unesp UNIVERSIDADE ESTADUAL PAULISTA
IBILCE - Câmpus São José do Rio Preto

Forma Traço Sobre Algumas Extensões Galoisianas de Corpos p-Ádicos

Janete do Prado

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
Fevereiro - 2005

"Mestre não é quem sempre ensina,
mas quem de repente aprende."

Guimarães Rosa

Ao meu noivo,
Danilo

dedico.

Agradecimentos

Ao concluir este trabalho agradeço:

A Deus.

A Danilo Carlos da Graça Silva, meu noivo, que desde o princípio me incentivou a concluir mais esta etapa da minha vida, me dando força e muito amor.

Aos meus pais e aos meus irmãos por sempre estarem ao meu lado.

Ao Prof. Dr. Clotilzio Moreira dos Santos, pela paciência, amizade, dedicação e orientação.

À banca examinadora.

Aos colegas da pós-graduação que estiveram ao meu lado nos momentos difíceis, em especial a amiga Raffaela Raposo Palmieri.

Aos professores do Departamento de Matemática do IBILCE - UNESP que de alguma forma contribuíram para este trabalho.

Aos professores da graduação, da FCT - UNESP, por terem auxiliado no meu processo de aprendizagem.

À CAPES por parte do apoio financeiro.

Resumo

Seja K um corpo p-ádico, com $p \neq 2$ e F $\supset$ K uma extensão galoisiana de K de grau n. Então F pode ser visto como espaço quadrático sobre K, com a forma quadrática dada por $\mathrm{T}(x) = tr_{\mathrm{F|K}}(x^2)$, para $x \in$ F. Determinaremos os invariantes determinante, dimensão e invariante de Hasse desta forma quadrática para n igual a 2,3 e 4.

Palavras-chave: Forma Quadrática, Forma Traço, Invariante de Hasse, Corpos p-Ádicos.

Abstract

Let K be a p-adic field with $p \neq 2$ and F a Galois extension field of K of degree n. Then F can be viewed as a quadratic space over K under the quadratic form $\mathrm{T}(x) = tr_{\mathrm{F|K}}(x^2)$ for $x \in \mathrm{F}$. The invariants of this quadratic form dimension, determinant and Hasse invariant are given in the case when n is equal to 2,3 and 4.

Keywords: Quadratic Form, Trace Form, Hasse Invariant, p-Adic Field.

Índice de Símbolos

p: primo

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

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

$\mathbb{Q}_p$: o corpo p-ádico

K, F, L: corpos

$\mathbb{K}_q$: corpo finito

$\frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$: grupo das classes de quadrados de K

V: espaço vetorial

V^*: espaço dual

q: forma quadrática

(V, q): espaço quadrático

$d(q)$ ou $det(q)$: determinante da forma quadrática q

$\mathrm{D}(q)$: conjunto dos elementos de $\dot{\mathrm{K}}$ representados por q

$\prod$: produtório

$\sum$: somatório

(a_{ij}): matriz

$det(\mathrm{A})$: determinante da matriz A

Ker: núcleo

$\mathbb{H}$: plano hiperbólico

$\simeq$: isometria

$\approx$: isomorfismo

$Z(\mathrm{A})$: centro da álgebra A

$\mathrm{M}_n(\mathrm{K})$: álgebra de matrizes de ordem n sobre K

A_0: conjunto dos quatérnios puros

T: forma traço

N: forma norma

A^{op}: álgebra oposta

$Br(\mathrm{K})$: grupo de Brauer de K

$s(q)$: invariante de Hasse da forma quadrática q

v: valorização

A_v: anel de valorização de K

$\mathcal{U}$: grupo das unidades

u: unidade

$\mathcal{P}$: ideal

δK ou Δ(K): discriminante do corpo K

[L : K]: grau de L sobre K

$f_x(X)$: polinômio característico de x

Sumário

Introdução

Os primeiros capítulos são constituídos de tópicos fundamentais, que servem de base para este trabalho. O Capítulo 1, consiste em um estudo sobre formas quadráticas sobre corpos, e alguns de seus invariantes.

Nos capítulos 2 e 3 foram vistos resultados importantes de álgebra de quatérnios, e feito uma introdução ao grupo de Brauer para que fosse possível definir o invariante de Hasse.

No capítulo 4 há um resumo sobre corpos locais, em especial os corpos p-ádicos, que são os corpos sobre os quais estudaremos a forma traço no capítulo 5. Aqui provamos que duas formas quadráticas são isométricas se, e somente se, elas tem a mesma dimensão, determinante e invariante de Hasse.

O capítulo 5 é o foco principal deste trabalho. Nele determinamos os invariantes da forma traço sobre os corpos p-ádicos, baseado na referência [G]. Particularmente a dimensão da forma traço é o grau da extensão $\mathrm{F} \supset \mathbb{Q}_p$; o determinante da forma traço é o discriminante da extensão $\mathrm{F} \supset \mathbb{Q}_p$, e finalmente para determinar o invariante de Hasse da forma traço basta provar se ele é ou não é representado pela única álgebra de quatérnios com divisão sobre o corpo p-ádico $\mathbb{Q}_p$.

Capítulo 1

Formas Quadráticas

Consideraremos em todo este trabalho, K um corpo com característica diferente de 2 e $\dot{\mathrm{K}}$ o grupo multiplicativo dos elementos não nulos de K.

Uma *forma bilinear simétrica* sobre V é uma aplicação $b : \mathrm{V} \times \mathrm{V} \longrightarrow \mathrm{K}$ (onde V é um espaço vetorial de dimensão finita sobre K) que satisfaz as propriedades:

- $b(x+y,z) = b(x,z) + b(y,z)$, para todos $x,\ y,\ z \in \mathrm{V}$;
- $b(\alpha x, y) = \alpha b(x,y) = b(x, \alpha y)$, para todos $x,\ y \in \mathrm{V}$ e $\alpha \in \mathrm{K}$;
- $b(x,y) = b(y,x)$, para todos $x, y \in \mathrm{V}$.

Um *espaço bilinear* é um par (V, b) onde V é um espaço vetorial de dimensão finita sobre K e b é uma forma bilinear simétrica sobre V.

Definição 1.0.1 *Um espaço quadrático é um par* (V, q)*, onde* V *é um espaço vetorial de dimensão finita sobre* K *e* q *é uma forma quadrática sobre* V*, ou seja,* q *é uma função de* V *em* K *que satisfaz as propriedades:*

- $q(\alpha x) = \alpha^2 q(x)$ *para todo* $x \in \mathrm{V}$ *e para todo* $\alpha \in \mathrm{K}$*, e;*
- $b_q : \mathrm{V} \times \mathrm{V} \longrightarrow \mathrm{K}$ *definida por* $b_q(x,y) := \frac{1}{2}(q(x+y) - q(x) - q(y))$*, para todos* $x, y \in \mathrm{V}$*, é uma forma bilinear simétrica.*

A função b_q *definida acima é dita a forma bilinear associada à* q*.*

Nota: Dada uma forma bilinear (simétrica) b sobre um espaço vetorial V, podemos definir uma forma quadrática $q : \mathrm{V} \longrightarrow \mathrm{K}$ por $q(x) := b(x, x)$. De fato, a função q definida é uma forma quadrática dita *forma quadrática associada* à b.

É imediata a verificação de que as correspondências $q \longrightarrow b_q$ e $b \longrightarrow q_b$ (ou entre espaços quadráticos e bilineares, $(V, q) \longrightarrow (V, b_q)$ e $(V, b) \longrightarrow (V, q_b)$) são inversas uma da outra desde que $q_{b_q} = q$ e $b_{q_b} = b$. Em outras palavras, podemos identificar formas quadráticas com formas bilineares de modo único. Segue-se que conceitos e propriedades de espaços quadráticos (ou formas quadráticas) podem ser transmitidos para espaços bilineares (ou formas bilineares) e vice-versa. Um exemplo disto é o conceito de isometria que vem a seguir.

Definição 1.0.2 *Dizemos que os espaços quadráticos* (V, q) *e* (V', q') *são isométricos, e denotamos por* $(\mathrm{V}, q) \simeq (\mathrm{V}', q')$*, se existe um isomorfismo* $\sigma : \mathrm{V} \longrightarrow \mathrm{V}'$ *tal que* $q'(\sigma(x)) = q(x)$*, para todo* $x \in \mathrm{V}$.

Dois espaços bilineares (V, b) *e* (V', b') *são ditos isométricos e denotemos este fato por* $(\mathrm{V}, b) \simeq (\mathrm{V}', b')$*, se existe um isomorfismo* $\sigma : \mathrm{V} \longrightarrow \mathrm{V}'$*, tal que* $b'(\sigma(x), \sigma(y)) = b(x, y)$*, para todos* $x,\ y \in \mathrm{V}$. *O isomorfismo* $\sigma : \mathrm{V} \longrightarrow \mathrm{V}'$*, em ambos os casos, é dito uma isometria.*

Por simplicidade muitas vezes diremos que as formas quadráticas q *e* q' *(ou as duas formas bilineares* b *e* b'*) são isométricas.*

Segue-se da definição que dois espaços quadráticos (bilineares) isométricos tem a mesma dimensão. Também tem-se que a relação de isometria definida entre espaços quadráticos (bilineares) é uma relação de equivalência.

Agora podemos ver que se q e q' são formas quadráticas isométricas então suas formas bilineares associadas também são isométricas, e a recíproca também é verdadeira. De fato, seja $\sigma : \mathrm{V} \longrightarrow \mathrm{V}'$ um isomorfismo tal que $q'(\sigma(x)) = q(x)$. Então $b_{q'}(\sigma(x), \sigma(y)) = \frac{1}{2}[q'(\sigma(x) + \sigma(y)) - q'(\sigma(x)) - q'(\sigma(y))] = \frac{1}{2}[(q' \circ \sigma)(x + y) - (q' \circ \sigma)(x) - (q' \circ \sigma)(y)] = \frac{1}{2}[q(x + y) - q(x) - q(y)] = b_q(x, y)$, para quaisquer $x, y \in \mathrm{V}$. Logo $b_{q'} \simeq b_q$. Do mesmo modo demonstra-se que se $b \simeq b'$, então $q_b \simeq q_{b'}$.

1.1 Notação Matricial

Sejam $C = \{e_1, e_2, \ldots, e_n\}$ uma base do espaço vetorial V e $x = \sum_{i=1}^{n} x_i e_i$, $y = \sum_{j=1}^{n} y_j e_j \in$ V. Se b é uma forma bilinear sobre K, então

$$b(x,y) = b\left(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\right) = \sum_{i=1}^{n} x_i b\left(e_i, \sum_{j=1}^{n} y_j e_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j b(e_i, e_j).$$

A matriz $\mathrm{B} = (b(e_i, e_j)) = (b_{ij})$ é dita *matriz da forma bilinear* b com respeito à base C. Vamos denotá-la por B_{bC}. Deste modo, temos:

$$b(x,y) = (x_1\ x_2\ \ldots\ x_n)\begin{pmatrix} b(e_1,e_1) & \ldots & b(e_1,e_n) \\ \vdots & \ddots & \vdots \\ b(e_n,e_1) & \ldots & b(e_n,e_n) \end{pmatrix}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x^t \mathrm{B}_{bC} y.$$

A *matriz de uma forma quadrática* q, é definida como sendo a matriz da forma bilinear associada a q. Assim,

$$\mathrm{B}_{qC} := \mathrm{B}_{b_q C} \quad \text{e} \quad q(x) = b_q(x,x) = x^t \mathrm{B}_{b_q C} x.$$

Consideremos agora (V, q) e (V', q') dois espaços quadráticos isométricos e σ a isometria entre eles. Se C e C' são bases de V e V$'$ respectivamente e $\mathrm{T} = (t_{ij})$ a matriz de σ em relação as bases C e C', então

$$\mathrm{B}_{qC} = \mathrm{T}^t \mathrm{B}_{q'C'} \mathrm{T}, \qquad (*)$$

onde T^t é a matriz transposta de T.

Dada uma base C de V, se tomarmos uma outra base C' de V, teremos que $\mathrm{B}_{qC'} = \mathrm{T}^t \mathrm{B}_{qC} \mathrm{T}$, onde T é a matriz de mudança de base, de C para C'.

Como o determinante de uma matriz quadrada é uma função multiplicativa e é invariante por transposição de matrizes temos que

$$det\mathrm{B}_{qC} = (det\mathrm{T})^2 . det\mathrm{B}_{q'C'}. \qquad (**)$$

Podemos dizer, então, que o determinante de formas quadráticas isométricas diferem por um fator quadrado de $\dot{\mathrm{K}}$. Vamos denotar por $\dot{\mathrm{K}}^2$ o seguinte subgrupo normal de $\dot{\mathrm{K}}$, $\dot{\mathrm{K}}^2 :=$

$\{x^2,\ x \in \dot{\mathrm{K}}\}$. Então $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$ é um grupo dito *grupo das classes de quadrados*. Este grupo tem papel fundamental na teoria de formas quadráticas. Isto nos permite definir o determinante de uma forma quadrática q como sendo um determinado elemento de $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$,

Definição 1.1.1 *Seja* $q : \mathrm{V} \longrightarrow \mathrm{K}$ *uma forma quadrática e* C *uma base fixa de* V. *Definimos o determinante de* q *ou o determinante do espaço quadrático* (V, q) *e denotemos por* $d(q)$ *ou* $det(q)$, *como sendo*

$$d(q) := det\mathrm{B}_{qC}.\dot{\mathrm{K}}^2.$$

Por (**) tem-se que o determinante de uma forma quadrática (ou de um espaço quadrático) está bem definido como elemento de $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$, e de (*) temos que o determinante de formas quadráticas é um invariante por isometrias.

1.2 Espaços Regulares e Decomposição Ortogonal

Definição 1.2.1 *Seja* (V, b) *um espaço bilinear. Dois vetores* $x, y \in \mathrm{V}$ *são ortogonais se* $b(x, y) = 0$. *Além disso,* $\mathrm{X}, \mathrm{Y} \subset \mathrm{V}$ *são ditos ortogonais se* $b(x, y) = 0$, *para todo* $x \in \mathrm{X}$ *e para todo* $y \in \mathrm{Y}$.

Notações*:* $x \perp y$, $\mathrm{X} \perp \mathrm{Y}$. *Trocando* b *por* b_q *define-se analogamente vetores ortogonais e subconjuntos ortogonais do espaço quadrático* (V, q).

Se X é um conjunto não vazio de V ((V, b): espaço bilinear), o *subespaço ortogonal* de X, denotado por $\mathrm{X}^{\perp}$, é definido por:

$$\mathrm{X}^{\perp} := \{y \in \mathrm{V} \mid b(x, y) = 0, \quad \text{para todo } x \in \mathrm{X}\}.$$

Com relação à definição acima, temos que $\mathrm{X}^{\perp}$ é, de fato, um subespaço de V, e ainda temos as propriedades:

- se $\mathrm{X} \subset \mathrm{Y}$ então $\mathrm{Y}^{\perp} \subset \mathrm{X}^{\perp}$;
- $\mathrm{X} \subset \mathrm{X}^{\perp\perp}$.

Se W é um subespaço de V, onde (V, q) é um espaço quadrático, então $(\mathrm{W}, q_{\mathrm{W}})$ (q_{W} a restrição de q a W) é um espaço quadrático dito *subespaço quadrático* de (V, q). Também diz-se que q_{W} é uma *subforma* da forma quadrática q.

Definição 1.2.2 *Um espaço quadrático* (V, q) *(ou uma forma quadrática* q*) é dito regular (ou não singular), se* $\mathrm{V}^{\perp} = \{0\}$*, isto é, para cada vetor não nulo* x *existe* y *tal que* $b_q(x, y) \neq 0$*. O subespaço* $\mathrm{V}^{\perp}$ *é chamado de radical de* (V, q)*. Um subespaço* W *de* V *é dito regular se* $(\mathrm{W}, q_{\mathrm{W}})$ *é regular. Se* (V, q) *não é regular, ele é dito singular.*

Observação 1.2.1 *Num espaço regular, somente o vetor nulo é perpendicular à todos os vetores.*

Para um espaço vetorial V, V^* denota seu espaço dual: o espaço vetorial de todos os funcionais lineares de V em K.

Se (V, b) é um espaço bilinear, então $\widehat{b} : \mathrm{V} \longrightarrow \mathrm{V}^*$ tal que $\widehat{b}(x) : \mathrm{V} \longrightarrow \mathrm{K}$ é definida por $\widehat{b}(x)(y) := b(x, y)$ é uma transformação linear, dita *transformação adjunta* de b.

Lema 1.2.1 *Sejam* (V, b) *um espaço bilinear e* W *um subespaço de* V*. Então* $\mathrm{W}^{\perp} = Ker(\rho\widehat{b})$*, onde* $\rho : \mathrm{V}^* \longrightarrow \mathrm{W}^*$ *denota a projeção canônica.*

Demonstração: Se $x \in \mathrm{W}^{\perp}$, então $\widehat{b}(x)(y) = b(x, y) = 0$, para todo $y \in \mathrm{W}$. Assim, $\widehat{b}(x)_{|\mathrm{W}} = 0$, e segue que $x \in Ker(\rho\widehat{b})$.

