticos imaginários

Como $n = 2$ e K é um corpo quadrático imaginário então $r_2 = 1$ e $r_1 = 0$. Logo $r = r_1 + r_2 - 1 = 0$ e neste caso o Teorema de Dirichlet afirma que as únicas unidades de K são as raízes da unidade contidas em K, um grupo cíclico finito, ou seja, pelo Teorema de Dirichlet temos que $\mathcal{D}^* \simeq W$. Mais formalmente temos:

Teorema 1.10. De Dirichlet. [ST] Seja $K = \mathbb{Q}(\sqrt{-d})$, onde d é um inteiro positivo livre de quadrados. O grupo W das unidades de K é constituído das seguintes raízes da unidade.

(a) Se $d = 1$ então $W = \{\pm 1, \pm\sqrt{-1}\}$,

(b) Se $d = 3$ então $W = \{\pm 1, \pm\varepsilon, \pm\varepsilon^2\}$, onde $\varepsilon = \frac{-1+\sqrt{-3}}{2}$,

(c) Se $d > 3$ então $W = \{\pm 1\}$.

Demonstração:

Pela Proposição 1.9 as unidades de K são inteiros algébricos de norma ± 1. Seja $-d \equiv 2, 3 (mod\ 4)$, ou seja, $d \equiv 1, 2 (mod\ 4)$. Então pelo Teorema 1.7 o anel de inteiros de K é $\mathcal{D} = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$. Seja $x = a + b\sqrt{-d} \in \mathcal{D}$. Então $N(x) = a^2 + db^2 \geq 0$ e $N(x) = \pm 1$. Logo x é uma unidade se, e somente se, $a^2 + db^2 = 1$. Assim

Se $d \geq 2$ Então $b = 0$ e $a = \pm 1$. Logo $W = \{\pm 1\}$. Isto demonstra o ítem **(c)** no caso em que $d \equiv 1, 2 (mod\ 4)$.

Se $d = 1$ temos $a^2 + b^2 = 1$ e as soluções inteiras são $a = 0$, $b = \pm 1$ ou $a = \pm 1$, $b = 0$. Isto nos dá que $W = \{\pm 1, \pm\sqrt{-1}\}$ e o ítem **(a)** está demonstrado.

Agora vamos considerar o caso $-d \equiv 1 (mod\ 4)$ ou seja $d \equiv 3 (mod\ 4)$.

Pelo Teorema 1.7, $\mathcal{D} = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-d}}{2})$. Seja $x = a + \frac{b}{2}(1 + \sqrt{-d}) \in \mathcal{D}$. Então $N(x) = (a + \frac{b}{2})^2 + d(\frac{b^2}{4})$. Para x ser uma unidade de K devemos ter $(2a + b)^2 + db^2 = 4$. Temos os casos:

Se $d \geq 7$ então $b = 0$. Assim $(2a)^2 = 4$, ou $a = \pm 1$. Logo $x = \pm 1$ e isto completa a demonstração do ítem **(c)**.

Finalmente para demonstrar o ítem **(b)**, suponhamos $d = 3$. Então $(2a + b)^2 + 3b^2 = 4$. Isto implica que $b = 0, 1, -1$. Caso $b = \pm 1$ então $(2a \pm 1)^2 = 1$. Isto nos dá as soluções adicionais $x = \frac{1}{2}(\pm 1 \pm \sqrt{-3})$ (com sinais $\pm$ sendo independentes). Seja $\varepsilon = \frac{-1+\sqrt{-3}}{2}$, segue-se que $W = \{\pm 1, \pm\varepsilon, \varepsilon^2\}$. Isto demonstra o ítem **(b)** e o teorema. □

Observação 1.11. Em todos os casos W é um grupo finitamente gerado de ordem par cujos elementos são raízes da unidade.

O estudo das unidades para $d > 0$ é bem mais difícil e será tratado no próximo parágrafo.

1.2.2 Teorema de Dirichlet em corpos quadráticos reais

Neste parágrafo tomamos $d > 1$, livre de quadrados. Para o menor deles, $d = 2$, vemos que $x = 1 + \sqrt{d}$ é uma unidade de $\mathcal{D}$ e também x^n é uma unidade para todo $n \in \mathbb{N}$. Sendo $x > 1$ e real temos que $x^n \longrightarrow \infty$, quando $n \longrightarrow \infty$. Assim o conjunto das unidades de $\mathcal{D}$ é infinito. Vamos mostrar que esse fato não é acidental e sim geral. De fato, demonstraremos o Teorema de Dirichlet neste caso em que K é um corpo quadrático real exibindo uma unidade x_0 tal que o grupo das unidades de $\mathcal{D}$ é precisamente $\mathcal{D}^* = \{\pm x_0^r \mid r \in \mathbb{Z}\}$.

Recordemos que $x \in \mathcal{D}$ é da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$, se $d \not\equiv 1 (mod\ 4)$ e $x = (a + b\sqrt{d})/2$ com $a, b \in \mathbb{Z}$ e de mesma paridade, se $d \equiv 1 (mod\ 4)$. Logo para $x = c + e\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ se $x \in \mathcal{D}$ com $c \geq 0$ e $e > 0$ resulta $x > 1$ (pois o primeiro caso de $d \equiv 1 (mod\ 4)$ ocorre com $d = 5$). Pela Proposição 1.9 dado $x \in \mathcal{D}$, $x \neq 0$ temos que x é uma unidade de $\mathcal{D}$ se, e somente se, $x^{-1} = \pm\bar{x}$, onde $\bar{x}$ é o conjugado de x. Assim, se $x = c + e\sqrt{d}$ é uma unidade de $\mathcal{D}$ tal

que $x \neq \pm 1$, então $c \neq 0$ e $e \neq 0$ e o conjunto $\{\pm x, \pm\overline{x}\}$ tem interseção não vazia com cada um dos seguintes intervalos $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$. Mais ainda, $x \in (1, \infty)$ se, e somente se, $c > 0$ e $e > 0$.

Seja $K = \mathbb{Q}[\sqrt{d}]$, onde $d \geq 2$ é um inteiro livre de quadrados, e seja $x = a + b\sqrt{d}$, $(a, b \in \mathbb{Z})$ uma unidade de K. Os números $x, x^{-1}, -x, -x^{-1}$ são unidades de K, e como $N(x) = (a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$, estes quatro números são $\pm a \pm b\sqrt{d}$. Para $x \neq \pm 1$ somente um dos quatro números $x, x^{-1}, -x, -x^{-1}$ é maior que um, e este é o maior dos quatro. Assim *as unidades maiores que um de* K *são aquelas da forma* $a + b\sqrt{d}$ *com* $a > 0,\ b > 0$.

Seja K um corpo quadrático real. Então $r_1 = 2, r_2 = 0$, assim $r_1 + r_2 - 1 = 1$. O Teorema de Dirichlet afirma que que o grupo das unidades de K é isomorfo ao produto de $\mathbb{Z}$ com o grupo das raízes da unidades contidas em K. Como K está mergulhado em $\mathbb{R}$, as únicas raízes da unidade são ± 1. Logo $\mathcal{D}^* \simeq \{\pm 1\} \times \mathbb{Z}$.

Para demonstrar que $\mathcal{D}^* \simeq \{\pm 1\} \times \mathbb{Z}$ são necessários alguns resultados. Estes resultados são dados abaixo:

Lema 1.12. [BE] Seja $\mathcal{D}$ o anel de inteiros de um corpo de números quadrático $K = \mathbb{Q}(\sqrt{d})$, onde $d \geq 2$ é um inteiro livre de quadrados. Se $x = c + e\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, é uma unidade de $\mathcal{D}$ diferente de ± 1, então:

(a) O conjunto $\{\pm x, \pm\overline{x}\}$ tem interseção não vazia com cada um dos seguintes intervalos $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$.

(b) $x > 1$ se, e somente se, $c > 0$ e $e > 0$.

(c) O intervalo $(1, M]$ contém apenas um número finito de unidades de $\mathcal{D}$, onde $M > 1$ é um número real.

Demonstração:

Só falta demonstrar o ítem **(c)**. Se $x = c + e\sqrt{d} \in (1, M]$ temos pelo ítem (b) que $c > 0$ e $e > 0$. Por outro lado $c + e\sqrt{d} \leq M$ implica $2c < 2M$ e $2e < 2M$. Logo a cada unidade $x \in (1, M]$ corresponde um par de *números inteiros* $(2c, 2e) \in [1, 2M) \times [1, 2M)$. Como o número de pares de inteiros nesse conjunto é finito, também o número de unidades no intervalo será finito. □

Observação 1.13. Para concluir que $\mathcal{D}^*$ é infinito basta mostrar que $\mathcal{D}^* \neq \{\pm 1\}$.

Para demonstrar o Teorema de Dirichlet para corpos quadráticos reais ainda vamos precisar de outros resultados. Continuamos com

Lema 1.14. (*Dirichlet*) [BE] Sejam $\alpha > 0$ um número irracional e M um inteiro positivo. Existem inteiros x e y, tais que $0 < y \leq M, x \geq 0$ e $\|x - \alpha y\| < \frac{1}{M}$.

Demonstração.

Dado $t \in \mathbb{R}$ definimos $[t]$ como sendo o maior inteiro menor ou igual à t. Assim é claro que $0 \leq t - [t] < 1$.

Agora dividimos o intervalo $[0, 1)$ em M subintervalos $[0, 1/M), [1/M, 2/M), \ldots, [(M-1)/M, 1)$, cada um com comprimento $\frac{1}{M}$. Considere os seguintes $M + 1$ números: $\beta_1 = \alpha - [\alpha]$, $\beta_2 = 2\alpha - [2\alpha], \ldots, \beta_M = M\alpha - [M\alpha]$, $\beta_{M+1} = (M+1)\alpha - [(M+1)\alpha]$. Como α é um número irracional temos que cada β_i satisfaz $0 < \beta_i < 1$ e assim existem inteiros $0 < u < v \leq M + 1$ tais que β_u e β_v pertencem a um mesmo intervalo. Isto é, $\|([v\alpha] - [u\alpha]) - (v-u)\alpha\| < \frac{1}{M}$. Chamando $x = [v\alpha] - [u\alpha]$ e $y = v - u$ temos que $\|x - \alpha y\| < \frac{1}{M}$ com $x \geq 0$ e $y > 0$. □

Lema 1.15. [BE] Seja $\alpha > 0$ um número irracional. Existem infinitos pares de inteiros (x, y) tais que $y \neq 0$ e $\|\frac{x}{y} - \alpha\| < \frac{1}{y^2}$.

Demonstração.

Primeiramente vemos que $x = [\alpha]$ e $y = 1$ satisfazem às condições do Lema. Suponhamos agora que já encontramos n pares distintos de inteiros $(x_i, y_i), i = 1, \ldots, n$ que satisfazem às condições do Lema. Tomemos $\delta = \min\{\|x_i - \alpha y_i\|, i = 1, \ldots, n\}$. Como α é irracional, $\|x_i - \alpha y_i\| > 0$ para todo i. Assim $\delta > 0$ também. Seja M um número natural tal que $\frac{1}{M} < \delta$. Pelo Lema anterior temos que existem $x, y \in \mathbb{Z}$ com $x \geq 0$ e $0 < y \leq M$ tais que $\|x - \alpha y\| < \frac{1}{M} < \delta$. Assim (x, y) é distinto de qualquer (x_i, y_i) e

$\|\frac{x}{y} - \alpha\| < \frac{1}{My} \leq \frac{1}{y^2}$. Concluímos então que o conjunto de tais pares é infinito. □

Teorema 1.16. [BE] Sejam $\mathcal{D}$ o anel de inteiros de um corpo de números quadrático $K = \mathbb{Q}(\sqrt{d})$, onde $d \geq 2$ é um inteiro livre de quadrados e $\mathcal{D}^*$ o grupo das unidades de K. Existem inteiros x e y, com $y \neq 0$, tais que $x^2 - dy^2 = 1$. Ou equivalentemente, $\mathcal{D}^* \cap \mathbb{Z}[\sqrt{d}] \neq \{\pm 1\}$.

A prova que daremos deste resultado é devida à Dirichlet e seu principal argumento depende de uma boa aproximação, por racionais, do número irracional $\sqrt{d}$.

Demonstração.

Vamos começar por encontrar $k \in \mathbb{Z}$ tal que $N(\alpha) = k$ para um número infinito de elementos $\alpha \in \mathbb{Z}[\sqrt{d}]$. Sejam $x, y \in \mathbb{Z}$ com $y \neq 0$ e

$$\|x/y - \sqrt{d}\| < 1/y^2. \qquad (1)$$

Temos então

$$\|N(x + y\sqrt{d})\| = \|x^2 - dy^2\| = \|x - y\sqrt{d}\| \,.\, \|x + y\sqrt{d}\| =$$

$$= y^2 \|\frac{x}{y} - \sqrt{d}\| \,.\, \|\frac{x}{y} + \sqrt{d}\| < \|\frac{x}{y} + \sqrt{d}\| = \|\frac{x}{y} - \sqrt{d} + 2\sqrt{d}\| \leq$$

$$\leq \|\frac{x}{y} - \sqrt{d}\| + 2\sqrt{d} < \frac{1}{y^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Portanto $N(x+y\sqrt{d})$ é um inteiro entre $-1-2\sqrt{d}$ e $1+2\sqrt{d}$. Como, pelo Lema 1.13, existem infinitos pares (x, y) que satisfazem (1) acima, temos que existe $k \in \mathbb{Z}, k \neq 0$, com $\|k\| < 1 + 2\sqrt{d}$ e tal que $N_k := \{\alpha \in \mathbb{Z}[\sqrt{d}] \mid N(\alpha) = k\}$ é um conjunto infinito.

Sejam $\alpha, \beta \in \mathbb{N}_k$ tais que $\alpha\beta^{-1} \neq \pm 1$ e $N(\alpha\beta^{-1}) = N(\alpha)/N(\beta) = k/k = 1$. Assim, se encontramos α, β nessas condições e tais que $\alpha\beta^{-1} \in \mathbb{Z}[\sqrt{d}]$ o teorema está demonstrado. Observemos que $\alpha\beta^{-1} = \alpha\bar{\beta}/N(\beta) = \alpha\bar{\beta}/k$. Estamos portanto procurando $\alpha, \beta \in \mathbb{N}_k$ tais que $\alpha\bar{\beta} \in k\mathbb{Z}[\sqrt{d}]$ e $\alpha \neq \pm\beta$. Seja $S_k = \{(\bar{x}, \bar{y}) \in \mathbb{Z}_{\|k\|} \times \mathbb{Z}_{\|k\|} | \alpha = x + y\sqrt{d} \in \mathbb{N}_k\}$, onde $\mathbb{Z}_{\|k\|}$ é o conjunto das classe de inteiros módulo $\|k\|$. Como S_k é finito e N_k é infinito, existem $\alpha = x + y\sqrt{d}$ e $\beta = x' + y'\sqrt{d}$ em N_k tais que $\alpha \neq \pm\beta$ e $(\bar{x}, \bar{y}) = (\bar{x'}, \bar{y'})$.

Isto é, k divide $x - x'$ e $y - y'$. Portanto $\alpha - \beta = k\gamma$ com $\gamma \in \mathbb{Z}[\sqrt{d}]$. Assim $k\gamma\bar{\beta} = (\alpha - \beta)\bar{\beta} = \alpha\bar{\beta} - k$, (pois $N(\beta) = \beta\bar{\beta}$). Logo $\alpha\bar{\beta} = k(\gamma\bar{\beta} + 1) \in k\mathbb{Z}[\sqrt{d}]$ e ainda $\alpha \neq \pm\beta$, como queríamos. □

Agora estamos em condições de demonstrar o Teorema de Dirichlet e vamos enunciá-lo destacando um gerador especial.

Teorema 1.17. [BE] Seja $\mathcal{D}$ o anel de inteiros de um corpo de números quadrático K. Existe uma única unidade $x_0 > 1$ em $\mathcal{D}$ tal que toda unidade de $\mathcal{D}$ é da forma $\pm x_0^n$ com $n \in \mathbb{Z}$.

Demonstração.

Usando o Lema e o Teorema podemos obter uma unidade $\omega = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, com $\omega > 1$. Mais ainda, existe apenas um número finito de unidades no intervalo $(1, \omega]$ (Lema 1.12-(c)). Tomamos então $x_0 = \min\{x \in \mathcal{D}^* \mid x > 1\}$ e seja ν uma unidade de $\mathcal{D}$ com $\nu > 1$. Como $x_0^k \longrightarrow \infty$ com $k \in \mathbb{N}$, temos que existe n tal que $0 < x_0^{n-1} < \nu \leq x_0^n$ e pela escolha de x_0, $n \geq 1$. Assim $0 < 1 < \nu x_0^{1-n} \leq x_0$. Novamente, pela escolha de x_0 temos $\nu x_0^{1-n} = x_0$, ou $\nu = x_0^n$. Seja agora $\nu \neq \pm 1$ uma unidade qualquer de $\mathcal{D}$. Sabemos, pelo Lema 1.12 que $\{\pm\nu, \pm\nu^{-1}\} \cap (1, \infty)$ não é vazio. Portanto $\nu = \pm x_0^n$, com $n \in \mathbb{Z}$.
A unicidade de x_0 decorre de sua escolha. □

Definição 1.18. A unidade x_0 do Teorema 1.17 é chamada de *unidade fundamental* de $\mathcal{D}$, onde $\mathcal{D}$ é o anel de inteiros de um corpo de números quadrático real K.