Agora seja $x \in Ker(\rho\widehat{b})$. Então $\widehat{b}(x)_{|\mathrm{W}} = 0$ ou $\widehat{b}(x)(y) = 0$, para todo $y \in \mathrm{W}$. Logo $b(x, y) = 0$, para todo $y \in \mathrm{W}$, ou seja $x \in \mathrm{W}^{\perp}$. □

Proposição 1.2.1 *As seguintes condições são equivalentes sobre um espaço quadrático* (V, q) :

(i) B_{qC} *é uma matriz não singular, qualquer que seja a base* C *de* V;

(ii) $x \longrightarrow \widehat{b_q}(x)(\cdot) = b_q(x, \cdot)$ *define um isomorfismo de* V *em* V^*;

(iii) *Se* $x \in \mathrm{V}$ *é tal que* $b_q(x, y) = 0$*, para todo* $y \in \mathrm{V}$*, então* $x = 0$*, isto é,* V *é regular.*

Demonstração: **(i)**$\Longrightarrow$ **(ii)** Seja C uma base de V e suponhamos que B_{qC} é uma matriz inversível. Sejam $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ as coordenadas dos vetores x e y de V na base C. Como B_{qC} é inversível, segue que $x^t\mathrm{B}_{qC} \neq y^t\mathrm{B}_{qC}$, para todo $x, y \in \mathrm{V}$, com $x \neq y$.

Logo $b_q(x,\cdot) \neq b_q(y,\cdot)$, para todo $x \neq y$ ou então $\widehat{b_q}(x) \neq \widehat{b_q}(y)$, quando $x \neq y$. Portanto $\widehat{b_q} : \mathrm{V} \longrightarrow \mathrm{V}^*$ definida por $\widehat{b_q}(x)(\cdot) = b_q(x,\cdot)$ é um isomorfismo.

(ii) $\Longrightarrow$ (iii) Seja $\begin{array}{rccc} \widehat{b_q}: & \mathrm{V} & \longrightarrow & \mathrm{V}^* \\ & x & \longmapsto & \widehat{b_q}(x)(\cdot) = b_q(x,\cdot) \end{array}$ um isomorfismo. Tomemos $x \in \mathrm{V}$ e suponhamos que $b_q(x,y) = 0$, para todo $y \in \mathrm{V}$. Isto implica que $\widehat{b_q}(x)(y) = 0$, para todo $y \in \mathrm{V}$. Logo $\widehat{b_q}(x) = 0$. Como $\widehat{b_q}$ é um isomorfismo, temos que $x = 0$. Portanto $\mathrm{V}^{\perp} = 0$, ou seja, V é regular.

(iii) $\Longrightarrow$ (i) Temos que $\mathrm{B}_{qC} = (b_{ij})$ é inversível $\Longleftrightarrow det\mathrm{B}_{qC} \neq 0$. Se $det\mathrm{B}_{qC} = 0$, então $\mathrm{B}_{qC}.y = 0$ tem solução não nula, ou seja, existe $y' = (y_1, \ldots, y_n) \in \mathrm{V}$, com $y_i \neq 0$ para algum i, tal que

$$\begin{cases} b_{11}y_1 + b_{12}y_2 + \ldots + b_{1n}y_n = 0 \\ \qquad\qquad\qquad\quad \vdots \\ b_{n1}y_1 + b_{n2}y_2 + \ldots + b_{nn}y_n = 0. \end{cases}$$

Assim, para todo $x = (x_1, \ldots, x_n) \in \mathrm{V}$ não nulo, $x^t\mathrm{B}_{qC}y' = 0$. Logo $y' \in \mathrm{V}^{\perp}$. Portanto $\mathrm{V}^{\perp} \neq \{0\}$ e assim (V, q) não é regular, o que contradiz a hipótese. □

Consideremos os espaços quadráticos (V_1, q_1), $(\mathrm{V}_2, q_2), \ldots, (\mathrm{V}_n, q_n)$, $n \geq 2$, e seja $\mathrm{V} = \mathrm{V}_1 \oplus \mathrm{V}_2 \oplus \cdots \oplus \mathrm{V}_n$. A aplicação $q : \mathrm{V} \longrightarrow \mathrm{K}$ definida por $q\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} q_i(x_i)$ é uma forma quadrática sobre K, pois:

$q\left(\alpha \sum x_i\right) = q\left(\sum \alpha.x_i\right) = \sum q_i(\alpha x_i) = \sum \alpha^2 q_i(x_i) = \alpha^2 \sum q_i(x_i) = \alpha^2 q\left(\sum x_i\right).$

E para a forma bilinear associada temos:

$b_q\left(\sum x_i, \sum y_i\right) = \frac{1}{2}\left[q\left(\sum x_i + \sum y_i\right) - q\left(\sum x_i\right) - q\left(\sum y_i\right)\right] =$

$\frac{1}{2}\left[q\left(\sum(x_i + y_i)\right) - q\left(\sum x_i\right) - q\left(\sum y_i\right)\right] = \sum\{\frac{1}{2}[(q_i(x_i + y_i) - q_i(x_i) - q_i(y_i)]\} = \sum b_{q_i}(x_i, y_i).$

Como cada uma das formas bilineres b_{q_i} é simétrica segue-se que b_q também é simétrica. Assim podemos definir:

Definição 1.2.3 *Dados os espaços quadráticos* (V_i, q_i), $i = 1, \ldots, n$ $(n \geq 2)$, *seja* $\mathrm{V} = \mathrm{V}_1 \oplus \mathrm{V}_2 \oplus \cdots \oplus \mathrm{V}_n$. *O par* (V, q), *onde* $q : \mathrm{V} \longrightarrow \mathrm{K}$ *é definida por* $q\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} q_i(x_i)$, *é um*

espaço quadrático denotado por $(\mathrm{V}, q) = (\mathrm{V}_1, q_1) \perp \ldots \perp (\mathrm{V}_n, q_n)$ *e é dito soma ortogonal dos espaços* $(\mathrm{V}_1, q_1), \ldots, (\mathrm{V}_n, q_n)$. *Esta soma ortogonal também será denotada resumidamente por* $q = q_1 \perp \ldots \perp q_n$, *e diz-se que* q *é uma soma ortogonal de* $q_1, \ldots, q_n$.

Nota: Segue-se que uma condição necessária e suficiente para que o espaço quadrático (V, q) seja a soma direta dos espaços quadráticos $(\mathrm{V}_1, q_1), \ldots, (\mathrm{V}_n, q_n)$ é que $\mathrm{V} = \mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_n$ e $\mathrm{V}_i \perp V_j$, para todos $i \neq j$.

De fato, como $b_q = \sum b_{q_i}$ temos que para $x_j \in \mathrm{V}_j$ e $x_k \in \mathrm{V}_k$, $j < k$, $b_q(x_j, x_k) = 0 + \cdots + 0 + b_{q_j}(x_j, 0) + 0 + \cdots + 0 + b_{q_k}(0, x_k) + 0 + \cdots + 0 = 0$. Logo $\mathrm{V}_j \perp \mathrm{V}_k$, se $j \neq k$.

Sejam (V, q) um espaço quadrático tal que $\mathrm{V} = \mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_n$ e $\mathrm{V}_i \perp V_j$, para todos $i \neq j$, e $q_i = q_{\mathrm{V}_i}$. É fácil verificar que (V_i, q_i) são espaços quadráticos para todo i. Segue que para todo $x = \sum_{i=1}^{n} x_i \in \mathrm{V}$, com $x_i \in \mathrm{V}_i$ temos que $q\left(\sum_{i=1}^{n} x_i\right) = b_q(x_1 + \cdots + x_n, x_1 + \cdots + x_n) = \sum_{i,j=1}^{n} b_q(x_i, x_j)$. Como $\mathrm{V}_i \perp \mathrm{V}_j$ temos $b_q(x_i, x_j) = 0$, para $i \neq j$. Assim $q\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} b_q(x_i, x_i) = \sum_{i=1}^{n} q(x_i) = \sum_{i=1}^{n} q_i(x_i)$.

Um caso particular de soma direta é quando V_i são subespaços de V ((V, q) um espaço quadrático), tais que $\mathrm{V}_i \perp \mathrm{V}_j$ e $\mathrm{V} = \oplus_{i=1}^{n} \mathrm{V}_i$ $(n > 1)$.

Temos que $(\mathrm{V}_i, q_{\mathrm{V}_i})$ são espaços quadráticos, e esta decomposição ortogonal é dita *soma direta ortogonal interna.*

Lema 1.2.2 *Sejam* (V_i, q_i) *espaços quadráticos,* $i = 1, 2, 3, 4$. *Então:*

(i) $(\mathrm{V}_1, q_1) \perp (\mathrm{V}_2, q_2) \simeq (\mathrm{V}_2, q_2) \perp (\mathrm{V}_1, q_1)$, *(ou* $q_1 \perp q_2 \simeq q_2 \perp q_1$*);*

(ii) *Se* $(\mathrm{V}_1, q_1) \simeq (\mathrm{V}_2, q_2)$ *e* $(\mathrm{V}_3, q_3) \simeq (\mathrm{V}_4, q_4)$, *então* $(\mathrm{V}_1, q_1) \perp (\mathrm{V}_3, q_3) \simeq (\mathrm{V}_2, q_2) \perp (\mathrm{V}_4, q_4)$;

(iii) $(\mathrm{V}_1, q_1) \perp (\mathrm{V}_2, q_2)$ *é regular se, e somente se,* (V_1, q_1) *e* (V_2, q_2) *são ambos regulares;*

(iv) *Se* B_1 *é a matriz de* q_1 *na base* C_1 *de* V_1 *e* B_2 *é a matriz de* q_2 *na base* C_2 *de* V_2, *então a soma ortogonal* $q_1 \perp q_2$ *tem a matriz* $\begin{pmatrix} \mathrm{B}_1 & 0 \\ 0 & \mathrm{B}_2 \end{pmatrix}$ *na base* $C_1 \cup C_2$ *de* $\mathrm{V}_1 \oplus \mathrm{V}_2$.

Observação 1.2.2 *Como o determinante de uma forma quadrática independe da base dada para expressá-la e desde que* $det \begin{pmatrix} \mathrm{B}_1 & 0 \\ 0 & \mathrm{B}_2 \end{pmatrix} = det(\mathrm{B}_1).det(\mathrm{B}_2)$, *segue que* $det(q_1 \perp q_2) =$

$det(q_1).det(q_2)$ como elemento de $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$.

Lema 1.2.3 *Se* W *é um subespaço regular do espaço quadrático* (V, q), *então* $(\mathrm{V}, q) \simeq (\mathrm{W}, q_{\mathrm{W}}) \perp (\mathrm{W}^{\perp}, q_{\mathrm{W}^{\perp}})$.

Demonstração: Como $\mathrm{W} \perp \mathrm{W}^{\perp}$, basta demonstrarmos que $\mathrm{V} = \mathrm{W} \oplus \mathrm{W}^{\perp}$.
O radical do espaço quadrático $(\mathrm{W}, q_{\mathrm{W}})$ é $\mathrm{W} \cap \mathrm{W}^{\perp}$, e como W é regular temos que $\mathrm{W} \cap \mathrm{W}^{\perp} = \{0\}$. Consideremos $\widehat{b_{(q_{\mathrm{W}})}} : \mathrm{W} \longrightarrow \mathrm{W}^*$ tal que $\widehat{b_{(q_{\mathrm{W}})}}(x)(\cdot) = b_{(q_{\mathrm{W}})}(x, \cdot)$. Como W é regular, pela Proposição 1.2.1 segue-se que $\widehat{b_{(q_{\mathrm{W}})}}$ é um isomorfismo.

Se $x \in \mathrm{V}$, temos que $\widehat{b_q}(x)_{\mathrm{W}} \in \mathrm{W}^*$ e como $\widehat{b_{(q_{\mathrm{W}})}}$ é um isomorfismo de W em W^*, existe $y \in \mathrm{W}$ tal que $\widehat{b_q}(x)_{\mathrm{W}} = \widehat{b_{(q_{\mathrm{W}})}}(y)$. Assim, $(\widehat{b_q}(x)_{\mathrm{W}})(z) = \widehat{b_{(q_{\mathrm{W}})}}(y)(z)$, para todo $z \in \mathrm{W}$. Daí $b_q(x, z) = b_{(q_{\mathrm{W}})}(y, z) = b_q(y, z)$, para todo $z \in \mathrm{W}$, ou $b_q(x - y, z) = 0$, para todo $z \in \mathrm{W}$. Logo $x - y \in \mathrm{W}^{\perp}$. Como $x = y + (x - y)$, segue-se que $\mathrm{V} = \mathrm{W} + \mathrm{W}^{\perp}$. Portanto $\mathrm{V} = \mathrm{W} \oplus \mathrm{W}^{\perp}$.

De $\mathrm{V} = \mathrm{W} \oplus \mathrm{W}^{\perp}$ temos que $\sigma : \mathrm{V} \longrightarrow \mathrm{W} \oplus \mathrm{W}^{\perp}$ definida por $\sigma(x) = x_1 + x_2$ (onde x_1 e x_2 são as projeções de x sobre W e $\mathrm{W}^{\perp}$, respectivamente), é um isomorfismo de V em V. Por definição de soma ortogonal temos que:
$(q_{\mathrm{W}} \perp q_{\mathrm{W}^{\perp}})(\sigma(x)) = (q_{\mathrm{W}} \perp q_{\mathrm{W}^{\perp}})(x_1 + x_2) = q_{\mathrm{W}}(x_1) + q_{\mathrm{W}^{\perp}}(x_2) \stackrel{\text{def}}{=} q(x_1) + q(x_2)$. Como $0 = 2b_q(x_1, x_2) = q(x_1 + x_2) - q(x_1) - q(x_2)$, segue-se que $(q_{\mathrm{W}} \perp q_{\mathrm{W}^{\perp}})(\sigma(x)) = q(x)$, $x = x_1 + x_2$. Logo σ é uma isometria e o lema está concluído. □

Teorema 1.2.1 *Seja* (V, q) *um espaço quadrático sobre* K. *Então* (V, q) *é isométrico a uma soma ortogonal de subespaços quadráticos unidimensionais. Em outras palavras,* V *tem uma base constituída de vetores dois a dois ortogonais (base ortogonal).*

Demonstração: (por indução em dimensão de V)

Se $b_q = 0$, qualquer decomposição de V na forma $\mathrm{V} = \mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_n$ com $dim\mathrm{V}_i = 1$ também é uma decomposição ortogonal.

Se $b_q \neq 0$, existem vetores $x, y \in \mathrm{V}$ tal que $b_q(x, y) \neq 0$. Como $b_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$, então existe $z \in \mathrm{V}$ tal que $q(z) \neq 0$, por exemplo, $z = x,\ y$ ou $x + y$.

Assim o subespaço unidimensional $\mathrm{W} = z\mathrm{K}$ é regular e pelo Lema 1.2.3, $(\mathrm{V}, q) \simeq (\mathrm{W}, q_{\mathrm{W}}) \perp (\mathrm{W}^{\perp}, q_{\mathrm{W}^{\perp}})$. Pela indução segue o resultado. □

Observação 1.2.3 *O Teorema 1.2.1 garante a existência de uma base ortogonal (ou seja, seus vetores são ortogonais, dois a dois)* $C = \{e_1, \ldots, e_n\}$ *de* V. *Assim, para todo* $x \in \mathrm{V}$, $x = \sum_{i=1}^{n} x_i e_i$ *e* $q(x) = b(x,x) = \sum_{i,j=1}^{n} x_i x_j b(e_i, e_j) = \sum_{i=1}^{n} b(e_i, e_i) x_i^2 = \sum_{i=1}^{n} q(e_i) x_i^2$. *Isto segue do fato de que a matriz de* q *na base* C *é uma matriz diagonal:*

$$\mathrm{B}_{qC} = \begin{pmatrix} b(e_1,e_1) & 0 & \cdots & 0 & 0 \\ 0 & b(e_2,e_2) & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & b(e_{n-1},e_{n-1}) & 0 \\ 0 & 0 & \cdots & 0 & b(e_n,e_n) \end{pmatrix}.$$

Segue-se também que toda matriz simétrica é congruente a uma matriz diagonal.

Denotando $q(e_i)$ *por* a_i *temos que para todo* $x = x_1e_1 + x_2e_2 + \cdots + x_ne_n$, $q(x) = a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$. *Esta forma é denotada por* $\langle a_1\rangle \perp \ldots \perp \langle a_n\rangle$ *ou resumidamente por* $\langle a_1, a_2, \ldots, a_n\rangle$, *e é dita uma diagonalização da forma* q. *Temos ainda a notação reduzida* $n\langle a\rangle$ *quando* $a_i = a$ *para todo* $i = 1, 2, \ldots, n$.