Sempre é possível encontrar a unidade fundamental. Por exemplo, quando: **(a)** $d \not\equiv 1 (mod\ 4)$ procedemos da seguinte maneira: Vamos calculando $\pm 1 + dy^2$, com $y = 1, 2, \ldots, etc$, até encontrar o primeiro quadrado perfeito (que existe pelo Teorema 1.16). Isto é, o menor x positivo tal que $x^2 = \pm 1 + dy^2$, e então $x_0 = x + y\sqrt{d}$ é a unidade fundamental pelo Teorema 1.17. O problema é que nem sempre isso ocorre rapidamente. Por exemplo, para $d = 31$ só temos sucesso quando $y = 273$ e então $x = 1520$. Assim sendo o processo não é muito efetivo. Usando a Teoria de Frações Contínuas, Lagrange obteve um algorítmo

eficiente para encontrar a unidade fundamental.

(b) $d \equiv 1(mod\ 4)$ podemos proceder da mesma forma em relação a equação $x^2 = \pm 4 + dy^2$. Por exemplo, para $d = 65$, tomando $y = 2$ obtemos $-4 + 65.4 = 16^2$. Isso nos leva $-1 = N((16 + 2\sqrt{65})/2)$, ou $-1 = N(8 + \sqrt{65})$. Temos que $8 + \sqrt{65} > 1$ e como os valores de x crescem com y vemos que $y = 2$ é o menor valor para o qual a equação tem solução maior que 1. Dessa forma $x_0 = 8 + \sqrt{65}$.

Capítulo 2

Diagonalização da forma traço sobre alguns anéis de corpos de números

Neste capítulo vamos estudar a forma bilinear traço sobre alguns anéis de inteiros de corpos de números. Determinaremos todos os corpos de números quadráticos para os quais a forma traço pode ser diagonalizada sobre o seu anel de inteiros, isto é, os corpos quadráticos com uma base integral ortogonal com respeito ao traço.

2.1 Diagonalização da Forma Traço

Sejam $K = \mathbb{Q}(\sqrt{d})$ um corpo de números quadrático, onde d é um inteiro livre de quadrados e $\mathcal{D}$ o seu anel de inteiros. Já vimos no capítulo anterior que $\{1, \sqrt{d}\}$, respectivamente, $\{1, (1+\sqrt{d})/2\}$ é uma base integral para K, no caso de $d \equiv 2,$ ou $3(mod\ 4)$, respectivamente, $d \equiv 1(mod\ 4)$. Denotemos por w o elemento

$$w = \begin{cases} \sqrt{d}, & \text{se} \quad d \equiv 2, 3(mod\ 4), \\ \dfrac{1+\sqrt{d}}{2}, & \text{se} \quad d \equiv 1(mod\ 4), \end{cases}$$

para uniformizar a notação. Se $b : \mathcal{D} \times \mathcal{D} \longrightarrow \mathbb{Z}$ é uma forma bilinear sobre $\mathcal{D}$ dizemos que o par $(\mathcal{D}, b)$ é um *espaço bilinear*. Uma $\mathbb{Z}$-base $\{\beta_1, \beta_2\}$ de $\mathcal{D}$ é dita *ortogonal* (em relação a b) se $b(\beta_1, \beta_2) = 0$. Também diremos que a base $\{\beta_1, \beta_2\}$ é uma base integral ortogonal para o espaço bilinear $(\mathcal{D}, b)$.

Inicialmente vamos estudar a forma bilinear

$$b : \mathcal{D} \times \mathcal{D} \longrightarrow \mathbb{Z},$$

definida por $b(\alpha, \beta) = Tr(\alpha.\overline{\beta})$, onde $\bar{\beta}$ é o complexo conjugado de β. Temos

Teorema 2.1. [D] Seja $\mathcal{D}$ o anel de números do corpo $\mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados, e considere a forma bilinear traço $Tr(\alpha.\overline{\beta})$ definida sobre $\mathcal{D}$. Então esta forma bilinear admite uma base integral ortogonal se, e somente se, $d \equiv 2$ ou 3 $(mod\ 4)$.

Demonstração:

De fato, se $d \equiv 2$ ou 3 $(mod\ 4)$, então $\{1, w\}$ é uma base integral ortogonal, pois,

$$b(1, w) = Tr(1\overline{w}) = Tr(\overline{w}) = Tr(-\sqrt{d}) = (-\sqrt{d}) + (\sqrt{d}) = 0.$$

Agora, para $d \equiv 1(mod\ 4)$ suponha que existe uma base integral ortogonal $C = \{\beta_1, \beta_2\}$ para o espaço bilinear $(\mathcal{D}, b)$. Como $\{1, w\}$ é uma base integral, existem $p, q, r, s \in \mathbb{Z}$ tais que $\beta_1 = p + qw$ e $\beta_2 = r + sw$. Logo

$$\begin{aligned} b(\beta_1, \beta_2) = \mathrm{Tr}(\beta_1\overline{\beta}_2) &= \mathrm{Tr}\left((p + qw)(r - sw)\right) \\ &= \mathrm{Tr}(pr + (qr - ps)w - qsw^2) \\ &= \frac{1}{2}\left((2p + q)(2r + s) - qsd\right) = 0, \end{aligned}$$

pois $w = \dfrac{1 + \sqrt{d}}{2}$. Logo $4pr + 2(ps + qr) + qs(1 - d) = 0$. Pelo Teorema 1.3 temos que a matriz

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix}$$

é unimodular, ou seja , $ps - qr = \pm 1$. Assim, fazendo congruência módulo 4 temos:

$$4pr + 2(ps + qr) + qs(1 - d) \equiv 0 \pm 2(mod\ 4) \equiv 2(mod\ 4),$$

pois $d \equiv 1(mod\ 4)$, o que é um absurdo.

Portanto, com relação à forma bilinear traço $Tr(\beta_1\overline{\beta_2})$ a base $C = \{\beta_1, \beta_2\}$ não é uma base integral ortogonal, qualquer que seja a base integral C de $\mathcal{D}$. □

Observação 2.2. A forma bilinear traço $Tr(\alpha\overline{\beta})$ também chamada forma bilinear *traço hermitiana* está relacionada com a distância usual do plano. De fato, se identificarmos o espaço vetorial real $\mathbb{C}$ com $\mathbb{R}^2$ temos que a distância usual de um ponto $P(x, y)$ à origem é dada por $d(P, 0) = \sqrt{x^2 + y^2}$. A forma quadrática $q(x, y) = x^2 + y^2$ está relacionada ao produto interno usual do plano $\langle (x, y), (x_1, y_1) \rangle = xx_1 + yy_1$. Como $q_{Tr}(x, y) = 2x^2 + 2y^2$, temos que $d(P, 0) = \sqrt{\frac{1}{2} q_{Tr}(x, y)}$.

Agora passemos ao estudo da forma bilinear traço

$$b : \mathcal{D} \times \mathcal{D} \longrightarrow \mathbb{Z}$$
$$b(\alpha, \beta) = \mathrm{Tr}(\alpha\beta),$$

para $\alpha, \beta \in \mathcal{D}$, onde $\mathrm{Tr} = \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}$ é o traço de K sobre $\mathbb{Q}$. Comecemos com o seguinte resultado imediato:

Lema 2.3. [D] Seja $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ um corpo de números tal que $d \equiv 2$ ou $3(mod\ 4)$. Então $\{1, w\}$ é uma base integral ortogonal para o espaço bilinear $(\mathcal{D}, b)$.

Demonstração:

Basta ver que $b(1, w) = Tr(\sqrt{d}) = 0$. □

Se $d \equiv 1(mod\ 4)$ então $b(1, w) = \mathrm{Tr}(w) = 1 \neq 0$. Assim a base integral $\{1, w\}$ de $\mathcal{D}$ não é ortogonal, neste caso. A seguir vamos caracterizar os inteiros

racionais d livre de quadrados, $d \equiv 1(mod\ 4)$, para os quais existe uma base integral ortogonal em $\mathcal{D}$ relativamente a forma traço b. Comecemos com os dois teoremas seguintes onde damos algumas condições equivalentes para a existência de uma base integral ortogonal do anel $\mathcal{D}$ do corpo de números $\mathbb{Q}(\sqrt{d})$, para $d \equiv 1(mod\ 4)$.

Teorema 2.4. [D] Sejam $K = \mathbb{Q}(\sqrt{d})$, onde $d \equiv 1(mod\ 4)$ é livre de quadrados e $\mathcal{D}$ seu anel de inteiros. Então as seguintes condições são equivalentes:

(1) Existe uma base integral ortogonal em $\mathcal{D}$ relativamente à forma traço.

(2) Existem $p, q, r, s \in \mathbb{Z}$ satisfazendo

$$ps - qr = 1. \tag{2.1.1}$$

$$(2p + q)(2r + s) + qsd = 0. \tag{2.1.2}$$

(3) Existem $p, q \in \mathbb{Z}$ tais que para

$$t = 2p + q \quad \text{e} \quad \Delta = t^2 + dq^2$$

os números

$$r = -\frac{t + dq}{\Delta}; \quad s = \frac{2t}{\Delta}. \tag{2.1.3}$$

são inteiros.

(4) Existe um divisor Δ' de d em $\mathbb{Z}$ tal que 2 é representado sobre $\mathbb{Z}$ pela forma quadrática $\Delta' X^2 + \Delta'' Y^2$, onde $\Delta'' = \dfrac{d}{\Delta'}$.