Assim toda forma quadrática q *é isométrica a uma forma quadrática diagonal.*

Lema 1.2.4 **(i)** *Se* θ *é uma permutação de* $1, \ldots, n$, *então* $\langle a_1, \ldots, a_n\rangle \simeq \langle a_{\theta(1)}, \ldots, a_{\theta(n)}\rangle$;

(ii) *Para* $b_i \in \dot{\mathrm{K}}$, $i = 1, 2, \ldots, n$, $\langle a_1, \ldots, a_n\rangle \simeq \langle a_1b_1^2, \ldots, a_nb_n^2\rangle$.

Demonstração: **(i)** O automorfismo de V obtido pela permutação θ dos vetores da base canônica é uma isometria.

(ii) Sejam $\sigma : \mathrm{V} \longrightarrow \mathrm{V}$ definida por $\sigma(x_1, \ldots, x_n) = (b_1x_1, \ldots, b_nx_n)$, e $b_{qC} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$ em alguma base C de V. Seja também $q = \langle a_1, \ldots, a_n\rangle$ e $q' = \langle a_1b_1^2, \ldots, a_nb_n^2\rangle$. Então a seguinte igualdade se verifica:

$q(\sigma(x)) = q(b_1x_1, \ldots, b_nx_n) = \sum_{i=1}^{n} a_i(b_ix_i)^2 = \sum_{i=1}^{n} (a_ib_i^2)x_i^2 = q'(x)$. Logo $q \simeq q'$. □

Observação 1.2.4 **(1)** *O ítem (ii) deste Lema nos permite considerar qualquer diagonalização de uma forma quadrática* q *tomando os elementos diagonais* a_i *em* $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$. *Logo podemos*

considerar todos os a_i livres de quadrados. Por exemplo a forma $q_1 = \langle 8, -4, 12\rangle$, sobre $\mathbb{Q}$ é isométrica a forma $q_2 = \langle 2, -1, 3\rangle$, cujos coeficientes são livres de quadrados. A mesma forma q_1 é isométrica a forma $q_3 = \langle 1, -1, 1\rangle$, sobre $\mathbb{R}$, pois todo número positivo em $\mathbb{R}$ é um quadrado, ou, $\dot{\mathbb{R}}^2 = \{x \in \mathbb{R} \mid x > 0\}$.

(2) *Se $q \simeq q' = \langle a_1, \ldots, a_n\rangle$ então $det(q) = det(q') = a_1 \ldots a_n.\dot{\mathrm{K}}^2$ e q é regular se, e somente se, todos os a_i's são não nulos.*

Lema 1.2.5 *Sejam (V, q) um espaço quadrático regular e W um subespaço de V. Então $dim\mathrm{W} + dim\mathrm{W}^{\perp} = dim\mathrm{V}$.*

Demonstração: Pelo Lema 1.2.1 sabemos que $\mathrm{W}^{\perp} = Ker(\rho\widehat{b_q})$, onde $\rho : \mathrm{V}^* \longrightarrow \mathrm{W}^*$ denota a projeção canônica. Como toda base de W pode ser completada à uma base de V é fácil verificar que ρ é sobrejetora. Logo $\rho \circ \widehat{b_q}$ é sobrejetora, e portanto $dim\mathrm{V} = dim(Ker(\rho \circ \widehat{b_q})) + dim(Im(\rho \circ \widehat{b_q})) = dim\mathrm{W}^{\perp} + dim\mathrm{W}^*$. Como $dim\mathrm{W}^* = dim\mathrm{W}$ para qualquer espaço vetorial W, temos que $dim\mathrm{V} = dim\mathrm{W}^{\perp} + dim\mathrm{W}$. □

Corolário 1.2.1 *Sob as mesmas hipóteses do Lema anterior temos que $(\mathrm{W}^{\perp})^{\perp} = \mathrm{W}$.*

Demonstração: De fato, como $\mathrm{W}^{\perp}$ também é subespaço de V temos que $dim\mathrm{V} = dim\mathrm{W}^{\perp} + dim(\mathrm{W}^{\perp})^{\perp}$. Assim, $dim\mathrm{W} + dim\mathrm{W}^{\perp} = dim\mathrm{V} = dim\mathrm{W}^{\perp} + dim(\mathrm{W}^{\perp})^{\perp}$. Cancelando $dim\mathrm{W}^{\perp}$, segue que $dim\mathrm{W} = dim(\mathrm{W}^{\perp})^{\perp}$. Como $\mathrm{W} \subseteq (\mathrm{W}^{\perp})^{\perp}$, temos a igualdade $\mathrm{W} = (\mathrm{W}^{\perp})^{\perp}$. □

1.3 Representação de Elementos

Definição 1.3.1 *Sejam $q : \mathrm{V} \longrightarrow \mathrm{K}$ uma forma quadrática sobre K e $d \in \dot{\mathrm{K}}$. Dizemos que q representa d, se existe $x \in \mathrm{V}$ tal que $q(x) = d$.*

Uma forma bilinear $b : \mathrm{V} \times \mathrm{V} \longrightarrow \mathrm{K}$ representa $d \in \dot{\mathrm{K}}$ se existe $x \in \mathrm{V}$ tal que $b(x, x) = d$.

Denotemos por $\mathrm{D}_{\mathrm{K}}(q)$, ou simplesmente por $\mathrm{D}(q)$ quando não houver possibilidade de confusão quanto ao corpo em questão, o conjunto dos valores de $\dot{\mathrm{K}}$ representados por q, isto é, $\mathrm{D}(q) = \{d \in \dot{\mathrm{K}} \mid q(x) = d, \text{ para algum } x \in \mathrm{V}\}$. Se $\mathrm{D}(q) = \dot{\mathrm{K}}$ dizemos que q é *universal*, ou seja, q representa todo elemento $d \in \dot{\mathrm{K}}$.

Se $a,\ d \in \dot{\mathrm{K}}$ tem-se que $d \in \mathrm{D}(q)$ se, e somente se, $a^2 d \in \mathrm{D}(q)$. De fato, $q(x) = d$ se, somente se, $q(ax) = a^2 d$. Dessa forma $\mathrm{D}(q)$ consiste da união de conjuntos de $\dot{\mathrm{K}}$ módulo $\dot{\mathrm{K}}^2$, isto é, $\mathrm{D}(q)$ é um subconjunto de $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$. Também é evidente que se $q \simeq q'$, então $\mathrm{D}(q) = \mathrm{D}(q')$. Existe o conceito análogo para uma forma bilinear b sobre K.

Teorema 1.3.1 *(Critério de Representação) Seja* (V, q) *um espaço quadrático e* $d \in \dot{\mathrm{K}}$. *Então* $d \in \mathrm{D}(q)$ *se, e somente se, existem um espaço quadrático* (V', q') *e* $x \in \mathrm{V}$, *tais que* $(\mathrm{V}, q) \simeq (x\mathrm{K}, \langle d \rangle) \perp (\mathrm{V}', q')$ *(ou* $q \simeq \langle d \rangle \perp q'$*).*

Demonstração: Se $q \simeq \langle d \rangle \perp q'$, então $d = d1^2 = (\langle d \rangle \perp q')(1, 0, \ldots, 0)$. Logo $d \in \mathrm{D}(\langle d \rangle \perp q') = \mathrm{D}(q)$.

Reciprocamente se $d \in \mathrm{D}(q)$, então existe $x \in \mathrm{V}$ tal que $q(x) = d$. O espaço quadrático $(x\mathrm{K}, \langle d \rangle)$ é regular, pois $d = det\langle d \rangle \neq 0$. Pelo Lema 1.2.3 segue o resultado. □

1.4 Espaços Hiperbólicos e Isotrópicos

Definição 1.4.1 *Seja* (V, q) *um espaço quadrático. Um vetor não nulo* $x \in \mathrm{V}$ *é dito isotrópico se* $q(x) = 0$. *Se* $q(x) \neq 0$ *diz-se que* x *é um vetor anisotrópico. Dizemos que* (V, q) *(ou* q*) é um espaço isotrópico (forma isotrópica) se existe um vetor isotrópico em* V. *Caso contrário se diz que* (V, q) *(ou* q*) é um espaço anisotrópico (forma anisotrópica), e neste caso* (V, q) *é necessariamente regular. Finalmente, dizemos que* (V, q) *ou simplesmente* q *é totalmente isotrópico se todo vetor* x *não nulo de* V *é isotrópico.*

Teorema 1.4.1 *Seja* (V, q) *um espaço quadrático bidimensional. As seguintes afirmações são equivalentes:*

(i) (V, q) *é regular e isotrópico;*

(ii) (V, q) *é regular e* $d(q) = -1\dot{\mathrm{K}}^2$*;*

(iii) q *é isométrica a* $\langle 1, -1 \rangle$.

Demonstração: **(i)** $\Longrightarrow$ **(ii)** Seja $\{e_1, e_2\}$ uma base ortogonal de V, com relação a q. Como (V, q) é regular, temos que $q \simeq \langle d_1, d_2 \rangle$, onde $d_i = q(e_i) \neq 0,\ i = 1, 2$. Seja $x = ae_1 + be_2,\ a,\ b \in \mathrm{K}$, um vetor isotrópico de V. Como $x \neq 0$ temos que $a \neq 0$ ou $b \neq 0$. Sem perda de generalidade podemos supor $a \neq 0$ para o que segue. Assim,

$0 = q(ae_1 + be_2) = a^2d_1 + b^2d_2 \Longrightarrow d_1 = -\left(\frac{b}{a}\right)^2 d_2$.
Portanto $d(q) = d_1d_2.\dot{\mathrm{K}}^2 = -1\dot{\mathrm{K}}^2$.

(ii) $\Longrightarrow$ (iii) Considere novamente $q \simeq \langle d_1, d_2\rangle$, a diagonalização de q suposta no início da demonstração. Como $det(q) = d_1.d_2 \in \frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$, por hipótese, temos que $d_1d_2 = -1$, o que implica que $d_2 \equiv -d_1(mod\dot{\mathrm{K}}^2)$. Logo $q \simeq \langle d_1, -d_1\rangle$, com $d_1 \in \dot{\mathrm{K}}$. Seja $q'(x, y) = d_1xy$ e $\sigma : \mathrm{V} \longrightarrow \mathrm{V}$ definida por $\sigma(x, y) = (x - y, x + y)$. Então, $q' \circ \sigma = \langle d_1, -d_1\rangle$, isto é, $q' \simeq q$. Como q' é claramente universal, temos que q também é. Logo $1 \in D(q)$. Portanto pelo Critério de Representação, $q \simeq \langle 1, c\rangle$. Como $det(q) = -1\dot{\mathrm{K}}^2$, temos que $c = -1(mod\dot{\mathrm{K}}^2)$, ou seja, $q \simeq \langle 1, -1\rangle$.

(iii) $\Longrightarrow$ (i) Como $\langle 1, -1\rangle$ é isotrópica e regular, q também é. □

Observação 1.4.1 *A forma quadrática $q \simeq \langle 1, -1\rangle$, dada por $q(x, y) = x^2 - y^2$ é isométrica a forma quadrática q_1, onde $q_1(x, y) = xy$.*

De fato: Basta considerarmos o isomorfismo $\sigma(x, y) = (x-y, x+y)$, que teremos $q_1(\sigma(x, y)) = q(x, y)$ e portanto $q \simeq q_1$.

Definição 1.4.2 *A classe de isometrias de um espaço quadrático bidimensional satisfazendo as condições do Teorema anterior é dito plano hiperbólico. O plano hiperbólico será denotado por $\mathbb{H}$. Uma soma (ortogonal) de m planos hiperbólicos será dita espaço hiperbólico e será denotada por $m\mathbb{H}$. A forma quadrática correspondente pode ser tomada como $x_1^2 - x_2^2 + \cdots + x_{2m-1}^2 - x_{2m}^2$ ou como $x_1x_2 + \cdots + x_{2m-1}x_{2m}$. Por simplicidade algumas vezes vamos identificar $\mathbb{H}$ por um de seus representantes, usando a expressão $\mathbb{H} = \langle 1, -1\rangle$.*

Corolário 1.4.1 *Seja (V, q) um espaço quadrático regular. Então:*

(i) *(V, q) é isotrópico se, e somente se, (V, q) contém um plano hiperbólico $\mathbb{H}$ como subespaço quadrático (um somando ortogonal);*

(ii) *Se q é isotrópica, então q é universal.*

Demonstração: **(i)** Suponhamos q isotrópica. Então existe $x \in \mathrm{V}$ não nulo tal que $q(x) = 0$. Como (V, q) é regular existe $y \in \mathrm{V}$ tal que $b_q(x, y) \neq 0$. Desde que $b_q(x, \alpha x) =$

0, para todo $\alpha \in \mathrm{K}$ o conjunto $C = \{x, y\}$ é linearmente independente. Seja $q' = q_{\mathrm{W}}$, onde W é o subespaço de V gerado por C. Então q' é regular desde que

$$B_{q'C} = \begin{pmatrix} 0 & b_{q'}(x,y) \\ b_{q'}(y,x) & b_{q'}(y,y) \end{pmatrix}$$

tem determinante $-1\dot{\mathrm{K}}^2$. Pelo Teorema 1.4.1 segue-se que $q' \simeq \mathbb{H}$. Agora o resultado segue do Lema 1.2.3.

Reciprocamente se $q = \mathbb{H} \perp q'$ para alguma forma quadrática q' e $\mathbb{H} = \langle 1, -1 \rangle$ então $q(1, 1, 0, \ldots, 0) = 1.1^2 - 1.1^2 + q'(0, \ldots, 0) = 0$. Logo q é isotrópica.

(ii) Se q é isotrópica por (i) q contém $\mathbb{H}$ que é universal. Logo q é universal, pois $\dot{\mathrm{K}} = D(\mathbb{H}) \subseteq D(q)$. □

Teorema 1.4.2 *(Da Representação) Sejam q uma forma quadrática e $d \in \dot{\mathrm{K}}$. Então, $d \in D(q)$ se, e somente se, $q \perp \langle -d \rangle$ é isotrópica.*

Demonstração: Sejam $d \in D(q)$ e $q \simeq q'$, com q' uma diagonalização de q, $q' = \langle a_1, \ldots, a_n \rangle$. Então existem $x_i \in \mathrm{K}$, $i = 1, \ldots, n$ tais que $q'(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2 = d$. Assim, $a_1 x_1^2 + \cdots + a_n x_n^2 - d1^2 = 0$. Logo $q' \perp \langle -d \rangle$ é isotrópica. Como $q \perp \langle -d \rangle \simeq q' \perp \langle -d \rangle$, segue que $q \perp \langle -d \rangle$ é isotrópica.

Agora suponha que $x = (x_1, \ldots, x_n, x_{n+1})$ seja um vetor isotrópico para $q' \perp \langle -d \rangle$. Assim $a_1 x_1^2 + \cdots + a_n x_n^2 - d x_{n+1}^2 = 0$. Se $x_{n+1} \neq 0$, então $d = a_1 \left(\frac{x_1}{x_{n+1}}\right)^2 + \cdots + a_n \left(\frac{x_n}{x_{n+1}}\right)^2 \in D(q') = D(q)$. Se $x_{n+1} = 0$, então $(x_1, \ldots, x_n) \neq 0$ é um vetor isotrópico para q'. Logo por (ii) do Corolário 1.4.1, q' é universal. Assim $d \in D(q') = D(q)$. □

Corolário 1.4.2 *Para r inteiro e positivo, são equivalentes:*

(i) *Toda forma quadrática regular q de dimensão r é universal;*

(ii) *Toda forma quadrática regular q_1 de dimensão $r + 1$ é isotrópica.*

Demonstração: Imediata. □

Definição 1.4.3 *Sejam $x \in \mathrm{V}$ um vetor anisotrópico e $\mathrm{W} = (x\mathrm{K})^{\perp}$. Então uma aplicação linear $\tau_x : \mathrm{V} \longrightarrow \mathrm{V}$ tal que $\tau_x(y) = y - \dfrac{2b_q(x,y)}{q(x)}.x$, para todo $y \in \mathrm{V}$ é dita reflexão segundo o hiperplano W ortogonal à x.*

Lema 1.4.1 *Considerando τ_x como definida acima, temos:*

(i) $\tau_x(x) = -x$ *e* $\tau_{x|\mathrm{W}} = id_{\mathrm{W}}$*;*

(ii) $\tau_x(x)$ *é uma isometria de* (V, q)*;*

(iii) $\tau_x \circ \tau_x = id$*;*

(iv)$det(\tau_x) = -1$.

Demonstração: A demonstração dos ítens **(i)**, **(ii)** e **(iii)** são simples.