Demonstração:

(2) implica (1): Por hipótese existem $p, q, r, s \in \mathbb{Z}$ tais que $ps - qr = 1$. Sejam $\beta_1 = p + qw$, $\beta_2 = r + sw$. Então o determinante da matriz

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix},$$

$ps - qr$ é igual a 1. Como $\{1, w\}$ é uma base integral de K, pelo Teorema 1.3 segue que $\{\beta_1, \beta_2\}$ é uma base integral. Calculando o traço, obtemos:

$$\begin{aligned} b(\beta_1, \beta_2) &= \mathrm{Tr}(\beta_1\beta_2) = \mathrm{Tr}((p+qw)(r+sw)) \\ &= \mathrm{Tr}(pr + (ps+qr)w + qsw^2) \\ &= \frac{1}{2}((2p+q)(2r+s) + qsd) \\ &= \frac{1}{2} \cdot 0 = 0. \end{aligned}$$

Portanto $\beta = \{\beta_1, \beta_2\}$ é uma base integral ortogonal.

(1) implica (2): Seja $\beta = \{\beta_1, \beta_2\}$ uma base integral ortogonal. Como $\{1, w\}$ é uma base integral, existem $p, q, r, s \in \mathbb{Z}$ tais que $\beta_1 = p + qw$ e $\beta_2 = r + sw$. Pelo Teorema 1.3, a matriz

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix}$$

é unimodular, ou seja , $ps - qr = \pm 1$.
Se $ps - qr = 1$ então vale (2.1.1). Se $ps - qr = -1$ então $p(-s) + q(-r) = 1$. Neste caso troquemos β_2 por $-\beta_2$ e temos novamente a equação (2.1.1).

Para obter a equação 2.1.2 vamos considerar as equações que se obtém de $b(\beta_1, \beta_2) = 0$. Temos:

$$\begin{aligned} b(\beta_1, \beta_2) &= \mathrm{Tr}(\beta_1\beta_2) = \mathrm{Tr}((p+qw)(r+sw)) \\ &= \mathrm{Tr}(pr + (ps+qr)w + qsw^2) \\ &= \frac{1}{2}((2p+q)(2r+s) + qsd) = 0, \end{aligned}$$

pois $w = \dfrac{1+\sqrt{d}}{2}$. Logo $(2p+q)(2r+s) + qsd = 0$ e portanto vale (2.1.2).

(2) implica (3): Para determinar r e s usemos as equações (2.1.1) e (2.1.2). Colocando r e s em evidência, obtemos:

$$\begin{cases} ps - qr = 1 \\ (2p + q + qd)s + (4p + 2q)r = 0. \end{cases}$$

Para usarmos a regra de Cramer, consideremos

$$D = \begin{vmatrix} p & -q \\ 2p+q+qd & 4p+2q \end{vmatrix}, \; D_s = \begin{vmatrix} 1 & -q \\ 0 & 4p+2q \end{vmatrix} \text{ e } D_r = \begin{vmatrix} p & 1 \\ 2p+q+qd & 0 \end{vmatrix}.$$

Daí obtemos

$$s = \frac{D_s}{D} = \frac{4p+2q}{4p^2+4pq+q^2+q^2d} = \frac{2(2p+q)}{(2p+q)^2+dq^2} = \frac{2t}{t^2+dq^2} = \frac{2t}{\Delta} \quad \text{e}$$

$$r = \frac{D_r}{D} = \frac{-2p-q-qd}{t^2+dq^2} = -\frac{(2p+q)+dq}{\Delta} = -\frac{t+dq}{\Delta},$$

que são números inteiros por hipótese.

(3) implica (2): Mostremos primeiramente que vale $ps - qr = 1$.

Sejam $p, q \in \mathbb{Z}$ tais que para $t = 2p + q$ e $\Delta = t^2 + dq^2$ os números $r = -\frac{t+dq}{\Delta}$; $s = \frac{2t}{\Delta}$ são inteiros. Assim $ps - qr = p(\frac{2t}{\Delta}) - q(\frac{-t-dq}{\Delta}) = p(\frac{2(2p+q)}{\Delta}) - q(\frac{-2p-q-dq}{\Delta}) = \frac{4p^2+4pq+q^2+dq^2}{t^2+dq^2} = 1.$

Demonstremos agora que $(2p + q)(2r + s) + qsd = 0$.

Temos $(2p+q)(2r+s)+qsd = (4p+2q)r+(2p+q+qd)s = (4p+2q)(-\frac{t+dq}{\Delta})+(2p+q+qd)(\frac{2t}{\Delta}) = (4p+2q)(-\frac{2p+q+dq}{\Delta}) + (2p+q+qd)(\frac{4p+2q}{\Delta}) = 0.$

(4) implica (1): Se $2 = \Delta' x^2 + \Delta'' y^2$ onde $\Delta'\Delta'' = d$ e $x, y \in \mathbb{Z}$, então x e y são ímpares (desde que d é ímpar). De fato, suponhamos que x é par. De $2 = \Delta' x^2 + \Delta'' y^2$ segue-se que $\Delta'' y^2$ é par. Como Δ'' é ímpar (pois é um divisor de d que é ímpar), vem que y^2 também é par. Logo y tem que ser par, e então 4 divide y^2 e x^2. Consequentemente 4 divide 2 em $\mathbb{Z}$, o que é um absurdo. Então $p = \frac{\Delta' x - y}{2}$ e $q = y$ são inteiros e devemos provar que r, s definidos em (2.1.3)

são inteiros. De fato, $t = 2p+q = 2(\frac{\Delta' x - y}{2}) + y = \Delta' x - y + y = \Delta' x$ e assim $\Delta = t^2 + dq^2 = (\Delta' x)^2 + \Delta' \Delta'' y^2 = \Delta'^2 x^2 + \Delta' \Delta'' y^2 = \Delta'(\Delta' x^2 + \Delta'' y^2) = 2\Delta'$, e $t + dq = \Delta' x + \Delta' \Delta'' y = \Delta'(x + \Delta'' y)$. Então $t + dq$ é divisível por $2\Delta' = \Delta$, isto é, $r = \frac{t+dq}{\Delta}$ é um inteiro. Analogamente $s = \frac{2t}{\Delta} = \frac{2t}{2\Delta'} = \frac{t}{\Delta'} = \frac{2p+q}{\Delta'} = \frac{2p+y}{\Delta'} = \frac{\Delta' x}{\Delta'} = x$ é um inteiro.

(1) implica (4): Usando as notações acima demonstremos que as condições equivalentes **(1)**, **(2)** e **(3)** já demonstradas, implicam **(4)**. Primeiro vamos demonstrar que q e s são ímpares.

Tomando a igualdade (2.1.2) módulo 4, temos

$$2 + qs(1 + d) \equiv 0 (\text{mod } 4)$$

Como $1 + d \equiv 2(mod\ 4)$, (pois $d \equiv 1(mod\ 4)$) temos que $2 + qs(1 + d) \equiv 2 + 2qs(mod\ 4) \equiv 0(mod\ 4)$. Desde que 2 não é congruente à zero módulo 4 temos que qs é ímpar. Consequentemente q e s são ímpares.

Agora vamos começar a demonstrar o ítem (4) exibindo um divisor Δ' de d em $\mathbb{Z}$.

Como q é ímpar, o número $t = 2p + q$ (definido no ítem (3)) é ímpar. Como para todo número ímpar x, $x^2 \equiv 1(mod\ 4)$ temos que $t^2 \equiv q^2(mod\ 4) \equiv 1(mod\ 4)$. Como $d \equiv 1(mod\ 4)$ segue-se que $\Delta = t^2 + dq^2 \equiv 1 + 1(mod\ 4)$ ou $\Delta \equiv 2(mod\ 4)$. Logo Δ é par e fazendo $\Delta' = \frac{\Delta}{2}$, então Δ' é ímpar. De (2.1.3) obtemos $\Delta' | (t + dq)$ e $\Delta' | t$. Como $dq = (t + dq) - t$, obtemos também que $\Delta' | dq$. Agora vamos demonstrar que Δ' divide d.

Seja $d_1 = mdc(t, q)$. Como $t = 2p + q$ é ímpar então d_1 é ímpar. Como d_1 divide $2p = t - q$ e é ímpar vem que d_1 divide p. Logo d_1 divide $mdc(p, q) = 1$, (por 2.1.1), ou seja, $d_1 = 1$. Pela identidade de Bezout existem $x_1, x_2 \in \mathbb{Z}$ tais que $1 = qx_1 + tx_2$. Logo $d = dq.x_1 + t.dx_2$. Como Δ' divide t e dq segue-se que $\Delta' | d$.

Agora para finalizar a demonstração, por definição de Δ' temos $2\Delta' = \Delta = t^2 + dq^2 = (s\Delta')^2 + \Delta' \Delta'' q^2 = \Delta'(\Delta' s^2 + \Delta'' q^2)$, isto é, $2 = \Delta' s^2 + \Delta'' q^2$ e vale (4). □

Corolário 2.5. [D] Seja $\mathcal{D}$ o anel de inteiros de $\mathbb{Q}(\sqrt{d})$, onde $d > 1$ é um inteiro livre de quadrados e $d \equiv 1(mod\ 4)$. Então não existe uma base integral ortogonal em $\mathcal{D}$ relativamente a forma traço.

Demonstração:

Por hipótese $d \geq 5$ e como $\Delta'.\Delta'' = d$, temos que Δ' e Δ'' tem o mesmo sinal. Se ambos são negativos então, evidentemente não existem $x,\ y \in \mathbb{Z}$ tais que $2 = \Delta' x^2 + \Delta'' y^2$. Se ambos são positivos, sem perda de generalidade, podemos supor que $\Delta' > 2$. Portanto se $2 = \Delta' x^2 + \Delta'' y^2$ para $x,\ y \in \mathbb{Z}$ então $x = 0$. Daí $2 = \Delta'' y^2$ com $y \in \mathbb{Z}$; o que é um absurdo. □.

Observação 2.6. Seja $\varepsilon = u + v\sqrt{a}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{a})$ onde $a \equiv 3(mod\ 4)$, $a > 0$ e livre de quadrados. Então $N\varepsilon = u^2 - av^2 = 1$, desde que $a \equiv 3(mod\ 4)$. Denota $\varepsilon^n = u_n + v_n\sqrt{a}$, para $n \in \mathbb{Z}$. Observemos que u é ímpar se, e somente se, v é par se, e somente se, todos u_n são ímpares. Vamos demonstrar estas afirmações:

De $u^2 - av^2 = 1$, a demonstração de que u é ímpar se, e somente se, v é par, é simples. Agora se todos os u_n são ímpares então $u = u_1$ é ímpar. Daí v é par.

Reciprocamente se u é ímpar, de $u^2 - av^2 = 1$ segue-se que v é par. Assim $u_1 = u$ é ímpar. De $\varepsilon^{k+1} = \varepsilon^k.\varepsilon$, segue-se que $u_{k+1} = u_k.u + avv_k$. Logo por indução em $n \in \mathbb{N}$ temos que u_n é ímpar, para todo $n \in \mathbb{N}$.

Negando as equivalências anteriores podemos concluir que: Se u_n é par para algum n então u é par.

Teorema 2.7. [D] Seja $K = \mathbb{Q}(\sqrt{d})$ onde $d \equiv 1(mod\ 4)$ é livre de quadrados e $d < 0$. Seja $\varepsilon = u + v\sqrt{a}$ a unidade fundamental do anel de inteiros $\mathcal{D}$ do corpo $\mathbb{Q}(\sqrt{a})$, onde $a = -d > 0$. Então as seguintes condições são equivalentes:

(1) Existe uma base integral ortogonal no anel $\mathcal{D}_K$ relativamente à forma traço.

(2) u é par.

Demonstração:

(2) implica (1): Suponha que u é par. Então de $1 = N\epsilon = u^2 - av^2$ segue que $u^2 - 1 = av^2$ o que implica que $(u+1)(u-1) = av^2$ e $mdc(u+1, u-1) = 1$. Consequentemente

$$u + 1 = a_1 x^2$$

$$u - 1 = a_2 y^2$$

onde $a_1 a_2 = a$ e $xy = v$. Subtraindo obtemos $2 = a_1 x^2 - a_2 y^2$ e tomando $\Delta' = a_1, \Delta'' = -a_2$ obtemos (4) onde $\Delta'\Delta'' = -a_1 a_2 = -a = d$. Logo, pelo Teorema 2.4 existe uma base integral ortogonal em $\mathcal{D}_K$ relativamente à forma traço.

(1) implica (2):. Pelo Teorema 2.4 existe Δ' dividindo d e $x, y \in \mathbb{Z}$ satisfazendo $\Delta' x^2 + \Delta'' y^2 = 2$, onde $\Delta'' = \dfrac{d}{\Delta'}$. Então $\Delta'\Delta'' = d = -a$ por hipótese. Observemos que como $2 = \Delta' x^2 + \Delta'' y^2$ segue que $\Delta' x^2 = 2 - \Delta'' y^2$. Subtraindo 1 de ambos os lados obtemos $\Delta' x^2 - 1 = 1 - \Delta'' y^2 = U$ e $V = xy$ satisfazendo $U^2 - aV^2 = (\Delta' x^2 - 1)(1 - \Delta'' y^2) + \Delta'\Delta'' x^2 y^2 = \Delta' x^2 - \Delta'\Delta'' x^2 y^2 - 1 + \Delta'' y^2 + \Delta'\Delta'' x^2 y^2 = \Delta' x^2 + \Delta'' y^2 - 1 = 2 - 1 = 1$. Além disso U é par. De fato, segue do Teorema 2.4 que $2 = x^2\Delta' + y^2\Delta''$, onde $\Delta'\Delta'' = d$ e $x, y \in \mathbb{Z}$. Então x, y são ímpares (desde que d é ímpar). Assim, $U = 1 - \Delta'' y^2$ é par. Portanto da observação 2.6 segue que vale (5) vale. □

Teorema 2.8. [D] Seja $p \equiv 3 (mod\ 4)$ um número primo, e seja $\varepsilon = u + v\sqrt{p}$ a unidade fundamental do anel de inteiros $\mathcal{D}$ de $\mathbb{Q}(\sqrt{p})$. Então u é par.

Demonstração:

Pela observação 2.6, $N\epsilon = 1$, assim $(u+1)(u-1) = pv^2$. Se u é ímpar, então v é par. Sejam $u = 2u_1 + 1$ e $v = 2v_1$, onde $u_1, v_1 \in \mathbb{Z}$. Então $(2u_1 + 1 + 1)(2u_1 + 1 - 1) = 4pv_1^2$ o que implica que $4u_1^2 + 4u_1 = 4pv_1^2$. Logo $u_1(u_1 + 1) = pv_1^2$ e como u_1 e $u_1 + 1$ são primos entre si, temos

$$\begin{cases} u_1 + 1 &= py^2 \\ u_1 &= x^2 \end{cases} \quad \text{ou} \quad \begin{cases} u_1 + 1 &= x^2 \\ u_1 &= py^2, \end{cases}$$

para alguns inteiros positivos x, y satisfazendo $xy = v_1$.

O primeiro caso é impossível módulo 4. De fato, $u_1 + 1 - py^2 \equiv 0(mod\ 4)$, e como $u_1 = x^2$ temos $x^2 + 1 - py^2 \equiv 0(mod\ 4)$. Para ver isto consideremos as quatro possibilidades:

(a) quando x e y são pares temos $1 \equiv 0(mod\ 4)$ o que é um absurdo.

(b) quando x e y são ímpares temos $-1 \equiv 0(mod\ 4)$ o que é um absurdo.

(c) quando x é par e y é ímpar temos $-2 \equiv 0(mod\ 4)$ o que é um absurdo.

(d) quando x é ímpar e y é par temos $2 \equiv 0(mod\ 4)$ o que é um absurdo.

No segundo caso subtraindo obtemos $py^2 + 1 = x^2$ o que implica $x^2 - py^2 = 1$, onde $x \leq u_1 + 1 < u$. Isto contradiz a minimalidade de u. Portanto u é par. □

Corolário 2.9. [D] Se $p \equiv 3(mod\ 4)$ é um número primo, então no anel de inteiros $\mathcal{D}$ do corpo $\mathbb{Q}(\sqrt{-p})$ existe uma base integral ortogonal relativamente à forma traço.

Demonstração:

Temos que $p \equiv 3(mod\ 4)$ assim $-p \equiv 1(mod\ 4)$. Seja $\varepsilon = u + v\sqrt{p}$ a unidade fundamental do anel de inteiros do corpo $\mathbb{Q}(\sqrt{p})$. Então pelo Teorema 2.8 u é par. Logo, pelo Teorema 2.7 segue que existe uma base integral ortogonal no anel $\mathcal{D}$. □

Teorema 2.10. [D] Sejam p, q números primos, $pq \equiv 3(mod\ 4)$, seja $\epsilon = u + v\sqrt{pq}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{pq})$. Se $\left(\frac{p}{q}\right) = -1$ então u é par.

Demonstração:

Temos $N\epsilon = u^2 - pqv^2 = 1$, onde $u, v > 0$. Sem perda de generalidade podemos assumir que $p \equiv 1(mod\ 4), q \equiv 3(mod\ 4)$.