(iv) Escolha uma base $\{e_2, \ldots, e_n\}$ de W e complete para a base de V, fazendo $e_1 = x$. A matriz de τ_x com relação à esta base é $\begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ que tem determinante -1. □

Lema 1.4.2 *Sejam (V, q) um espaço quadrático e $x, y \in \mathrm{V}$ tais que $q(x) = q(y) \neq 0$. Então existe uma isometria $\tau : \mathrm{V} \longrightarrow \mathrm{V}$ tal que $\tau(x) = y$.*

Demonstração: Para que $\tau(x) = y$, é necessário que $x + y \in \mathrm{W} = (w\mathrm{K})^{\perp}$ para algum $w \in \mathrm{V}$. Para $w = x - y$, temos $b_q(x-y, x+y) = q(x) - q(y) = 0$. Logo $x - y \perp x + y$. Então devemos fazer uma reflexão segundo o hiperplano $\mathrm{W} = ((x-y)\mathrm{K})^{\perp}$, desde que $q(x-y) \neq 0$. Pela lei do paralelogramo, temos

$$q(x+y) + q(x-y) = 2q(x) + 2q(y) = 4q(x) \neq 0.$$

Isto implica que $q(x+y), q(x-y)$ não podem ser ambos nulos. Trocando y por $-y$ (se for necessário), podemos assumir que $q(x-y) \neq 0$ (se acharmos uma isometria $\tau : \mathrm{V} \longrightarrow \mathrm{V}$ tal que $\tau(x) = -y$, então $-\tau$ leva x em y). Aplicando a reflexão τ_{x-y} à x, obtemos $\tau_{x-y}(x) = x - \dfrac{2b(x, x-y)}{q(x-y)}.(x-y)$. Mas $q(x-y) = 2b(x, x-y)$, assim $\tau_{x-y}(x) = x - (x-y) = y$, como queríamos. □

Teorema 1.4.3 *(Cancelamento de Witt) Sejam q, q_1, q_2 formas quadráticas arbitrárias. Se $q \perp q_1 \simeq q \perp q_2$, então $q_1 \simeq q_2$.*

Demonstração: (1^{o} passo) Suponhamos q totalmente isotrópica e q_1 regular. Sejam B_q, B_{q_1} e B_{q_2} as matrizes simétricas associadas à q, q_1 e q_2 em bases convenientes. Pelas hipóteses temos que $\begin{pmatrix} \mathrm{B}_q & 0 \\ 0 & \mathrm{B}_{q_1} \end{pmatrix}$ é congruente à $\begin{pmatrix} \mathrm{B}_q & 0 \\ 0 & \mathrm{B}_{q_2} \end{pmatrix}$, isto é, existe uma matriz inversível $\mathrm{E} = \begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix}$, tal que $\begin{pmatrix} \mathrm{B}_q & 0 \\ 0 & \mathrm{B}_{q_1} \end{pmatrix} = \mathrm{E}^t \begin{pmatrix} \mathrm{B}_q & 0 \\ 0 & \mathrm{B}_{q_2} \end{pmatrix} \mathrm{E} = \begin{pmatrix} * & * \\ * & \mathrm{D}^t\mathrm{B}_{q_2}\mathrm{D} \end{pmatrix}$. Em particular, $\mathrm{B}_{q_1} = \mathrm{D}^t\mathrm{B}_{q_2}\mathrm{D}$. Como B_{q_1} é não singular, temos que D também é e assim B_{q_1} e B_{q_2} são congruentes. Portanto $q_1 \simeq q_2$.

(2^{o} passo) Suponhamos q totalmente isotrópica. Diagonalizemos q_1, q_2 e assumamos que q_1 tenha exatamente r zeros na diagonalização e que q_2 tem r zeros ou mais.

Reescrevendo as hipóteses, temos que $q \perp r\langle 0\rangle \perp q_1' \simeq q \perp r\langle 0\rangle \perp q_2'$. Como q_1' é regular, pelo 1^{o} passo, temos que $q_1' \simeq q_2'$. Assim, $q_1 \simeq r\langle 0\rangle \perp q_1' \simeq r\langle 0\rangle \perp q_2' \simeq q_2$.

(3^{o} passo, caso geral) Seja $q \simeq \langle a_1, \ldots, a_n\rangle$ e provemos por indução sobre n.

Para $n = 1$, $\langle a_1\rangle \perp q_1 \simeq \langle a_1\rangle \perp q_2$. Se $a_1 = 0$, retornamos ao segundo caso. Se $a_1 \neq 0$, sejam $q_3 = \langle a_1\rangle \perp q_1$, $q_4 = \langle a_1\rangle \perp q_2$ e $\sigma : \mathrm{V} \longrightarrow \mathrm{V}$ tal que $q_3 = q_4 \circ \sigma$. Como $a_1 \in D(q_3) \cap D(q_4)$, existem $x, y, z \in \mathrm{V}$, com $\sigma(z) = x$ tal que $q_3(z) = a_1 = q_4(y)$ ou $a_1 = q_3(z) = q_4(\sigma(z)) = q_4(x)$. Logo $q_4(x) = q_4(y) \neq 0$. Pelo Lema 1.4.2, existe $\tau : \mathrm{V} \longrightarrow \mathrm{V}$ tal que $\tau(x) = y$ $(q_4 \circ \tau = q_4)$. Temos $q_3 = q_4 \circ \sigma = q_4 \circ \tau \circ \sigma$ e $a_1 = q_3(z) = (q_4 \circ \tau \circ \sigma)(z) = q_4((\tau \circ \sigma)(z)) = q_4(y)$ (onde $(\tau \circ \sigma)(z) = y$). Logo $(\tau \circ \sigma)_{|(z\mathrm{K})^{\perp}} : (z\mathrm{K})^{\perp} \longrightarrow (y\mathrm{K})^{\perp}$ é um isomorfismo tal que $q_{4|(y\mathrm{K})^{\perp}} \circ (\tau \circ \sigma)_{|(z\mathrm{K})^{\perp}} = q_{3|(z\mathrm{K})^{\perp}}$, ou seja, $q_2 \circ (\tau \circ \sigma) = q_1$. Assim, $q_1 \simeq q_2$. O resto segue por indução. □

Proposição 1.4.1 *Sejam $q = \langle a, b\rangle$ e $q' = \langle c, d\rangle$ formas binárias regulares. Então $q \simeq q'$ se, e somente se, $d(q) = d(q')$ e $D(q) \cap D(q') \neq \emptyset$ (isto é, q e q' representam um elemento em comum $e \in \dot{\mathrm{K}}$).*

Demonstração: ($\Longrightarrow$) É clara.

($\Longleftarrow$) Suponhamos $e \in D(q) \cap D(q')$. Pelo Critério da Representação, $q \simeq \langle e, x\rangle$ e $q' \simeq \langle e, y\rangle$ para algum $x, y \in \dot{\mathrm{K}}$. Calculando o determinante, temos que $ab = ex$ e $cd = ey$, assim $q \simeq \langle e, abe\rangle$ e $q' \simeq \langle e, cde\rangle$. Mas por hipótese $ab = cd$, e portanto $q \simeq q'$. □

Corolário 1.4.3 *Assuma que toda forma binária sobre o corpo* K *é universal. Então, duas formas quadráticas são isométricas se, e somente se, elas têm o mesmo determinante e a mesma dimensão.*

Demonstração: Se q e q' tem dimensão 1 é evidente. Como a forma binária $\langle a_1, a_2\rangle$ representa 1, pois é universal, segue do Critério de Representação que $\langle a_1, a_2\rangle \simeq \langle 1, a_1a_2\rangle$. Por indução, temos que qualquer forma quadrática regular $q = \langle a_1, \ldots, a_n\rangle$, $(n \geq 2)$ é equivalente a $\langle 1, \ldots, 1, d(q)\rangle$. Disto o Corolário segue fácil. □

Dizemos que duas formas quadráticas diagonalizadas $q = \langle a_1, \ldots, a_n\rangle$ e $q_1 = \langle b_1, \ldots, b_n\rangle$, são de *equivalência simples* se existirem i e j tais que $\langle a_i, a_j\rangle \simeq \langle b_i, b_j\rangle$ e $a_k = b_k$ quando $k \neq i, j$.

Definição 1.4.4 *Dizemos que duas formas quadráticas diagonalizadas q e q', são equivalentes por cadeia e denotemos por $q \simeq_C q_1$, se existe uma sequência de formas quadráticas diagonalizadas, $q_0, q_1, \ldots, q_m$ tais que $q_0 = q$ e $q_m = q'$, e para cada i, q_i e q_{i+1} são de equivalência simples* $(0 \leq i \leq m-1)$.

A equivalência por cadeia é claramente uma relação de equivalência, sobre o conjunto de todas as formas quadráticas diagonais sobre um corpo K. Note que $q \simeq_C q'$ implica $q \simeq q'$. O seguinte Teorema mostra que a recíproca também é verdadeira.

Teorema 1.4.4 *(Equivalência Por Cadeia) Sejam q e q_1 formas quadráticas diagonais quaisquer (de mesma dimensão). Se $q \simeq q_1$, então $q \simeq_C q_1$.*

Demonstração: Sejam $q = \langle a_1, \ldots, a_n\rangle$ e $q_1 = \langle b_1, \ldots, b_n\rangle$. Primeiro notemos que se θ é uma permutação dos índices $\{1, 2, ..., n\}$ e $q^\theta = \langle a_{\theta(1)}, \ldots, a_{\theta(n)}\rangle$, então $q \simeq_C q^\theta$, pois o grupo das permutações de n elementos é gerado por transposições. Temos ainda que se $q \simeq q_1$, então q e q_1 têm o mesmo número de termos nulos em suas diagonalizações. Assim é suficiente verificarmos que as partes regulares de q e q_1 são equivalentes por cadeia. Deste

modo podemos assumir que q e q_1 são regulares, isto é, a_i, b_j são todos não-nulos. Daí procedemos por indução em n.

Se $n = 1, 2$ o resultado segue direto. Assim consideremos $n \geq 3$. Dentre todas as formas quadráticas diagonais que são equivalentes por cadeia a q, escolha uma $q' = \langle c_1, \ldots, c_n \rangle$ tal que alguma subforma diagonalizada $\langle c_1, \ldots, c_k \rangle$ represente b_1, e k seja o menor número natural possível.

Verifiquemos que $k = 1$. De fato, se $b_1 = c_1e_1^2 + \cdots + c_ke_k^2$ (com $k \geq 2$), então para todo $m \geq 1$ e $m \leq k$, $c_1e_1^2 + \cdots + c_me_m^2 \neq 0$. Caso contrário $b_1 = c_1e_1^2 + \cdots + c_me_m^2 + c_{m+1}c_{m+1}^2 + \cdots + c_ke_k^2 = c_{m+1}c_{m+1}^2 + \cdots + c_ke_k^2$ e $\langle c_1, \ldots, c_m, c_{m+1}, \ldots, c_k \rangle \simeq_C \langle c_{m+1}, \ldots, c_k, c_1, \ldots, c_n \rangle$ e $b_1c_{m+1}e_{m+1}^2 + \cdots + c_ke_k^2$ com $k - m < k$ (absurdo pela escolha de q.) Em particular $d = c_1e_1^2 + c_2e_2^2 \neq 0$. Pela Proposição 1.4.1 $\langle c_1, c_2 \rangle \simeq \langle d, c_1c_2d \rangle$. Deste modo $q \simeq_C q' = \langle c_1, c_2, \ldots, c_n \rangle \simeq_C \langle d, c_1c_2d, c_3, \ldots, c_k, \ldots, c_n \rangle \simeq_C \langle d, c_3, \ldots, c_k, \ldots, c_n, c_1c_2d \rangle$ e $b_1 = d + c_3e_3^2 + \cdots + c_ke_k^2$ é representado por $\langle d, c_3, \ldots, c_k \rangle$, que tem dimensão $k-1$, contradizendo a escolha de k, portanto $k = 1$.

Consequentemente $\langle c_1 \rangle = \langle b_1 \rangle$, e assim $q \simeq_C \langle b_1, c_2, \ldots, c_n \rangle$. Pelo Teorema do Cancelamento de Witt $\langle b_1, c_2, \ldots, c_n \rangle \simeq \langle b_1, b_2, \ldots, b_n \rangle$ segue-se que $\langle c_2, \ldots, c_n \rangle \simeq \langle b_2, \ldots, b_n \rangle$. Por hipótese de indução, tem-se $\langle c_2, \ldots, c_n \rangle \simeq_C \langle b_2, \ldots, b_n \rangle$. Finalmente $q \simeq_C \langle b_1, c_2, \ldots, c_n \rangle \simeq_C \langle b_1, b_2, \ldots, b_n \rangle = q_1$. □

1.5 Produto de Kronecker de Espaços Quadráticos

Já foi definido soma ortogonal de formas quadráticas. Agora definiremos produto de formas quadráticas.

Definição 1.5.1 *Sejam* (V_1, q_1), (V_2, q_2) *espaços quadráticos sobre* K *de dimensões* m *e* n, *e* $\mathrm{V} = \mathrm{V}_1 \otimes \mathrm{V}_2$. *Definimos* $b : \mathrm{V} \times \mathrm{V} \to \mathrm{K}$ *a única forma bilinear simétrica satisfazendo* $b(x_1 \otimes x_2, y_1 \otimes y_2) = b_1(x_1, y_1).b_2(x_2, y_2)$ *para todos* $x_1, y_1 \in \mathrm{V}_1$ *e* $x_2, y_2 \in \mathrm{V}_2$, *onde* b_i *é a forma bilinear associada a* q_i, $i = 1, 2$. *Agora definimos* $q : \mathrm{V} \longrightarrow \mathrm{K}$ *por* $q(x_1 \otimes x_2) = b(x_1 \otimes x_2, x_1 \otimes x_2)$. *Portanto* $q(x_1 \otimes x_2) = b_1(x_1, x_1).b_2(x_2, x_2) = q_1(x_1).q_2(x_2)$. *Segue-se que* (V, q) *é um espaço quadrático de dimensão* $m.n$, *e a forma bilinear associada à quadrática* q *é a forma bilinear definida acima. Denotemos* q *por* $q_1 \otimes q_2$ *(ou* $q = q_1.q_2$*).*

Sejam $\{e_1, ..., e_m\}$ base de V_1, $\{e'_1, .., e'_n\}$ base de V_2, $a_{ij} = b_1(e_i, e_j)$ e $b_{kl} = b_2(e'_k, e'_l)$. Então $\mathrm{A} = (a_{ij})$ e $\mathrm{B} = (b_{kl})$ são as matrizes de q_1 e q_2 nestas bases. Na base $\{e_1 \otimes e'_1, e_1 \otimes e'_2, ..., e_1 \otimes e'_n, ..., e_m \otimes e'_1, ..., e_m \otimes e'_n\}$ de V a matriz de q é

$$\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{12}b_{11} & a_{12}b_{12} & \cdots \\ a_{11}b_{12} & a_{11}b_{22} & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \ddots & \cdots & \cdots & \cdots \\ a_{21}b_{11} & a_{21}b_{12} & \cdots & \cdots & \cdots & \cdots \\ a_{21}b_{12} & a_{21}b_{22} & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix} = \begin{pmatrix} a_{11}\mathrm{B} & a_{12}\mathrm{B} & \cdots & a_{1m}\mathrm{B} \\ a_{21}\mathrm{B} & a_{22}\mathrm{B} & \cdots & a_{2m}\mathrm{B} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}\mathrm{B} & a_{m2}\mathrm{B} & \cdots & a_{mm}\mathrm{B} \end{pmatrix}$$

que é chamado de *produto de Kronecher* das matrizes A e B. Em particular $\langle a \rangle \otimes \langle b \rangle = \langle ab \rangle$ para todos $a, b \in \dot{\mathrm{K}}$.

Propriedades 1.5.1 **(i)** $q_1 \otimes q_2 \simeq q_2 \otimes q_1$ *(lei comutativa);*

(ii) $(q_1 \otimes q_2) \otimes q_3 \simeq q_1 \otimes (q_2 \otimes q_3)$ *(lei associativa);*

(iii) $q \otimes (q_1 \perp q_2) \simeq (q \otimes q_1) \perp (q \otimes q_2)$ *(lei distributiva).*

Demonstração: **(i)** $\sigma : \mathrm{V} = \mathrm{V}_1 \otimes \mathrm{V}_2 \to \mathrm{V}_2 \otimes \mathrm{V}_1$ dada por $\sigma(x \otimes y) = y \otimes x$, leva base em base e $q = q' \circ \sigma$, onde $q = q_1 \otimes q_2$ e $q' = q_2 \otimes q_1$.

(ii) $\sigma : (\mathrm{V}_1 \otimes \mathrm{V}_2) \otimes \mathrm{V}_3 \to \mathrm{V}_1 \otimes (\mathrm{V}_2 \otimes \mathrm{V}_3)$, onde $\sigma((x \otimes y) \otimes z) = x \otimes (y \otimes z)$, leva base em base e $(q_1 \otimes (q_2 \otimes q_3)) \circ \sigma = (q_1 \otimes q_2) \otimes q_3$.