Suponhamos que u é ímpar. Então v é par, isto é , $u = 2u_1 + 1, v = 2v_1$. De $u^2 - pqv^2 = 1$ segue que $u^2 - 1 = pqv^2$, logo $(u+1)(u-1) = pqv^2$. Substituindo

os valores de u e v obtemos $(2u_1+1+1)(2u_1+1-1) = 4pqv_1^2$ o que implica $(2u_1+2)(2u_1) = 4pqv_1^2$. Então $4u_1^2+4u_1 = 4pqv_1^2$, ou seja, $u_1(u_1+1) = pqv_1^2$. Novamente como u_1 e u_1+1 são primos entre si temos as quatro possibilidades:

(i) $u_1+1 = pqx^2$ e $u_1 = y^2$,

(ii) $u_1+1 = x^2$ e $u_1 = pqy^2$,

(iii) $u_1+1 = px^2$ e $u_1 = qy^2$,

(iv) $u_1+1 = qx^2$ e $u_1 = py^2$,

onde x, y são inteiros positivos de diferentes paridades e $xy = v_1$. Subtraindo obtemos:

Em (i) e em (iv) são impossíveis módulo 4. Primeiramente vamos analisar o caso (i). De (i) segue que $y^2+1 = pqx^2$ que implica $pqx^2 - y^2 = 1$. Assim, temos dois casos a considerar: quando x é par e y é ímpar e quando x é ímpar e y é par. Do primeiro caso temos $-2 \equiv 0(mod\ 4)$ e do segundo caso temos $2 \equiv 0(mod\ 4)$, ambos absurdo. Agora analisemos o caso (iv). De (iv) temos $py^2+1 = qx^2$ que implica $qx^2 - py^2 = 1$. Assim, analogamente ao caso (i) temos dois casos a considerar: quando x é par e y é ímpar e quando x é ímpar e y é par. Do primeiro caso temos $-2 \equiv 0(mod\ 4)$ e do segundo caso temos $2 \equiv 0(mod\ 4)$, ambos absurdo.

De (iii): $qy^2+1 = px^2$ implica $px^2 - qy^2 = 1$. Logo $px^2 \equiv 1(mod\ q)$ e daí $(px)^2 \equiv p(mod\ q)$. Isto contradiz a hipótese de que $\left(\frac{p}{q}\right) = -1$.

De (ii): $x^2 - pqy^2 = 1$ obtemos $N(x+y\sqrt{pq}) = 1$. Pela minimalidade de u temos $u \leq x \leq v_1 \leq u_1 < u$, o que é uma contradição. Logo u é par, como queríamos demonstrar. □

Corolário 2.11. [D] Se p, q são primos satisfazendo $pq \equiv 3(mod\ 4)$ e $\left(\frac{p}{q}\right) = -1$, então no anel de inteiros do corpo $\mathbb{Q}(\sqrt{-pq})$ existe uma base integral ortogonal relativamente à forma traço.

Demonstração:

Pelo Teorema 2.10 segue que u é par, então pelo Teorema 2.7 existe uma base integral ortogonal no anel de inteiros do corpo $\mathbb{Q}(\sqrt{-pq})$, onde $-pq \equiv 1(mod\ 4)$. □

Observação 2.12. Existem corpos do tipo $\mathbb{Q}(\sqrt{-pq})$ que não satisfazem as hipóteses do Corolário 2.11 e no entanto admitem uma base integral ortogonal. Em outras palavras, a recíproca do Corolário 2.11 não é válida. Por exemplo, para $p = 17$ e $q = 19$ temos $pq \equiv 3(mod\ 4)$, mas $\left(\frac{p}{q}\right) = 1$, (pois $6^2 \equiv 17(mod\ 19)$). Logo as hipóteses do Corolário 2.11 não estão satisfeitas. Mas para estes valores temos a unidade fundamental $\epsilon = 18 + \sqrt{pq}$, em $\mathbb{Q}(\sqrt{pq})$. Então pelo Teorema 2.7 existe uma base integral ortogonal no corpo $\mathbb{Q}(\sqrt{-pq})$, pois u é par e $-pq \equiv 1(mod\ 4)$.

Ainda, se $\left(\frac{p}{q}\right) = 1$ podemos afirmar que existem corpos do tipo $\mathbb{Q}(\sqrt{-pq})$ que não admitem uma base integral ortogonal. Por exemplo, para $p = 11$ e $q = 5$ temos $pq \equiv 3(mod\ 4)$, e $\left(\frac{p}{q}\right) = 1$, (pois $1^2 \equiv 11(mod\ 5)$). Para estes valores temos a unidade fundamental $\epsilon = 89 + 12\sqrt{pq}$, em $\mathbb{Q}(\sqrt{pq})$. Então pelo Teorema 2.7 não existe uma base integral ortogonal no corpo $\mathbb{Q}(\sqrt{-pq})$, pois u é ímpar.

Teorema 2.13. Sejam p, q e r números primos tais que $pqr \equiv 3(mod\ 4)$ e $\epsilon = u + v\sqrt{pqr}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{pqr})$. Se $\left(\frac{pq}{r}\right) = -1$, $\left(\frac{pr}{q}\right) = -1$, $\left(\frac{qr}{p}\right) = -1$ e se ocorrer uma das condições:

(i)
$$\left(\frac{p}{q}\right) = -1 \text{ e } \left(\frac{p}{r}\right) = -1,$$

(ii)
$$\left(\frac{q}{p}\right) = -1 \text{ e } \left(\frac{q}{r}\right) = -1,$$

(iii)
$$\left(\frac{r}{p}\right) = -1 \text{ e } \left(\frac{r}{q}\right) = -1,$$

então u é par.

Demonstração:

Temos $N\epsilon = u^2 - pqrv^2 = 1$, onde $u, v > 0$. Podemos assumir que $p \equiv 1(mod\ 4)$, $q \equiv 1(mod\ 4)$ e $r \equiv 3(mod\ 4)$. Suponhamos que u é ímpar. Então v é par, isto é, $u = 2u_1 + 1$ e $v = 2v_1$. De $u^2 - pqrv^2 = 1$ segue que

$u^2 - 1 = pqrv^2$, logo $(u+1)(u-1) = pqrv^2$. Substituindo obtemos $(2u_1 + 1 + 1)(2u_1 + 1 - 1) = 4pqrv_1^2$ o que implica $(2u_1 + 2)(2u_1) = 4pqrv_1^2$. Então $4u_1^2 + 4u_1 = 4pqrv_1^2$, ou seja, $u_1(u_1 + 1) = pqrv_1^2$. Novamente como u_1 e $u_1 + 1$ são primos entre si temos as oito possibilidades:

(i) $u_1 + 1 = pqrx^2$ e $u_1 = y^2$,

(ii) $u_1 + 1 = x^2$ e $u_1 = pqry^2$,

(iii) $u_1 + 1 = pqx^2$ e $u_1 = ry^2$,

(iv) $u_1 + 1 = prx^2$ e $u_1 = qy^2$,

(v) $u_1 + 1 = qrx^2$ e $u_1 = py^2$,

(vi) $u_1 + 1 = px^2$ e $u_1 = qry^2$,

(vii) $u_1 + 1 = qx^2$ e $u_1 = pry^2$,

(viii) $u_1 + 1 = rx^2$ e $u_1 = pqy^2$,

onde x, y são inteiros positivos de diferentes paridades e $xy = v_1$. Subtraindo obtemos:

Em (i) é impossível módulo 4. De (i) segue que $y^2 + 1 = pqrx^2$ que implica $pqrx^2 - y^2 = 1$. Assim, temos dois casos a considerar: quando x é par e y é ímpar e quando x é ímpar e y é par. Do primeiro caso temos $-2 \equiv 0(mod\ 4)$ e do segundo caso temos $2 \equiv 0(mod\ 4)$, ambos absurdo.

De (ii): $x^2 - pqry^2 = 1$ obtemos $N(x + y\sqrt{pqr}) = 1$, então pela minimalidade de u temos $u \leq x \leq v_1 \leq u_1 < u$, o que é uma contradição.

De (iii): $ry^2 + 1 = pqx^2$ implica $pqx^2 - ry^2 = 1$ então $pqx^2 \equiv 1(mod\ r)$. Disto segue que $p^2q^2x^2 \equiv pq(mod\ r)$, logo pq é um resíduo quadrático módulo r, contrariando o fato de que $(\frac{pq}{r}) = -1$.

De (iv): $qy^2 + 1 = prx^2$ implica $prx^2 - qy^2 = 1$ então $prx^2 \equiv 1(mod\ q)$. Disto segue que $p^2r^2x^2 \equiv pr(mod\ q)$. Logo pr é um resíduo quadrático módulo q, contrariando o fato de que $\left(\frac{pr}{q}\right) = -1$.

De (v): $py^2 + 1 = qrx^2$ implica $qrx^2 - py^2 = 1$ então $qrx^2 \equiv 1(mod\ p)$. Disto segue que $q^2r^2x^2 \equiv qr(mod\ p)$, contrariando o fato de que $\left(\frac{qr}{p}\right) = -1$.

De (vi): $qry^2 + 1 = px^2$ implica $px^2 - qry^2 = 1$ então $px^2 \equiv 1(mod\ q)$ ou $px^2 \equiv 1(mod\ r)$. Disto segue que $p^2x^2 \equiv p(mod\ q)$ ou $p^2x^2 \equiv p(mod\ r)$. Logo

p é um resíduo quadrático módulo q ou p é um resíduo quadrático módulo r, contrariando o fato de que $\left(\frac{p}{q}\right) = -1$ e $\left(\frac{p}{r}\right) = -1$.

De (vii): $pry^2 + 1 = qx^2$ implica $qx^2 - pry^2 = 1$ então $qx^2 \equiv 1(mod\ p)$ ou $qx^2 \equiv 1(mod\ r)$. Disto segue que $q^2x^2 \equiv q(mod\ p)$ ou $q^2x^2 \equiv q(mod\ r)$. Logo q é um resíduo quadrático módulo p ou q é um resíduo quadrático módulo r, contrariando o fato de que $\left(\frac{q}{p}\right) = -1$ e $\left(\frac{q}{r}\right) = -1$.

De (viii): $pqy^2 + 1 = rx^2$ implica $rx^2 - pqy^2 = 1$ então $rx^2 \equiv 1(mod\ p)$ ou $rx^2 \equiv 1(mod\ q)$. Disto segue que $r^2x^2 \equiv r(mod\ p)$ ou $r^2x^2 \equiv r(mod\ q)$. Logo r é um resíduo quadrático módulo p ou r é um resíduo quadrático módulo q, contrariando o fato de que $\left(\frac{r}{p}\right) = -1$ e $\left(\frac{r}{q}\right) = -1$. Logo u é par, como queríamos demonstrar. □

Generalizando o Teorema anterior para um número finito de primos distintos obtivemos o Corolário:

Corolário 2.14. Sejam $p_1, p_2, \ldots, p_n$ números primos, $p_1p_2 \ldots p_n \equiv 3(mod\ 4)$, seja $\epsilon = u + v\sqrt{p_1p_2 \cdots p_n}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{p_1p_2 \cdots p_n})$. Se $(\frac{\prod_{i=1, i\neq j}^{s} p_i}{p_j}) = -1$, para $s = 1, 2, \ldots, n-1$ então u é par.

Demonstração:

A demonstração é análoga à demonstração do Teorema 2.13. □

2.2 Exemplos

Para melhor entender os resultados aqui apresentados daremos alguns exemplos da existência ou não de uma base integral ortogonal para o anel de inteiros de corpos quadráticos imaginários.

Seja $d \equiv 1(mod\ 4)$. Para alguns d em questão serão dados:

$$-d, \quad (\Delta', \Delta''), \quad (x, y)$$

satisfazendo

$$x^2\Delta' + y^2\Delta'' = 2$$

e uma base integral ortogonal

$$\{\beta_1, \beta_2\} = \{p + qw, r + sw\}.$$

Como $d = -(\Delta'\Delta'')$ podemos sempre assumir $\Delta'' < 0$.

(a) $d = -3$.

Seja $\varepsilon = u + v\sqrt{a}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{a})$ onde $a = -d = 3$. (Então $a \equiv 3(mod\ 4)$). De $N\varepsilon = u^2 - 3v^2 = 1$ encontramos $u = \pm 2$ e $v = \pm 1$, ou seja, u é par. Então a unidade fundamental do corpo $\mathbb{Q}(\sqrt{3})$ é $\varepsilon = 2 + \sqrt{3}$. Logo, pelo Teorema 2.7 existe uma base integral ortogonal em $\mathbb{Q}(\sqrt{-3})$.

Agora calculemos a base integral ortogonal.

Pelo Teorema 2.4 temos que $\Delta'\Delta'' = -3$ o que implica que $\Delta' > 0$ e $\Delta'' < 0$. Logo $\Delta' = 3$ e $\Delta'' = -1$ ou então $\Delta' = 1$ e $\Delta'' = -3$. Temos dois casos a analisar:

(i) $(\Delta', \Delta'') = (1, -3)$. Pelo Teorema 2.4 segue que $x^2 - 3y^2 = 2$. Como $x^2 \equiv 2(mod\ 3)$ não admite solução, então $x^2 - 3y^2 = 2$ não admite solução em $\mathbb{Z}$.

(ii) $(\Delta', \Delta'') = (3, -1)$. Pelo Teorema 2.4 segue que $3x^2 - y^2 = 2$ admite a solução $(x, y) = (1, 1)$.

Ainda, pelo Teorema 2.4 temos $p = \dfrac{\Delta' x - y}{2}$ e $q = y$. Substituindo os valores de x, y e Δ' obtemos $p = 1$ e $q = 1$. Assim utilizando as equações 2.1.1 e 2.1.2 obtemos $r = 0$ e $s = 1$. Portanto, $\{\beta_1, \beta_2\} = \{p+qw, r+sw\} = \{1+w, w\}$, onde $w = \dfrac{1 + \sqrt{-3}}{2}$.

(b) $d = -11$.

Seja $\varepsilon = u + v\sqrt{a}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{a})$ onde $a = -d = 11$, $(a \equiv 3(mod\ 4))$. De $N\varepsilon = u^2 - 11v^2 = 1$ encontramos $u = \pm 10$ e $v = \pm 3$, ou seja, u é par. Então a unidade fundamental do corpo $\mathbb{Q}(\sqrt{11})$ é $\varepsilon = 10 + 3\sqrt{11}$. Logo, pelo Teorema 2.7 existe uma base integral ortogonal em $\mathbb{Q}(\sqrt{-11})$.

Calculemos agora a base integral ortogonal.

Pelo Teorema 2.4 temos que $\Delta'\Delta'' = -11$ que implica $\Delta' > 0$ e $\Delta'' < 0$. Logo $\Delta' = 11$ e $\Delta'' = -1$ ou então $\Delta' = 1$ e $\Delta'' = -11$. Temos dois casos a analisar:

(i) $(\Delta', \Delta'') = (1, -11)$. Pelo Teorema 2.4 segue que $x^2 - 11y^2 = 2$. Como

$x^2 \equiv 2(mod\ 11)$ não admite solução, então $x^2 - 11y^2 = 2$ não admite solução em $\mathbb{Z}$.

(ii) $(\Delta', \Delta'') = (11, -1)$. Pelo Teorema 2.4 segue que $11x^2 - y^2 = 2$ admite a solução $(x, y) = (1, 3)$.

Ainda, pelo Teorema 2.4 temos $p = \dfrac{\Delta' x - y}{2}$ e $q = y$. Substituindo os valores obtidos de x, y e Δ' obtemos $p = 4$ e $q = 3$. Assim utilizando as equações 2.1.1 e 2.1.2 obtemos $r = 1$ e $s = 1$. Portanto, $\{\beta_1, \beta_2\} = \{p + qw, r + sw\} = \{4 + 3w, 1 + w\}$, onde $w = \dfrac{1 + \sqrt{-11}}{2}$.

Veremos que para $d = -39$ não existe uma base integral ortogonal.

(c) $d = -39$.

Seja $\varepsilon = u + v\sqrt{a}$ a unidade fundamental do corpo $\mathbb{Q}(\sqrt{a})$ onde $a = -d = 39$, $(a \equiv 3(mod\ 4))$, então $N\varepsilon = u^2 - 39v^2 = 1$ então $u = \pm 25$ e $v = \pm 4$, ou seja, u é ímpar. Então a unidade fundamental do corpo $\mathbb{Q}(\sqrt{39})$ é $\varepsilon = 25 + 4\sqrt{39}$. Logo, pelo Teorema 2.7 não existe uma base integral ortogonal em $\mathbb{Q}(\sqrt{-39})$.

Outra maneira de verificar que não existe uma base integral ortogonal é provar que a equação $\Delta' x^2 + \Delta'' y^2 = 2$ não admite solução em $\mathbb{Z}$. De fato, pelo Teorema 2.4 temos que $\Delta'\Delta'' = -39$ que implica $\Delta' > 0$ e $\Delta'' < 0$. Logo temos quatro casos a analisar:

(i) $(\Delta', \Delta'') = (1, -39)$. Pelo Teorema 2.4 segue que $x^2 - 39y^2 = 2$. Como $x^2 \equiv 2(mod\ 13)$ não admite solução, então $x^2 - 39y^2 = 2$ não admite solução em $\mathbb{Z}$.

(ii) $(\Delta', \Delta'') = (39, -1)$. Pelo Teorema 2.4 segue que $39x^2 - y^2 = 2$. Como $-y^2 \equiv 2(mod\ 13)$ não admite solução, então $39x^2 - y^2 = 2$ não admite solução em $\mathbb{Z}$.

(iii) $(\Delta', \Delta'') = (3, -13)$. Pelo Teorema 2.4 segue que $3x^2 - 13y^2 = 2$, o que implica $3x^2 \equiv 2(mod\ 13)$. Multiplicando por 9 temos $x^2 \equiv 5(mod\ 13)$, o qual não admite solução. Assim $3x^2 - 13y^2 = 2$ não admite solução em $\mathbb{Z}$.

(iv) $(\Delta', \Delta'') = (13, -3)$. Pelo Teorema 2.4 segue que $13x^2 - 3y^2 = 2$, o que implica $13x^2 \equiv 2(mod\ 3)$. Daí $x^2 \equiv 2(mod\ 3)$, o qual não admite solução.

Assim $13x^2 - 3y^2 = 2$ não admite solução em $\mathbb{Z}$.

Observação 2.15. Não conhecemos qualquer corpo cúbico com uma base integral ortogonal.