(iii) $\sigma : \mathrm{V} \otimes (\mathrm{V}_1 \perp \mathrm{V}_2) \to (\mathrm{V} \otimes \mathrm{V}_1) \perp (\mathrm{V} \otimes \mathrm{V}_2)$ definida por $\sigma(x \otimes (y_1 + y_2)) = (x \otimes y_1) + (x \otimes y_2)$ satisfaz $(q' \circ \sigma)[x \otimes (y_1 + y_2)] = q'((x \otimes y_1) + (x \otimes y_2)) = (q \otimes q_1)(x \otimes y_1) + (q \otimes q_2)(x \otimes y_2) = q(x)(q_1 \perp q_2)(y_1 + y_2) = q \otimes (q_1 \perp q_2)(x \otimes (y_1 + y_2))$, onde $q' = (q \otimes q_1) \perp (q \otimes q_2)$. Logo $q \otimes (q_1 \perp q_2) \simeq (q \otimes q_1) \perp (q \otimes q_2)$. □

Observação 1.5.1 **(i)** *Pela lei distributiva tem-se:*

$\langle a_1, ..., a_m \rangle \otimes \langle b_1, ..., b_n \rangle \simeq \langle a_1 b_1, a_1 b_2, \ldots, a_1 b_n, a_2 b_1, \ldots, a_m b_n \rangle$;

(ii) *Se q é regular então $q \otimes \mathbb{H} \simeq (dim(q)).\mathbb{H}$;*

(iii) $(q_1 \perp q_2) \perp q_3 = q_1 \perp (q_2 \perp q_3)$ *(lei associativa).*

Capítulo 2

Álgebra dos Quatérnios

Definição 2.0.2 *Sejam* K *um corpo com característica diferente de 2, e* $a, b \in \dot{\mathrm{K}}$. *A* K*-álgebra gerada por* i *e* j *tal que* $i^2 = a, j^2 = b$ *e* $ij = -ji = k$ *é dita álgebra de quatérnios e é denotada por* $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right)$.

Como espaço vetorial A tem dimensão 4 sobre K e uma base é $\{1, i, j, k\}$. Além disso A não é comutativa, pois $ij = -ji$.

Se considerarmos $\mathrm{K} = \mathbb{R}$ e $\mathrm{A} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, então A é o *anel de divisão usual dos quatérnios*, denotado por $\mathcal{H}$.

Observação 2.0.2 *A construção da álgebra dos quatérnios é simétrica em relação à* a *e* b*, ou seja,* $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right) \approx \left(\frac{b,a}{\mathrm{K}}\right) = \mathrm{A}'$.

De fato, seja $i',\ j',\ k' \in \mathrm{A}'$ tais que $i'^2 = b,\ j'^2 = a,\ -i'j' = j'i' = k'$ e considere $\varphi : \mathrm{A} \longrightarrow \mathrm{A}'$ tal que $\varphi(1) = 1,\ \varphi(i) = j',\ \varphi(j) = i'$ e $\varphi(k) = \varphi(ij) = \varphi(i).\varphi(j) = j'i' = k'$, e estende por linearidade a todo A. A função φ é, claramente, um homomorfismo de álgebras.

Definição 2.0.3 **(i)** *Uma* K*-álgebra* A *é dita central se* $Z(\mathrm{A}) = \mathrm{K}\ \ (= \mathrm{K}.1_{\mathrm{A}})$*, onde* $Z(\mathrm{A}) = \{x \in \mathrm{A} \mid xa = ax,\ \text{para todo } a \in \mathrm{A}\}$ *(*$Z(\mathrm{A})$ *é dito centro de* A*).*

(ii) *Uma* K*-álgebra* A *é dita simples se* A *não possui ideais bilaterais próprios.*

(iii) *Uma* K*-álgebra* A *é central simples se satisfaz (i) e (ii).*

Proposição 2.0.1 **(i)** $\left(\frac{a,b}{\mathrm{K}}\right) \approx \left(\frac{ax^2, by^2}{\mathrm{K}}\right)$*, para todos* $a, b, x, y \in \dot{\mathrm{K}}$*;*

(ii) *O centro de* $\left(\frac{a,b}{\mathrm{K}}\right)$ *é* $\mathrm{K}(=\mathrm{K}.1)$*, para quaisquer* $a,\ b \in \dot{\mathrm{K}}$;

(iii) $\left(\frac{a,b}{\mathrm{K}}\right)$ *é uma álgebra simples, para todos* $a,\ b \in \dot{\mathrm{K}}$;

(iv) $\left(\frac{-1,1}{\mathrm{K}}\right) \approx \mathrm{M}_2(\mathrm{K})$ *(álgebra de matrizes* 2×2 *sobre* K*).*

Demonstração: **(i)** Sejam $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right)$ com base $\{1, i, j, k\}$ e $\mathrm{A}' = \left(\frac{ax^2, by^2}{\mathrm{K}}\right)$ com base $\{1, i', j', k'\}$ tal que $i'^2 = ax^2$ e $j'^2 = by^2$. Observe que $xi, yj \in \mathrm{A}'$, pois $i'^2 = ax^2 = x^2i^2 = (xi)^2$, $j'^2 = by^2 = y^2j^2 = (yj)^2$, $k'^2 = i'^2j'^2 = abx^2y^2$ e mais, $(xi)(yj) = (xy)(ij) = (xy)(-ji) = -(yj)(xi)$. Assim, $\varphi : \mathrm{A} \longrightarrow \mathrm{A}'$ tal que $\varphi(i) = xi$, $\varphi(j) = yj$ e $\varphi(k) = \varphi(ij) = \varphi(i)\varphi(j) = xiyj = xyij = xyk$, e estendendo por linearidade, obtemos um isomorfismo de K-álgebra entre A e A′.

(ii) $\mathrm{Z(A)} = \{x \in \mathrm{A} \mid xa = ax, \text{ para todo } a \in \mathrm{A}\}$. Seja $x = \alpha + \beta i + \gamma j + \delta k \in \mathrm{Z(A)}$. Assim, de $xi = ix$, vem que $2\gamma k + 2a\delta j = 0$. Como $k,\ j$ são linearmente independentes segue que $\gamma = \delta = 0$. Logo $x = \alpha + \beta i$. De $xj = jx$ encontramos $2\beta k = 0$. Logo $\beta = 0$. Portanto $x = \alpha \in \mathrm{K}$. Logo $\mathrm{Z(A)} = \mathrm{K}$.

(iii) Seja $\mathrm{J} \subseteq \mathrm{A}$ um ideal bilateral ($\mathrm{AJ} = \mathrm{J}$ e $\mathrm{JA} = \mathrm{J}$).

Se $\mathrm{J} \neq \{0\}$, tome $x = \alpha + \beta i + \gamma j + \delta k \neq 0,\ x \in \mathrm{J}$. Suponhamos $\gamma \neq 0$. Como $xi, ix \in \mathrm{J}$, temos que $y = xi - ix \in \mathrm{J}$. Fazendo os cálculos temos que $y = -2a\delta j - 2\gamma k \in \mathrm{J}$. De $yj - jy \in \mathrm{J}$, temos que $-4b\gamma i \in \mathrm{J}$. Assim $-4b\gamma i.i = -4ab\gamma \in \mathrm{J}$. Como $-4ab\gamma \neq 0$, segue que $1 \in \mathrm{J}$. Logo $\mathrm{J} = \mathrm{A}$. Se $\beta \neq 0$ ou $\delta \neq 0$, de modo análogo se prova que $\mathrm{J} = \mathrm{A}$.

(iv) Seja $i_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, j_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ em $\mathrm{M}_2(\mathrm{K})$. Temos $i_0^2 = -Id, j_0^2 = Id$ e $i_0j_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -j_0i_0$. Assim existe um homomorfismo de álgebra $\varphi : \left(\frac{-1,1}{\mathrm{K}}\right) \longrightarrow \mathrm{M}_2(\mathrm{K})$, onde $\varphi(1) = Id, \varphi(i) = i_0, \varphi(j) = j_0, \varphi(k) = i_0j_0$. Como Id, i_0, j_0, i_0j_0 geram $\mathrm{M}_2(\mathrm{K})$, temos um isomorfismo entre as K-álgebras. □

Os ítens (ii) e (iii) da Proposição 2.0.1, nos moatram que toda álgebra de quatérnios é *central simples.*

Definição 2.0.4 *Um quatérnio* $x = \alpha + \beta i + \gamma j + \delta k \in \mathrm{A}$ *é dito quatérnio puro se* $\alpha = 0$. *O conjunto dos quatérnios puros será denotado por* A_0.

A proposição abaixo mostra que a "pureza"dos quatérnios independe da base $\{1, i, j, k\}$.

Proposição 2.0.2 *Seja* $x \in \mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right), x \neq 0$. *Então* $x \in \mathrm{A}_0$ *se, e somente se,* $x \notin \mathrm{K}$ *e* $x^2 \in \mathrm{K}$.

Demonstração: Seja $x = \alpha + \beta i + \gamma j + \delta k$. Então,

$$x^2 = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha(\beta i + \gamma j + \delta k). \tag{2.1}$$

($\Longrightarrow$) Se $x \in \mathrm{A}_0$ então $\alpha = 0$. Assim $x^2 = a\beta^2 + b\gamma^2 - ab\delta^2 \in \mathrm{K}$ e $x \notin \mathrm{K}$.

($\Longleftarrow$) Se $x \notin \mathrm{K}$ então $\beta \neq 0$ ou $\gamma \neq 0$ ou $\delta \neq 0$. Como $x^2 \in \mathrm{K}$, pela equação 2.1 devemos ter $\alpha = 0$. E assim x é um quatérnio puro, isto é, $x \in \mathrm{A}_0$. □

Corolário 2.0.1 *Se* $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right), \mathrm{A}' = \left(\frac{a',b'}{\mathrm{K}}\right)$, *e* $\varphi : \mathrm{A} \longrightarrow \mathrm{A}'$ *um isomorfismo de álgebras, então* $\varphi(\mathrm{A}_0) = \mathrm{A}'_0$.

Demonstração: Seja $x \in \mathrm{A}_0$ então $x \notin \mathrm{K}$ e $x^2 \in \mathrm{K}$. Como $\varphi(\mathrm{K}) = \mathrm{K}$ (pois $\varphi(\mathrm{Z}(\mathrm{A})) = \mathrm{Z}(\mathrm{A}')$) e φ é injetor, temos que $\varphi(x) \notin \mathrm{K}$ e $\varphi(x)^2 = \varphi(x^2) \in \mathrm{K}$. Logo $\varphi(x) \in \mathrm{A}'_0$ e portanto $\varphi(\mathrm{A}_0) \subset \mathrm{A}'_0$.

Por outro lado, se $y \in \mathrm{A}'_0$, então $y \notin \mathrm{K}$ e $y^2 \in \mathrm{K}$. Seja $x \in \mathrm{A}$ tal que $\varphi(x) = y$. Como $\varphi(\mathrm{K}) = \mathrm{K}$ temos que $x \notin \mathrm{K}$ (pois φ é injetor) e de $\varphi(x^2) = \varphi(x)^2 = y^2 \in \mathrm{K}$, segue que $x^2 \in \mathrm{K}$ e então $x \in \mathrm{A}_0$. Portanto $\mathrm{A}'_0 \subset \varphi(\mathrm{A}_0)$. □

2.1 Álgebra dos Quatérnios Como Espaço Quadrático

Seja $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right)$, $a, b \in \dot{\mathrm{K}}$ uma álgebra de quatérnios com base $\{1, i, j, k\}$. Veremos que A tem uma estrutura de espaço quadrático.

Definição 2.1.1 *Para $x = \alpha + \beta i + \gamma j + \delta k \in \mathrm{A}$, o conjugado de x é definido como sendo $\overline{x} = \alpha - \beta i - \gamma j - \delta k$.*

Segue desta definição que para todos $x, y \in \mathrm{A}$ tem-se:

1. $\overline{x+y} = \overline{x} + \overline{y}$;
2. $\overline{xy} = \overline{y}\ \overline{x}$;
3. $\overline{\overline{x}} = x$;
4. $\overline{rx} = r\overline{x},\ r \in \mathrm{K}$;
5. Se $x \in \mathrm{A}_0$, então $\overline{x} = -x$;
6. $x \in \mathrm{K}$ se, e somente se, $\overline{x} = x$.

Definição 2.1.2 *Dado $x \in \mathrm{A} = \left(\dfrac{a,b}{\mathrm{K}}\right)$, definimos a norma de x por $N(x) = x.\overline{x}$ e o traço de x por $\mathrm{T}(x) = x + \overline{x}$.*

Observação 2.1.1 *Note que $N(x), \mathrm{T}(x) \in \mathrm{K}$, para todo $x \in \mathrm{A}$, pois: $\overline{\mathrm{T}(x)} = \mathrm{T}(x)$ e $\overline{N(x)} = N(x)$.*

Definição 2.1.3 *Definimos $b : \mathrm{A} \times \mathrm{A} \longrightarrow \mathrm{K}$ por $b(x,y) = \frac{1}{2}(x\overline{y} + y\overline{x}) = \frac{1}{2}\mathrm{T}(x\overline{y}) \in \mathrm{K}$. Esta função é uma forma bilinear simétrica e portanto (A, b) é um espaço bilinear. A forma quadrática associada à b é $q_b = N : \mathrm{A} \longrightarrow \mathrm{K}$, pois $q_b(x) = b(x,x) = \frac{1}{2}\mathrm{T}(x\overline{x}) = N(x)$. Assim, N é uma forma quadrática em A chamada forma norma de A. Dessa forma, (A, N) é um espaço quadrático.*

Corolário 2.1.1 *O espaço quadrático (A, N) tem base ortogonal $\{1, i, j, k\}$ e a forma quadrática N é isométrica à $\langle 1, -a, -b, ab\rangle$.*

Demonstração: Se $x, y \in \mathrm{A}_0$ temos que $b(x,y) = \frac{1}{2}(x\overline{y}+y\overline{x}) = \frac{1}{2}(-xy-yx) = -\frac{1}{2}(xy+yx)$. Assim, $x \perp y$ em A_0, se, e somente se, $b(x,y) = 0$, ou seja, $xy = -yx$. Em particular, $\{i, j, k\}$ é uma base ortogonal para o espaço quadrático (A_0, N_0), pois $ij = -ji, ik = -ki, kj = -jk$ (isto é, são ortogonais dois a dois). Além disso, se x é um quatérnio puro $b(x,1) = \frac{1}{2}(x\overline{1} +$

$1\overline{x}) = \frac{1}{2}(x - x) = 0$. Logo 1 é ortogonal à i, j, k. Portanto $\{1, i, j, k\}$ é base ortogonal para (A, N).

Como $N(i) = i\overline{i} = -i^2 = -a, N(j) = j\overline{j} = -j^2 = -b$ e $N(k) = k\overline{k} = -k^2 = ab$, segue que se $x = \alpha + \beta i + \gamma j + \delta k \in \mathrm{A}$ então $N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 = \langle 1, -a, -b, ab\rangle(x)$. Concluímos assim que $\langle 1, -a, -b, ab\rangle$ é uma diagonalização de N. Logo $(\mathrm{A}, N) \simeq (\mathrm{A}, \langle 1, -a, -b, ab\rangle)$. □

Note que se $x = \alpha + \beta i + \gamma j + \delta k \in \mathrm{A}$, então $N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2$.

Proposição 2.1.1 *Todo* $x = \alpha + \beta i + \gamma j + \delta k \in \mathrm{A}$ *satisfaz a equação* $x^2 - \mathrm{T}(x)x + N(x) = 0$.

Demonstração: $x^2 = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha\beta i + 2\alpha\gamma j + 2\alpha\delta k = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha(\beta i + \gamma j + \delta k) = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha x - 2\alpha^2$.

Temos que $(\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) - 2\alpha^2 = -\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2 = -N(x)$. Logo $x^2 = 2\alpha x - N(x)$, ou então, $x^2 - \mathrm{T}(x)x + N(x) = 0$. □

Proposição 2.1.2 **(i)** *Para todos* $x,\ y \in \mathrm{A}, N(xy) = N(x)N(y)$;

(ii) $x \in \mathrm{A}$ *é inversível se, e somente se,* $N(x) \neq 0$ *(isto é, se* x *é anisotrópico). Em particular,* $D(N)$ *é um subgrupo de* $\dot{\mathrm{K}}$ $\left(\text{ou de } \frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}\right)$.

Demonstração: **(i)** $N(xy) = xy\overline{xy} = xy\overline{y}\ \overline{x} = x\mathrm{N}(y)\overline{x}$. Como $N(y) \in \mathrm{K} = \mathrm{Z}(\mathrm{A})$ temos que $N(xy) = x\overline{x}.N(y) = N(x)N(y)$.

(ii) Seja $x \in \mathrm{A}$, não nulo. Se existe x^{-1} então $N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1$, assim $N(x) \neq 0$.

Reciprocamente se $N(x) \neq 0$ da equação $x\overline{x} = N(x).1$ segue que $x.\dfrac{\overline{x}}{N(x)} = \dfrac{\overline{x}}{N(x)}.x$. Logo $x^{-1} = \dfrac{\overline{x}}{N(x)}$.