2.3 Corpos Biquadráticos

Baseando nos resultados anteriores é fácil dar exemplos de corpos biquadráticos cujos anéis de inteiros admitem bases integrais ortogonais relativamente à forma traço.

Fixemos a seguinte notação: Para $j = 1, 2$, seja $\mathrm{K}_j = \mathbb{Q}(\sqrt{d_j})$ o corpo de número quadrático de discriminante d_j, ou seja, $d_j \equiv 1(mod\ 4)$, e $d_1 \neq d_2$. Então $\mathrm{K} = \mathrm{K}_1\mathrm{K}_2$ é um *corpo biquadrático*. Suponha que $\{\beta_1^j,\ \beta_2^j\}$ é uma base integral de K_j, e considere o conjunto

$$B = \{\beta_i^1.\beta_k^2 : 1 \leq i, k \leq 2\}.$$

Vamos demonstrar que nesta situação B é uma base integral para K.

Em geral é muito difícil o cálculo de uma base integral para um corpo de números, e como a definição de discriminante envolve a princípio o conhecimento de uma base integral espera-se que o discriminante também seja difícil de se calcular. No entanto existe um Teorema devido a Hilbert, cuja demonstração envolve a teoria analítica de números, (Fórmula Condutor Discriminante), que determina o discriminante de alguns corpos sem ter a necessidade de conhecer qualquer base integral do corpo de números em questão. Com isto em mente temos:

Teorema 2.16. Para $j = 1, 2$ sejam $K_j = \mathbb{Q}(\sqrt{d_j})$, $d_j \equiv 1(mod\ 4)$ e $d_1 \neq d_2$. Se $mdc(d_1, d_2) = 1$, então o discriminante de $\mathrm{K} = \mathrm{K}_1\mathrm{K}_2$ é igual a $(d_1.d_2)^2$ e B é uma base integral de K.

Demonstração:

Que o discriminante de K é $(d_1.d_2)^2$ segue do Teorema de Hilbert (Veja [H], Teorema 88).

Para demonstrar que B é uma base integral, primeiramente note que se $Gal(\mathrm{K}_1, \mathbb{Q}) = \{1, \sigma_1\}$ e $Gal(\mathrm{K}_2, \mathbb{Q}) = \{1, \sigma_2\}$ então $Gal(\mathrm{K}_1\mathrm{K}_2, \mathbb{Q})$ é isomorfo a $\{1, \sigma_1\} \times \{1, \sigma_2\}$. Como $d_j \equiv 1 (mod\ 4)$, $j = 1, 2$ então $\beta_1 = \{1, \frac{1}{2} + \frac{1}{2}\sqrt{d_1}\}$ e $\beta_2 = \{1, \frac{1}{2} + \frac{1}{2}\sqrt{d_2}\}$ são bases integrais de K_1 e K_2, respectivamente. Assim $B = \beta_1\beta_2 = \{1,\ \frac{1}{2}(1+\sqrt{d_1}),\ \frac{1}{2}(1+\sqrt{d_2}),\ \frac{1}{4}(1+\sqrt{d_1}+\sqrt{d_2}+\sqrt{d_1d_2})\}$ e o discriminante de B é

$$\Delta[B] = \begin{vmatrix} 1 & \frac{1}{2}(1+\sqrt{d_1}) & \frac{1}{2}(1+\sqrt{d_2}) & \frac{1}{4}(1+\sqrt{d_1}+\sqrt{d_2}+\sqrt{d_1d_2}) \\ 1 & \frac{1}{2}(1-\sqrt{d_1}) & \frac{1}{2}(1+\sqrt{d_2}) & \frac{1}{4}(1-\sqrt{d_1}+\sqrt{d_2}-\sqrt{d_1d_2}) \\ 1 & \frac{1}{2}(1+\sqrt{d_1}) & \frac{1}{2}(1-\sqrt{d_2}) & \frac{1}{4}(1+\sqrt{d_1}-\sqrt{d_2}-\sqrt{d_1d_2}) \\ 1 & \frac{1}{2}(1-\sqrt{d_1}) & \frac{1}{2}(1-\sqrt{d_2}) & \frac{1}{4}(1-\sqrt{d_1}-\sqrt{d_2}+\sqrt{d_1d_2}) \end{vmatrix}^2 =$$

$$= \left(\frac{1}{2}.\frac{1}{2}.\frac{1}{4}\right)^2 \begin{vmatrix} 1 & 1+\sqrt{d_1} & 1+\sqrt{d_2} & 1+\sqrt{d_1}+\sqrt{d_2}+\sqrt{d_1d_2} \\ 1 & 1-\sqrt{d_1} & 1+\sqrt{d_2} & 1-\sqrt{d_1}+\sqrt{d_2}-\sqrt{d_1d_2} \\ 1 & 1+\sqrt{d_1} & 1-\sqrt{d_2} & 1+\sqrt{d_1}-\sqrt{d_2}-\sqrt{d_1d_2} \\ 1 & 1-\sqrt{d_1} & 1-\sqrt{d_2} & 1-\sqrt{d_1}-\sqrt{d_2}+\sqrt{d_1d_2} \end{vmatrix}^2 =$$

$$= \left(\frac{1}{16}\right)^2 \begin{vmatrix} 1 & 1+\sqrt{d_1} & 1+\sqrt{d_2} & 1+\sqrt{d_1}+\sqrt{d_2}+\sqrt{d_1 d_2} \\ 0 & -2\sqrt{d_1} & 0 & -2(\sqrt{d_1}+\sqrt{d_1 d_2}) \\ 0 & 0 & -2\sqrt{d_2} & -2(\sqrt{d_2}+\sqrt{d_1 d_2}) \\ 0 & -2\sqrt{d_1} & -2\sqrt{d_2} & -2(\sqrt{d_1}+\sqrt{d_2}) \end{vmatrix}^2 =$$

$= \left(\frac{1}{16}\right)^2 (16 d_1 d_2)^2 = (d_1 d_2)^2$. Como $B \subset \mathcal{D}_{\mathrm{K}}$ e é linearmente independente e $\Delta[B] = \delta(\mathrm{K})$ segue que B é uma base integral de K. □

Para o teorema seguinte vamos usar as seguintes notações: $Tr_j = Tr_{\mathrm{K}_j/\mathbb{Q}}$, $Tr_{j'} = Tr_{\mathrm{K}/\mathrm{K}_j}$ e $Tr = Tr_{\mathrm{K}/\mathbb{Q}}$.

Teorema 2.17. Para $j = 1,\ 2$ sejam $\mathrm{K}_j = \mathbb{Q}(\sqrt{d_j})$, $d_j \equiv 1 (mod\ 4)$ e $\{\beta_1^j, \beta_2^j\}$ uma base integral ortogonal de K_j. Então B é ortogonal com respeito a forma traço $b(x,y) = Tr(xy)$. Além disso, se $mdc(d_1, d_2) = 1$ então B é uma base integral ortogonal de K.

Demonstração:

Sejam $i,k,l,m \in \{1,2\}$. Desde que $Tr = Tr_1 \circ Tr_{1'}$, $Tr_{1'|\mathrm{K}_2} = Tr_2$ e $Tr_{1'}$ é K_1- linear , então

$$Tr(\beta_i^{(1)}\beta_k^{(2)} \cdot \beta_l^{(1)}\beta_m^{(2)}) = Tr_1\left(Tr_{1'}(\beta_i^{(1)}\beta_l^{(1)} \cdot \beta_k^{(2)}\beta_m^{(2)})\right) =$$
$$= Tr_1\left(\beta_i^{(1)}\beta_l^{(1)} \cdot Tr_{1'}(\beta_k^{(2)}\beta_m^{(2)}\right) = Tr_1\left(\beta_i^{(1)}\beta_l^{(1)} \cdot Tr_2(\beta_k^{(2)}\beta_m^{(2)})\right) =$$
$$= Tr_1(\beta_i^{(1)}\beta_l^{(1)}) \cdot Tr_2(\beta_k^{(2)}\beta_m^{(2)}) = 0,$$

a menos que $i = l$ e $k = m$. Assim B é ortogonal com respeito a forma traço. O resto da demonstração segue do Teorema anterior. □

Observação 2.18. Também não sabemos se existe uma base integral ortogonal em um corpo biquadrático que não satisfaz as hipóteses do Teorema 2.17.

BIBLIOGRAFIA

[BE] BRUMATTI, P.; ENGLER, A. *Inteiros quadráticos e o grupo de classes.* Rio de Janeiro: IMPA, 2001. (Colóquio Brasileiro de Matemática; 23).

[D] DABROWSKA, A.; Diagonalizing the trace form in some number fields, *Ann.Math.Sil*, v.15, p.17-26, 2001.

[H] D. HILBERT, Die theorie der algebraischen Zahkörper, *Jahresber, Deutsch. Math Verein*, v.4, p.175-546, 1897.

[ST] STEWART, I.; Tall, D.; *Algebric Number Theory.* London: Chapman & Hall, 1987.


cm 1 2 3 4 5 6 7
unesp
11 12 13 14 15 16 17 18