$D(N)$ é subgrupo, pois $1 = N(1) \in D(N)$. Assim $D(N) \neq \emptyset$. Se $c, d \in D(N)$, sejam $c = N(x),\ d = N(y)$, com $x,\ y \in \mathrm{A}$. Como $N(y).N(y^{-1}) = N(y.y^{-1}) = N(1) = 1$, segue que $N(y)^{-1} = N(y^{-1})$, para todo $y \in \mathrm{K}$. Logo $cd^{-1} = N(x)N(y)^{-1} = N(x)N(y^{-1}) = N(xy^{-1}) \in D(N)$. □

Proposição 2.1.3 *Para* $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right)$, $\mathrm{A}' = \left(\frac{a',b'}{\mathrm{K}}\right)$ *as seguintes afirmações são equivalentes:*

(i) A *é isomorfa à* A′ *como* K*-álgebras;*

(ii) $(\mathrm{A}, N) \simeq (\mathrm{A}', N')$*;*

(iii) $(\mathrm{A}_0, N_0) \simeq (\mathrm{A}'_0, N'_0)$*, onde* $N_0 = \langle -a, -b, a.b\rangle$ *e* $N'_0 = \langle -a', -b', a'b'\rangle$*.*

Demonstração: **(i)** $\Longrightarrow$ **(ii)** Seja $\varphi : \mathrm{A} \longrightarrow \mathrm{A}'$ um isomorfismo de álgebras. Pelo Corolário 2.0.1, $\varphi(\mathrm{A}_0) = \mathrm{A}'_0$. Se $x = \alpha + x_0$, onde $\alpha \in \mathrm{K}$ e $x_0 \in \mathrm{A}_0$, então $\overline{x} = \alpha - x_0$. Daí $\varphi(x) = \varphi(\alpha + x_0) = \varphi(\alpha) + \varphi(x_0)$, $\overline{\varphi(x)} = \overline{\varphi(\alpha) + \varphi(x_0)} = \varphi(\alpha) - \varphi(x_0) = \varphi(\alpha) + \varphi(-x_0) = \varphi(\alpha - x_0) = \varphi(\overline{x})$. Assim, $N'(\varphi(x)) = \varphi(x)\overline{\varphi(x)} = \varphi(x).\varphi(\overline{x}) = \varphi(x\overline{x}) = \varphi(N(x)) = N(x)$. Logo φ é uma isometria de (A, N) em (A', N').

(ii) $\Longleftrightarrow$ **(iii)** Pelo Corolário 2.1.1 temos que $N \simeq \langle 1, -a, -b, ab\rangle$ e $N' \simeq \langle 1, -a', -b', a'.b'\rangle$. Dessa forma, utilizando o Teorema do Cancelamento de Witt, segue a equivalência.

(iii) $\Longrightarrow$ **(i)** Seja $\sigma : \mathrm{A}_0 \longrightarrow \mathrm{A}'_0$ uma isometria. Então, $-a = N(i) = N'(\sigma(i)) = \sigma(i)\overline{\sigma(i)} = -\sigma(i)^2$. Assim, $\sigma(i)^2 = a$. Analogamente, verificamos que $\sigma(j)^2 = b$. Como $i \perp j$, $b_{N'}(\sigma(i), \sigma(j)) = b_N(i, j) = 0$. Assim, $\frac{1}{2}(\sigma(i)\overline{\sigma(j)} + \sigma(j)\overline{\sigma(i)}) = 0$, ou seja, $\sigma(i)\sigma(j) = -\sigma(j)\sigma(i) \in \mathrm{A}'_0$. Então temos a K-base para A′ $\{1, \sigma(i) = i', \sigma(j) = j', \sigma(i)\sigma(j) = k'\}$ e considerando $\varphi : \mathrm{A} \longrightarrow \mathrm{A}'$ tal que $\varphi(1) = 1, \varphi(i) = i', \varphi(j) = j'$ e $\varphi(k) = k'$, verifica-se facilmente que φ é um isomorfismo de K-álgebras. □

Corolário 2.1.2 $\mathrm{A} = \left(\frac{a,a}{\mathrm{K}}\right) \approx \left(\frac{a,-1}{\mathrm{K}}\right) = \mathrm{A}'$.

Demonstração: As formas nornas $\langle 1, -a, -a, a^2\rangle$ e $\langle 1, -a, 1, -a\rangle$ são isométricas. □

Definição 2.1.4 *Uma álgebra* A *é dita com divisão se todo elemento não nulo de* A *é inversível.*

Teorema 2.1.1 *Para* $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right)$ *as seguintes afirmações são equivalentes:*

(1) $\mathrm{A} \approx \left(\frac{1,-1}{\mathrm{K}}\right)$ $(\approx \mathrm{M}_2(\mathrm{K}))$*;*

(2) A *não é uma álgebra com divisão;*

(3) (A, N) *é um espaço quadrático isotrópico ;*

(4) (A, N) *é um espaço quadrático hiperbólico;*

(5) $(\mathrm{A}_0, \langle -a, -b, ab\rangle)$ *é um espaço quadrático isotrópico;*

(6) *A forma quadrática binária* $\langle a, b\rangle$ *representa 1;*

(7) $a \in N_{\mathrm{E}|\mathrm{K}}$*, onde* $\mathrm{E} = \mathrm{K}(\sqrt{b})$.

Demonstração:**(1)** $\Longrightarrow$ **(2)** Como $\mathrm{A} \approx \mathrm{M}_2(\mathrm{K})$ e $\mathrm{M}_2(\mathrm{K})$ tem divisores de zero, segue que A também tem e assim, não é uma álgebra com divisão.

(2) $\Longrightarrow$ **(3)** Existe $x \in \mathrm{A}$ não nulo tal que x não é inversível. Logo pela Proposição 2.1.2(ii), $N(x) = 0$. Portanto (A, N) é um espaço quadrático isotrópico.

(3) $\Longrightarrow$ **(4)** Como N é isotrópica, pelo Corolário 1.4.1(i) $N \simeq \mathbb{H} \perp q$, onde $\mathbb{H}$ é o plano hiperbólico e q uma forma quadrática regular, isto é, $\langle 1, -a, -b, ab\rangle \simeq \mathbb{H} \perp \langle c, d\rangle$. Calculando o determinante, obtemos $d(N) = d(\mathbb{H}).d(\langle c, d\rangle)$ ou $1 = -cd$. Assim $d(\langle c, d\rangle) = -1\dot{\mathrm{K}}^2$. Dessa forma $q \simeq \mathbb{H}$. Logo $N \simeq \mathbb{H} \perp \langle c, d\rangle = 2\mathbb{H}$: uma forma hiperbólica. Portanto (A, N) é um espaço quadrático hiperbólico.

(4) $\Longrightarrow$ **(5)** Como (A, N) é hiperbólico, segue que $N \simeq \langle 1, -1, 1, -1\rangle \simeq \langle 1\rangle \perp \langle -a, -b, ab\rangle$. Pelo Teorema do Cancelamento de Witt, $\langle -a, -b, ab\rangle \simeq \langle -1\rangle \perp \mathbb{H}$. Portanto $\langle -a, -b, ab\rangle$ é isotrópica.

(5) $\Longrightarrow$ **(6)** Por hipótese e Corolário 1.4.1(i) temos que $\langle -a, -b, ab\rangle \supseteq \mathbb{H}$. Portanto $\langle -a, -b, ab\rangle \simeq \mathbb{H} \perp \langle d\rangle$. Calculando o determinante, temos que $d = -1$. Daí $\langle -a, -b, ab\rangle \simeq \langle 1, -1, -1\rangle$. Somando $\langle a, b, 1\rangle$ de ambos os lados, obtemos $\langle 1, a, -a, b, -b, ab\rangle \simeq \langle a, b, 1, 1, -1, -1\rangle$. Como $\langle a, -a\rangle \simeq \mathbb{H} \simeq \langle b, -b\rangle$, cancelando $2\mathbb{H}$ de ambos os lados obtemos $\langle 1, ab\rangle \simeq \langle a, b\rangle$. Daí $1 \in \mathrm{D}(\langle 1, ab\rangle) = \mathrm{D}(\langle a, b\rangle)$. Portanto, $\langle a, b\rangle$ representa 1.

(6) $\Longrightarrow$ **(7)** Se $\sqrt{b} \in \mathrm{K}$, segue por tautologia.

Podemos assumir que $\sqrt{b} \notin \mathrm{K}$.

Para $x + y\sqrt{b} \in \mathrm{E}$ $(x, y \in \mathrm{K})$, temos $N_{\mathrm{E}|\mathrm{K}}(x + y\sqrt{b}) = x^2 - by^2$. Por hipótese temos que $ax_0^2 + by_0^2 = 1$ $(x_0, y_0 \in \mathrm{K})$, onde x_0 não pode ser zero senão $\sqrt{b} \in \mathrm{K}$. Assim,

$a = \dfrac{1}{x_0^2}(1 - by_0^2) = \left(\dfrac{1}{x_0}\right)^2 - b\left(\dfrac{y_0}{x_0}\right)^2 = N_{\mathrm{E|K}}\left(\dfrac{1}{x_0} + \dfrac{y_0}{x_0}\sqrt{b}\right)$. Portanto $a \in N_{\mathrm{E|K}}(\mathrm{E})$.

(7) $\Longrightarrow$ **(2)** Se $d = \sqrt{b} \in \mathrm{K}$ então $d^2 = b = j^2$, assim $(d+j)(d-j) = 0$. Como $\{i, j\}$ são independentes, esta equação diz que A tem divisores de zero.

Se $\sqrt{b} \notin \mathrm{K}$, por hipótese existe uma equação $x^2 - by^2 = a$, onde $x, y \in \mathrm{K}$ e um ou outro é não nulo. O quatérnio não nulo $z = x + i + yj \in \mathrm{A}$ tem norma $z.\overline{z} = x^2 - a - by^2 = 0$. Como $i \neq 0$ então z é um divisor de zero. Como os divisores de zero não são inversíveis, A não é álgebra de divisão.

(2) $\Longrightarrow$ **(1)** Pelo Teorema de Wedderburn, "toda álgebra simples A é isomorfa a uma álgebra de matrizes $\mathrm{M}_m(\mathrm{D})$, onde D é uma álgebra de divisão sobre K", segue-se que neste caso $dim(\mathrm{A}) = 4$ e $dim\mathrm{A} = m^2.dim\mathrm{D}$. Se $m = 1$ então $dim(\mathrm{D}) = 4$ e $\mathrm{A} \approx \mathrm{M}_1(\mathrm{D}) \approx \mathrm{D}$, o que é um absurdo (pois A não é álgebra de divisão e D é). Se $m = 2$ então $dim(\mathrm{D}) = 1$, assim $\mathrm{D} \approx \mathrm{K}$ e $\mathrm{A} \approx \mathrm{M}_2(\mathrm{K})$. □

Observação 2.1.2 *Temos que* $\langle -1, -1\rangle$ *não representa* 1, *quando* $\mathrm{K} = \mathbb{R}$. *Assim a álgebra de quatérnios* $\left(\dfrac{-1,-1}{\mathrm{K}}\right)$ *é uma álgebra com divisão pelo Teorema 2.1.1. Por outro lado uma álgebra de quatérnios sobre* $\mathbb{R}$ *será isomorfa à* $\left(\dfrac{1,-1}{\mathbb{R}}\right)$ *ou* $\left(\dfrac{-1,-1}{\mathbb{R}}\right)$ *(Proposição 2.0.1(i)) desde que* $\dot{\mathbb{R}} = 1.\dot{\mathbb{R}}^2 \cup (-1)\dot{\mathbb{R}}^2$. *Assim, existem essencialmente duas álgebras de quatérnios sobre o corpo* $\mathbb{R}$, *a saber:* $\left(\dfrac{1,-1}{\mathbb{R}}\right)$ *e* $\left(\dfrac{-1,-1}{\mathbb{R}}\right)$.

Definição 2.1.5 *Dizemos que uma álgebra de quatérnios* $\mathrm{A} = \left(\dfrac{a,b}{\mathrm{K}}\right)$ *se fatora, se ela satisfaz uma das condições (portanto todas) do Teorema anterior.*

Corolário 2.1.3 (i) *Se* $a \in \dot{\mathrm{K}}$, *então as álgebras de quatérnios* $\left(\dfrac{1,a}{\mathrm{K}}\right), \left(\dfrac{a,-a}{\mathrm{K}}\right)$ *se fatoram;*

(ii) *Se* $a \neq 0, 1$, *então* $\left(\dfrac{a,1-a}{\mathrm{K}}\right)$ *também se fatora.*

Demonstração: As formas binárias $\langle 1, a\rangle, \langle a, -a\rangle, \langle a, 1-a\rangle$ representam 1. Pelo ítem (i) do Teorema 2.1.1 elas se fatoram. □

Exemplo 2.1.1 $\left(\frac{1,-1}{\mathrm{K}}\right)$ *se fatora, pois sua forma norma* $\langle 1,-1,1,-1\rangle$ *é hiperbólica.*

Corolário 2.1.4 *(Linearidade) Para* $a,b,c \in \dot{\mathrm{K}}$*, temos:*
$\left(\frac{a,b}{\mathrm{K}}\right) \otimes \left(\frac{a,c}{\mathrm{K}}\right) \approx \left(\frac{a,bc}{\mathrm{K}}\right) \otimes \left(\frac{c,-a^2c}{\mathrm{K}}\right) \approx \left(\frac{a,bc}{\mathrm{K}}\right) \otimes \mathrm{M}_2(\mathrm{K})$.

Demonstração: Sejam $\{1,i,j,k\}$ e $\{1,i',j',k'\}$ bases de $\mathrm{A} = \left(\frac{a,b}{\mathrm{K}}\right)$ e $\mathrm{A}' = \left(\frac{a,c}{\mathrm{K}}\right)$, respectivamente. Queremos analisar o produto tensorial das álgebras, ou seja, $\mathrm{A} \otimes \mathrm{A}'$. Consideremos $\mathrm{X} = \mathrm{K}(1\otimes 1) + \mathrm{K}(i\otimes 1) + \mathrm{K}(j\otimes j') + \mathrm{K}(k\otimes j') = \mathrm{K}.1 + \mathrm{K}.I + \mathrm{K}.J + \mathrm{K}.(IJ)$, pois $(i\otimes 1)(j\otimes j') = (ij)\otimes(1j') = k\otimes j'$, onde $I = i\otimes 1$ e $J = j\otimes j'$. Esta é uma subálgebra de dimensão 4 de $\mathrm{A}\otimes\mathrm{A}'$. De fato, temos que $I^2 = (i\otimes 1)(i\otimes 1) = i^2\otimes 1 = a\otimes 1 = a$, $J^2 = j^2\otimes j'^2 = b\otimes c = bc$ e $-IJ = -(i\otimes 1)(j\otimes j') = -ij\otimes j' = ji\otimes j' = JI$. Assim a subálgebra X é uma cópia da álgebra dos quatérnios $\left(\frac{a,bc}{\mathrm{K}}\right)$.

Também temos , $\mathrm{Y} = \mathrm{K}(1\otimes 1)+\mathrm{K}(1\otimes j')+\mathrm{K}(i\otimes k')+\mathrm{K}(-ci\otimes i') = \mathrm{K}.1+\mathrm{K}.\tilde{I}+\mathrm{K}.\tilde{J}+\mathrm{K}.\tilde{K}$ $(\tilde{I} = 1\otimes j', \tilde{J} = i\otimes k', \tilde{K} = i\otimes -ci')$, onde $\tilde{I}^2 = 1\otimes j'^2 = c, \tilde{J}^2 = i^2\otimes k'^2 = -a^2c, \tilde{I}\tilde{J} = i\otimes j'k' = i\otimes(-ci')$ e $\tilde{J}\tilde{I} = i\otimes k'j' = -\tilde{K} = -\tilde{I}\tilde{J}$. Dessa forma Y também é uma cópia da álgebra de quatérnios $\left(\frac{c,-a^2c}{\mathrm{K}}\right)$. Pelos ítens (i) da Proposição 2.0.1 e (i) do Corolário 2.1.3, temos que $\mathrm{Y} \approx \left(\frac{c,-a^2c}{\mathrm{K}}\right) \approx \left(\frac{c,-c}{\mathrm{K}}\right) \approx \mathrm{M}_2(\mathrm{K})$.

Para completar a prova é suficiente demonstrar que $\mathrm{A}\otimes\mathrm{A}'$ é o produto tensorial das subálgebras X e Y. Primeiro observemos que os elementos de $\{1,I,J,K\}$ comutam com os elementos de $\{1,\tilde{I},\tilde{J},\tilde{K}\}$. Por exemplo,
$I\tilde{J} = (i\otimes 1)(i\otimes k') = (i^2\otimes k') = (i\otimes k')(i\otimes 1) = \tilde{J}I$, $K\tilde{J} = (k\otimes j')(i\otimes k') = ki\otimes j'k' = (-ik)\otimes(-k'j') = (ik)\otimes(k'j') = (i\otimes k')(k\otimes j') = \tilde{J}K$, e analogamente se verifica que os outros elementos também comutam.

Uma base para $\mathrm{X}\otimes\mathrm{Y}$ é o produto das bases de X e de Y. Assim
$\mathrm{B} = \{1\otimes 1 = e_1,\ 1\otimes\tilde{I} = e_2,\ 1\otimes\tilde{J} = e_3,\ 1\otimes\tilde{K} = e_4,\ I\otimes 1 = e_5,\ I\otimes\tilde{I} = e_6,\ I\otimes\tilde{J} = e_7,\ I\otimes\tilde{K} = e_8,\ J\otimes 1 = e_9,\ J\otimes\tilde{I} = e_{10},\ J\otimes\tilde{J} = e_{11},\ J\otimes\tilde{K} = e_{12},\ K\otimes 1 = e_{13},\ K\otimes\tilde{I} = e_{14},\ K\otimes\tilde{J} = e_{15},\ K\otimes\tilde{K} = e_{16}\}$.

Cada elemento de B é da forma $x\otimes y$, com $x\in\{1,I,J,K\}$ e $y\in\{1,\tilde{I},\tilde{J},\tilde{K}\}$. Definimos $\varphi : \mathrm{X}\otimes\mathrm{Y} \longrightarrow \mathrm{A}\otimes\mathrm{A}'$ tal que $\varphi(x\otimes y) = xy$, com $x\otimes y\in\mathrm{B}$ e estendemos por linearidade. Como os elementos da base de X e de Y comutam entre si temos que se $x\otimes y,\ x_1\otimes y_1\in\mathrm{B}$, então $\varphi((x\otimes y).(x_1\otimes y_1)) = \varphi((xx_1)\otimes(yy_1)) = xx_1.yy_1 = xy.x_1y_1 = \varphi(x\otimes y).\varphi(x_1\otimes y_1)$.

Dessa forma temos que $\varphi(Z.W) = \varphi(Z).\varphi(W)$, para todos $Z,\ W \in \mathrm{X} \otimes \mathrm{Y}$. Como φ é linear e $dim(\mathrm{X} \otimes \mathrm{Y}) = 16 = dim(\mathrm{A} \otimes \mathrm{A}')$, se demonstrarmos que φ é sobrejetora teremos um isomorfismo linear entre $\mathrm{X} \otimes \mathrm{Y}$ e $\mathrm{A} \otimes \mathrm{A}'$. E assim $\mathrm{X} \otimes \mathrm{Y} \approx \mathrm{A} \otimes \mathrm{A}'$ como K-álgebras.

Para mostrar que φ é sobrejetora, basta verificar que um conjunto de geradores de $\mathrm{A} \otimes \mathrm{A}'$ é C= $\{1, i, j, k\} \otimes \{1, i', j', k'\}$. Fazendo os cálculos, temos:
$\varphi(e_1) = 1 \otimes 1,\ \varphi(e_2) = 1 \otimes j',\ \varphi(e_3) = i \otimes k',\ \varphi(e_4) = -c(i \otimes i')$. Isto implica que $\left(-\dfrac{e_4}{c}\right) = i \otimes i',\ \varphi(e_5) = i \otimes 1,\ \varphi(e_6) = i \otimes j',\ \varphi(e_7) = a(1 \otimes k')$. Segue que $\varphi\left(\dfrac{1}{a}e_7\right) = 1 \otimes k'$, e assim por diante. Com este processo podemos ver que cada elemento de C é da forma $\varphi(\alpha_i e_i)$, para algum $\alpha_i \in \mathrm{K}$ e e_i conveniente. Isto completa a prova. □

2.2 Corpos Finitos

Seja $\mathrm{K} = \mathbb{K}_q$ um corpo finito com q ($= p^m$, p : primo e $p \neq 2$) elementos. Temos que $\dot{\mathrm{K}}$ é grupo cíclico de ordem par ($|\dot{\mathrm{K}}| = q - 1$). Seja s o gerador de $\dot{\mathrm{K}}$. Dessa forma $\dot{\mathrm{K}} = \dot{\mathrm{K}}^2 \cup s\dot{\mathrm{K}}^2$, ou então $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} = \{\dot{\mathrm{K}}^2, s\dot{\mathrm{K}}^2\}$, que também representamos por $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} = \{\overline{1}, \overline{s}\}$. Concluímos então que $\left|\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}\right| = 2$, ou seja, todo corpo finito tem duas classes de quadrados. Temos ainda que, $-1 \in \dot{\mathrm{K}}^2 \iff \mathrm{q} \equiv 1(mod 4)$, e $-1 \notin \dot{\mathrm{K}}^2 \iff \mathrm{q} \equiv 3(mod 4)$ e neste caso podemos tomar $s = -1$.

Proposição 2.2.1 *Seja* $\mathrm{K} = \mathbb{K}_q$, *e* $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} = \{1, s\}$. *Então* s *é uma soma de dois quadrados.*

Demonstração: Temos dois casos a considerar:

(i) Se $-1 \in \dot{\mathrm{K}}^2$, então $\langle 1, 1\rangle \simeq \langle 1, -1\rangle = \mathbb{H}$. Pelo Corolário 1.4.1 (ii) , temos que $\langle 1, 1\rangle$ é universal. Logo $s = x^2 + y^2$, para algum $x, y \in \dot{\mathrm{K}}$.

(ii) Se $-1 \notin \dot{\mathrm{K}}^2$, temos que os conjuntos $\dot{\mathrm{K}}^2$ e $1 + \dot{\mathrm{K}}^2$ tem a mesma cardinalidade, igual a $\dfrac{q-1}{2}$ e são distintos pois $1 \in \dot{\mathrm{K}}^2$, mas $1 \notin 1 + \dot{\mathrm{K}}^2$. Assim, existe $1 + z^2$ que não pertence a $\dot{\mathrm{K}}^2$ e $1 + z^2 \neq 0$ (pois $-1 \notin \dot{\mathrm{K}}^2$). Portanto podemos tomar $s = 1 + z^2$, isto é, s é uma soma de dois quadrados. □

Consideremos a forma quadrática binária $q = \langle a, b\rangle$, com $a, b \in \dot{\mathrm{K}}$. Assim, $a, b \in \left\{\overline{1}, \overline{s}\right\}$,

o que implica que a e b são da forma $1r^2$ ou sr^2. Logo as formas binárias regulares sobre K, a menos de isometria, são $\langle 1,1\rangle, \langle 1,s\rangle$ e $\langle s,s\rangle$.

Proposição 2.2.2 *Toda forma quadrática binária regular sobre um corpo finito é universal. Além disso, existe uma única forma quadrática binária anisotrópica, dependendo do corpo.*

Demonstração: É evidente que $\langle 1,s\rangle$ representa 1 e s, logo é universal.

Verifiquemos $\langle 1,1\rangle$ e $\langle s,s\rangle$. Como $\langle 1,1\rangle$ representa 1, temos que $\langle 1,1\rangle$ é universal. Além disso, pelo Critério de Representação $\langle 1,1\rangle \simeq \langle s,x\rangle$ e calculando o determinante, temos que $x = s$. Portanto $\langle 1,1\rangle \simeq \langle s,s\rangle$. Logo $\langle s,s\rangle$ também é universal.

Se $-1 \in \dot{\mathrm{K}}^2$ então $\langle 1,1\rangle \simeq \langle 1,-1\rangle = \mathbb{H}$, e como $\langle s,s\rangle \simeq \langle 1,1\rangle$, segue que $\langle 1,1\rangle$ e $\langle s,s\rangle$ são isotrópicas. Logo a única forma binária anisotrópica é $\langle 1,s\rangle$, isto segue do Teorema 1.4.1(ii).

Se $-1 \notin \dot{\mathrm{K}}^2$, podemos tomar $s = -1$ $\left(\text{ou seja, } \dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} = \{1,-1\}\right)$. Dessa forma $\langle 1,s\rangle \simeq \mathbb{H}$, e portanto é isotrópica. Segue do Teorema 1.4.1(ii) que $\langle 1,1\rangle \simeq \langle s,s\rangle$ é anisotrópica e é única a menos de isometria. □

Corolário 2.2.1 *Se* K *é um corpo finito, então* $\left(\dfrac{a,b}{\mathrm{K}}\right)$ *se fatora.*

Demonstração: Toda forma binária é universal, logo representa 1. Portanto, pelo item (6) do Teorema 2.1.1, segue o resultado. □

Observação 2.2.1 *Como toda álgebra de quatérnios sobre um corpo finito se fatora, existe essencialmente uma álgebra de quatérnios sobre um corpo finito* K*, a saber* $\left(\dfrac{1,-1}{\mathrm{K}}\right)$.

A teoria de álgebra de quatérnios pode ser usada para classificar formas quadráticas binárias.

Corolário 2.2.2 *(Classificação de formas quadráticas binárias) As formas quadráticas regulares* $q = \langle a,b\rangle$ *e* $q_1 = \langle c,d\rangle$ *são isométricas se, e somente se,* $d(q) = d(q_1)$ *e* $\left(\dfrac{a,b}{\mathrm{K}}\right) \approx \left(\dfrac{c,d}{\mathrm{K}}\right)$.

Demonstração: ($\Longrightarrow$) Se $\langle a,b\rangle \simeq \langle c,d\rangle$, então $ab = cd$, isto é, $d(q) = d(q_1)$. E mais, $\langle 1,-a,-b,ab\rangle \simeq \langle -1\rangle(\langle -1,a,b,-ab\rangle) \simeq \langle -1\rangle(\langle -1,c,d,-cd\rangle) \simeq \langle 1,-c,-d,cd\rangle$. Logo pela

Proposição 2.1.3, $\left(\frac{a,b}{\mathrm{K}}\right) \approx \left(\frac{c,d}{\mathrm{K}}\right)$.

($\Longleftarrow$) Se $ab = cd$ e $\left(\frac{a,b}{\mathrm{K}}\right) \approx \left(\frac{c,d}{\mathrm{K}}\right)$, então pela Proposição 2.1.3 , $\langle 1, -a, -b, ab\rangle \simeq \langle 1, -c, -d, cd\rangle$. Cancelando $\langle ab\rangle$, $\langle 1\rangle$ (pelo Teorema do Cancelamento de Witt), temos que $\langle -a, -b\rangle \simeq \langle -c, -d\rangle$. Portanto $q \simeq q_1$. □

Capítulo 3

Invariante de Hasse

3.1 O Grupo de Brauer

Esta seção é uma breve introdução ao grupo de Brauer, o suficiente para definir o invariante de Hasse de uma forma quadrática.

Definição 3.1.1 *Seja* A *uma* K*-álgebra. Para um subconjunto* $S \subset \mathrm{A}$*, definimos o centralizador de* S *em* A *como:*

$$C_{\mathrm{A}}(S) = \{x \in \mathrm{A} \mid xs = sx, \textit{para todos} \in S\}.$$

É imediata a verificação de que $C_{\mathrm{A}}(S)$ é uma subálgebra de A. No caso em que $S = \mathrm{A}$, $C_{\mathrm{A}}(\mathrm{A})$ é exatamente o centro de A, $Z(\mathrm{A})$, conforme definido em 2.0.3 (i).

Teorema 3.1.1 *Sejam* A *e* B K*-álgebras, e* $\mathrm{A}' \subset \mathrm{A}$, $\mathrm{B}' \subset \mathrm{B}$ K*-subálgebras então:*

(i) $C_{\mathrm{A}\otimes\mathrm{B}}(\mathrm{A}' \otimes \mathrm{B}') = C_{\mathrm{A}}(\mathrm{A}') \otimes C_{\mathrm{B}}(\mathrm{B}')$*. Em particular, se* A *e* B *são centrais então* $\mathrm{A} \otimes \mathrm{B}$ *é central ;*

(ii) *Se* A *é central simples e* B *é simples, então* $\mathrm{A} \otimes \mathrm{B}$ *é uma* K*-álgebra simples;*

(iii) *Se* A *e* B *são centrais simples então* $\mathrm{A} \otimes \mathrm{B}$ *é uma* K*-álgebra central simples.*

Demonstração: **(i)** $C_{\mathrm{A}}(\mathrm{A}') \otimes C_{\mathrm{B}}(\mathrm{B}') \subset C_{\mathrm{A}\otimes\mathrm{B}}(\mathrm{A}' \otimes \mathrm{B}')$ (pela definição de produto tensorial).

Sejam $\{b_1, \ldots, b_n\}$ uma K-base de B e $x \in C_{\mathrm{A}\otimes\mathrm{B}}(\mathrm{A}' \otimes \mathrm{B}')$. Assim, $x = x_1 \otimes b_1 + \cdots + x_n \otimes b_n$, onde $x_i \in \mathrm{A}$ são unicamente determinados. Para todo $a \in \mathrm{A}'$, temos que $(a \otimes 1)x = x(a \otimes 1)$,

portanto $(ax_1) \otimes b_1 + \cdots + (ax_n) \otimes b_n = (x_1a) \otimes b_1 + \cdots + (x_na) \otimes b_n$ o que implica que $x_i \in C_{\mathrm{A}}(\mathrm{A}')$, pela unicidade da representação.

Seja $\{a_1, \ldots, a_k\}$ uma K-base de A. Então podemos escrever $x = a_1 \otimes y_1 + \cdots + a_k \otimes y_k$ onde $y_i \in \mathrm{B}$ são unicamente determinados. Logo para todo $b \in \mathrm{B}'$, temos $(1 \otimes b)x = x(1 \otimes b)$, assim $a_1 \otimes (by_1) + \cdots + a_k \ldots (by_k) = a_1 \otimes (y_1b) + \cdots + a_k \otimes (y_kb)$, o que implica que $y_i \in C_{\mathrm{B}}(\mathrm{B}')$. Portanto $x \in C_{\mathrm{A}}(\mathrm{A}') \otimes C_{\mathrm{B}}(\mathrm{B}')$.

(ii) Seja I um ideal bilateral não nulo de $\mathrm{A} \otimes \mathrm{B}$. Mostremos que $\mathrm{I} = \mathrm{A} \otimes \mathrm{B}$.

Assumamos que I contém um elemento $a \otimes b \neq 0$. O ideal bilateral de A gerado por a é A (pois A é central simples). Assim existem a_i's, a_i''s elementos de A tais que $\sum a_i a a_i' = 1$. Portanto $\sum (a_i \otimes 1)(a \otimes b)(a_i' \otimes 1) = 1 \otimes b \in \mathrm{I}$.

O mesmo argumento aplicado à b nos dá $1 \otimes 1 \in \mathrm{I}$.

Em geral, escolhemos $x \in \mathrm{I}$ e uma representação $x = a_1 \otimes b_1 + \cdots + a_k \otimes b_k$, $a_i \in \mathrm{A}, b_i \in \mathrm{B}$ tal que k é o menor possível. Usando o mesmo argumento para a_k, podemos assumir sem perda de generalidade que $a_k = 1$.

Admita agora $k > 1$. Então a_{k-1} e a_k são linearmente independentes, pois se $a_{k-1} = \lambda a_k$, tomando um k menor para $a_{k-1} \otimes b_{k-1} + a_k \otimes b_k = a_k \otimes (\lambda b_{k-1} + b_k)$. Como A é central $a_{k-1} \notin C(\mathrm{A})$. Assim existe $a \in \mathrm{A}$ tal que $aa_{k-1} - a_{k-1}a \neq 0$.

Consideramos agora o comutador $(a \otimes 1)x - x(a \otimes 1) = (aa_1 - a_1a) \otimes b_1 + \cdots + (aa_k - a_{k-1}a) \otimes b_{k-1}$. Como os $b_i's$ são linearmente independentes e o somando acima é não nulo, a soma total é não nula. Assim, construímos um elemento em I com um k menor. Portanto $k = 1$ e reduzimos o problema ao caso considerado acima.

(iii) É consequência de (i) e (ii). □

O objetivo de construir o grupo de Brauer é classificar todas álgebras centrais simples sobre K por uma relação de equivalência, e então construir uma estrutura de grupo no conjunto das classes de equivalências pelo produto tensorial.

Definição 3.1.2 *Duas álgebras centrais simples* A *e* A′ *são ditas similares* ($\mathrm{A} \sim \mathrm{A}'$) *se existem espaços vetoriais* V *e* V′ *de dimensões finitas sobre* K *tais que:*

$$\mathrm{A} \otimes End\mathrm{V} \approx \mathrm{A}' \otimes End\mathrm{V}' \quad \textit{como } \mathrm{K}\textit{-álgebras},$$

onde $End(\mathrm{V})$ *é a álgebra dos endomorfismos do espaço vetorial* V.

Similaridade é uma relação de equivalência, pois:

(i) $\mathrm{A} \sim \mathrm{A}$ (reflexiva);

(ii) $\mathrm{A} \sim \mathrm{B} \Longrightarrow \mathrm{B} \sim \mathrm{A}$ (simétrica);

(iii) Se $\mathrm{A} \sim \mathrm{B}$ e $\mathrm{B} \sim \mathrm{C}$ então $\mathrm{A} \sim \mathrm{C}$ (transitiva).

Considere o fato que $End\mathrm{V}_1 \otimes End\mathrm{V}_2 \approx End(\mathrm{V}_1 \otimes \mathrm{V}_2)$.

Como $\mathrm{A} \sim \mathrm{B}$ e $\mathrm{B} \sim \mathrm{C}$, existem espaços vetoriais $\mathrm{V}_1, \mathrm{V}_2, \mathrm{V}_3, \mathrm{V}_4$ sobre K tais que $\mathrm{A} \otimes End\mathrm{V}_1 \approx \mathrm{B} \otimes End\mathrm{V}_2$ e $\mathrm{B} \otimes End\mathrm{V}_3 \approx \mathrm{C} \otimes End\mathrm{V}_4$. Logo, $\mathrm{A} \otimes End(\mathrm{V}_1 \otimes \mathrm{V}_3) \approx \mathrm{A} \otimes (End\mathrm{V}_1 \otimes End\mathrm{V}_3) \approx (\mathrm{A} \otimes End\mathrm{V}_1) \otimes End\mathrm{V}_3 \approx (\mathrm{B} \otimes End\mathrm{V}_2) \otimes End\mathrm{V}_3 \approx \mathrm{B} \otimes End(\mathrm{V}_2 \otimes \mathrm{V}_3) \approx \mathrm{B} \otimes (End\mathrm{V}_3 \otimes End\mathrm{V}_2) \approx (\mathrm{C} \otimes End\mathrm{V}_4) \otimes End\mathrm{V}_2 \approx \mathrm{C} \otimes End(\mathrm{V}_4 \otimes \mathrm{V}_2)$. Logo $\mathrm{A} \sim \mathrm{C}$.

O conjunto das classes de similaridades será denotado por $Br(\mathrm{K})$.

Notação: [A]: classe de equivalência da álgebra central simples A.

Definição 3.1.3 (i) *A aplicação* $Br(\mathrm{K}) \times Br(\mathrm{K}) \longrightarrow Br(\mathrm{K})$ *dada por* $[\mathrm{A}_1].[\mathrm{A}_2] = [\mathrm{A}_1 \otimes \mathrm{A}_2]$ *é a classe do produto tensorial de álgebras centrais simples.*

O produto está bem definido, pois: se $\mathrm{A}_1 \sim \mathrm{A}_1'$ e $\mathrm{A}_2 \sim \mathrm{A}_2'$ então

$$\begin{cases} \mathrm{A}_1 \otimes End\mathrm{V}_1 \approx \mathrm{A}_1' \otimes End\mathrm{V}_1' \\ \mathrm{A}_2 \otimes End\mathrm{V}_2 \approx \mathrm{A}_2' \otimes End\mathrm{V}_2'. \end{cases}$$

Logo, $(\mathrm{A}_1 \otimes End\mathrm{V}_1) \otimes (\mathrm{A}_2 \otimes End\mathrm{V}_2) \approx (\mathrm{A}_1' \otimes End\mathrm{V}_1') \otimes (\mathrm{A}_2' \otimes End\mathrm{V}_2')$. Portanto $(\mathrm{A}_1 \otimes \mathrm{A}_2) \otimes End(\mathrm{V}_1 \otimes \mathrm{V}_2) \approx (\mathrm{A}_1' \otimes \mathrm{A}_2') \otimes End(\mathrm{V}_1' \otimes \mathrm{V}_2')$, isto é, $[\mathrm{A}_1 \otimes \mathrm{A}_2] = [\mathrm{A}_1' \otimes \mathrm{A}_2']$. Como $\mathrm{A}_1 \otimes (\mathrm{A}_2 \otimes \mathrm{A}_3) \approx (\mathrm{A}_1 \otimes \mathrm{A}_2) \otimes \mathrm{A}_3$ e $\mathrm{A}_1 \otimes \mathrm{A}_2 \approx \mathrm{A}_2 \otimes \mathrm{A}_1$, o produto é associativo e comutativo.

(ii) *A classe das álgebras de matrizes* $\mathrm{M}_n(\mathrm{K})$ *é o elemento neutro deste produto, pois* $[\mathrm{A}].[\mathrm{M}_n(\mathrm{K})] = [\mathrm{A} \otimes \mathrm{M}_n(\mathrm{K})] = [\mathrm{A}]$*, desde que* $\mathrm{A} \otimes \mathrm{M}_n(\mathrm{K}) \sim \mathrm{A}$*. Temos também que* $[\mathrm{K}] = [\mathrm{M}_n(\mathrm{K})] = [End\mathrm{V}]$.

Para exibir um inverso para cada elemento de $Br(\mathrm{K})$, definiremos a álgebra oposta.

Definição 3.1.4 *Seja* A *uma álgebra. A álgebra oposta de* A*, denotada por* A^{op}*, é a álgebra tal que como conjunto* $\mathrm{A}^{op} = \mathrm{A}$*, a multiplicação de* A^{op} *é dada por* $a \odot b = ba$ *e as outras*

operações (adição e multiplicação por escalares), permanecem as mesmas de A. *Observe que* $\mathrm{A} = \mathrm{A}^{op}$ *como grupo abeliano aditivo.*

Proposição 3.1.1 *Seja* A *uma álgebra central simples. Então* $\mathrm{A} \otimes \mathrm{A}^{op} \approx End\mathrm{A}$ *(álgebra dos endomorfismos do* K*-espaço vetorial* A*).*

Em particular, $Br(\mathrm{K})$ *é um grupo comutativo, com* $[\mathrm{A}]^{-1} = [\mathrm{A}^{op}]$. *O grupo* $Br(\mathrm{K})$ *é dito grupo de Brauer de* K.

Demonstração: Provemos que $\mathrm{A} \otimes \mathrm{A}^{op} \approx End\mathrm{A}$, onde A é considerado como um K-espaço vetorial.

Para $a \in \mathrm{A}$, $b \in \mathrm{A}^{op}$, a aplicação $\psi_{a,b} : \mathrm{A} \longrightarrow \mathrm{A}$, dada por $\psi_{a,b}(x) = axb$ é um endomorfismo do K-espaço vetorial A, pois $\psi_{a,b}(\alpha x+y) = a(\alpha x+y)b = a(\alpha xb+yb) = a\alpha xb+ ayb = \alpha(axb)+ayb = \alpha\psi_{a,b}(x)+\psi_{a,b}(y)$. Isto define uma aplicação $\psi : \mathrm{A} \times \mathrm{A}^{op} \longrightarrow End_{\mathrm{K}}(\mathrm{A})$, dada por $\psi(a,b) = \psi_{a,b}$. Esta aplicação é bilinear pois, $\psi(\alpha x + y, z)(t) = \psi_{\alpha x+y,z}(t) = (\alpha x + y)tz = \alpha xtz + ytz = \alpha\psi_{x,z}(t) + \psi_{y,z}(t) = (\alpha\psi_{x,z} + \psi_{y,z})(t) = (\alpha\psi(x,z) + \psi(y,z))(t)$.

E como $\psi_{ac,b\circ d}(x) = a(cxd)b = \psi_{a,b}(cxd) = \psi_{a,b}(\psi_{c,d}(x)) = (\psi_{a,b} \circ \psi_{c,d})(x)$, também é multiplicativa. Assim, existe um homomorfismo de K-álgebras $\varphi : \mathrm{A} \otimes \mathrm{A}^{op} \longrightarrow End\mathrm{A}$.

Como $\mathrm{A} \otimes \mathrm{A}^{op}$ é álgebra simples, φ é injetivo (pois o núcleo de φ é 0). Como as dimensões de $\mathrm{A} \otimes \mathrm{A}^{op}$ e de $End\mathrm{A}$ coincidem, φ é sobrejetora. Portanto $\mathrm{A} \otimes \mathrm{A}^{op} \approx End(\mathrm{A})$. □

Para um dado corpo K, precisamos saber como representar um elemento de $Br(\mathrm{K})$.

Pelo teorema de Wedderburn, temos que "toda K-álgebra central simples A é isomorfa a $\mathrm{M}_n(\mathrm{D})$, onde D é uma K-álgebra central com divisão". Assim $\mathrm{A} \approx \mathrm{M}_n(\mathrm{D}) \approx \mathrm{D} \otimes \mathrm{M}_n(\mathrm{K})$, o que implica que $[\mathrm{A}] = [\mathrm{D}]$ em $Br(\mathrm{K})$. Além disso, este teorema diz que "A é unicamente determinada por D". Dessa forma, se D e D' são álgebras centrais simples com divisão e $[\mathrm{D}] = [\mathrm{D}']$ em $Br(\mathrm{K})$, então existem $m, n \in \mathbb{N}$ tais que $\mathrm{D} \otimes \mathrm{M}_n(\mathrm{K}) \approx \mathrm{D}' \otimes \mathrm{M}_m(\mathrm{K})$. Isto implica que $\mathrm{M}_n(\mathrm{D}) \approx \mathrm{M}_m(\mathrm{D}')$. Portanto $\mathrm{D} \approx \mathrm{D}'$ e $n = m$.

Como consequência, temos:

Proposição 3.1.2 *Seja* K *um corpo. Os elementos de* $Br(\mathrm{K})$ *estão em correspondência 1 a 1 com as classes de isomorfismos das* K*-álgebras centrais com divisão* D. *A correspondência é* $\mathrm{D} \longleftrightarrow [\mathrm{D}]$.

Em geral, a classe das álgebras de quatérnios não formam um subgrupo de $Br(\mathrm{K})$. No entanto, cada classe de álgebra de quatérnios com divisão representa um elemento de ordem 2 em $Br(\mathrm{K})$. De fato, $\left(\frac{a,b}{\mathrm{K}}\right) \otimes \left(\frac{a,b}{\mathrm{K}}\right) \approx \left(\frac{a,b^2}{\mathrm{K}}\right) \otimes \mathrm{M}_2(\mathrm{K}) \approx \left(\frac{a,1}{\mathrm{K}}\right) \otimes \mathrm{M}_2(\mathrm{K})$. Pelo Teorema 2.1.1, segue que $\left[\left(\frac{a,b}{\mathrm{K}}\right)\right]^2 = 1$ em $Br(\mathrm{K})$. Também temos que o subgrupo de $Br(\mathrm{K})$ gerado pelas classes de isomorfismos de álgebras de quatérnios tem expoente 1 ou 2, porém não se sabe se este subgrupo contém todos elementos de ordem 2 de $Br(\mathrm{K})$.

3.2 Invariante de Hasse

Definição 3.2.1 *Seja* (V, q) *um espaço quadrático. Se* $\langle a_1, \ldots, a_n\rangle$ *é uma diagonalização de* q*, definimos o invariante de Hasse, como sendo a classe de* $s(q) = \prod_{1\leq i<j}^{n} \left[\left(\frac{a_i, a_j}{\mathrm{K}}\right)\right]$ *no grupo de Brauer* $Br(\mathrm{K})$ *(onde* $s(q) = 1$ *se* $n = 1$*).*

Observação 3.2.1 *Por comodidade, denotaremos* $\left[\left(\frac{a_i, a_j}{\mathrm{K}}\right)\right] \in Br(\mathrm{K})$ *por* $[a_i, a_j]$*.*

Proposição 3.2.1 *Dada uma forma quadrática* q *sobre* K*, temos que* $s(q)$ *independe da diagonalização de* q*, depende apenas da classe de isometrias de* q*.*

Demonstração: Sejam $q_1 = \langle a_1, \ldots, a_n\rangle$ e $q_2 = \langle b_1, \ldots, b_n\rangle$ duas diagonalizações de q. Então q_1 e q_2 são isométricas e portanto equivalentes por cadeia (Teorema de Equivalência por Cadeia). Dessa forma é suficiente comparar duas diagonalizações $\langle a, b, a_3, \ldots, a_n\rangle$ e $\langle c, d, a_3, \ldots, a_n\rangle$ com $\langle a, b\rangle \simeq \langle c, d\rangle$.

Pela isometria acima, segue do Corolário 2.2.2 que $ab = cd$ e $\left(\frac{a,b}{\mathrm{K}}\right) \approx \left(\frac{c,d}{\mathrm{K}}\right)$. Por Linearidade (Corolário 2.1.4), temos

$s(\langle a, b, a_3, \ldots, a_n\rangle) = [a, ba_3 \ldots a_n][b, a_3 \ldots a_n].\prod_{3\leq i<j}^{n}[a_i, a_j] = [a, b][a, a_3 \ldots a_n][b, a_3 \ldots a_n].$
$.\prod_{3\leq i<j}^{n}[a_i, a_j] = [a, b][ab, a_3 \ldots a_n].\prod_{3\leq i<j}^{n}[a_i, a_j] = [c, d][cd, a_3 \ldots a_n].\prod_{3\leq i<j}^{n}[a_i, a_j] = [c, d]$
$[c, a_3 \ldots a_n][d, a_3 \ldots a_n].\prod_{3\leq i<j}^{n}[a_i, a_j] = [c, da_3 \ldots a_n][d, a_3 \ldots a_n].\prod_{3\leq i<j}^{n}[a_i, a_j] =$
$s(\langle c, d, a_3, \ldots, a_n\rangle)$. Logo $s(q_1) = s(q_2)$. □

Teorema 3.2.1 *Sejam q e q_1 formas quadráticas sobre* K *tais que* $dimq \leq 3$, $dimq_1 \leq 3$. *Então,* $q \simeq q_1$ *se, e somente se,* $s(q) = s(q_1)$, $d(q) = d(q_1)$ *e* $dim(q) = dim(q_1)$.

Demonstração: ($\Longrightarrow$) Óbvia, pelo que já foi visto.

($\Longleftarrow$) Se $dim(q) = dim(q_1) = 2$, o resultado segue do Corolário 2.2.2.

Suponhamos então $dim(q) = dim(q_1) = 3$ e sejam $d = det(q) = det(q_1)$, $q \simeq \langle a, b, c\rangle$ e $q_1 \simeq \langle a_1, b_1, c_1\rangle$. Logo $s(\langle -d\rangle q) = s(\langle -ad, -bd, -cd\rangle) = [-ad, (-bd)(-cd)]$ $[-bd, -cd] = [-ad, bc][b(-d), c(-d)] = [a, b][a, c][-d, b][-d, c][b, c][b, -d][-d, c][-d, -d][a, b]$ $[a, c][b, c][-d, b]^2[-d, c]^2[-d, -d] = s(q)[-d, -d]$. Como $d = abc$, temos $\langle -d\rangle q \simeq \langle -abc\rangle$ $\langle a, b, c\rangle \simeq \langle -bc, -ac, -ab\rangle = \langle x, y, -xy\rangle$, onde $x = -bc$, $y = -ac$ e $s(\langle -d\rangle q) = s(\langle x, y, -xy\rangle)$ $= [x, y][x, -xy][y, -xy] = [x, y][xy, -xy] = [x, y]$. Do mesmo modo, $s(\langle -d\rangle q_1) =$ $s(\langle x_1, y_1, -x_1y_1\rangle) = [x_1, y_1][x_1, -x_1y_1][y_1, -x_1y_1] = [x_1, y_1][x_1y_1, -x_1y_1] = [x_1, y_1] = [x, y]$, pois $s(\langle -d\rangle q) = s(\langle -d\rangle q_1)$. Assim suas formas normas são isométricas, ou seja, $\langle 1, -x, -y, xy\rangle \simeq \langle 1, -x_1, -y_1, x_1y_1\rangle$. Pelo Teorema do Cancelamento de Witt, $\langle -x, -y, xy\rangle$ $\simeq \langle -x_1, -y_1, x_1y_1\rangle$, o que implica que $\langle -d\rangle q \simeq \langle -d\rangle q_1$. Multiplicando ambos os lados por $\langle -d\rangle$ temos que $q \simeq q_1$. □

Teorema 3.2.2 *Suponhamos que toda forma quadrática de dimensão 5 sobre* K *é isotrópica. Então dimensão, determinante e invariante de Hasse classificam formas quadráticas sobre* K*, ou seja,* $q \simeq q_1$ *se, e somente se,* $dim(q) = dim(q_1)$, $d(q) = d(q_1)$ *e* $s(q) = s(q_1)$.

Demonstração: ($\Longrightarrow$) É óbvio.

($\Longleftarrow$) Se $dim(q) \leq 3$, temos o Teorema 3.2.1.

Assim, suponhamos $dim(q) = dim(q_1) \geq 4$, $d(q) = d(q_1)$ e $s(q) = s(q_1)$. Como q e q_1 são universais pelos Corolários 1.4.1 (ii) e 1.4.2, q e q_1 representam 1, e portanto $q \simeq \langle 1\rangle \perp q'$ e $q_1 \simeq \langle 1\rangle \perp q_1'$. Dessa forma, $d(q') = 1.d(q') = d(q) = d(q_1) = 1.d(q_1') = d(q_1')$ e $dim(q') = dim(q_1')$.

Sejam $q' \simeq \langle a_1, \ldots, a_n\rangle$ e $q_1' \simeq \langle b_1, \ldots, b_n\rangle$. Então, $s(q') = \prod_{i<j}[a_i, a_j]$ e $s(q_1') = \prod_{i<j}[b_i, b_j]$.

Como $s(q) = s(q_1)$, tem-se que $[1, a_1.\ldots.a_n]s(q') = [1, b_1.\ldots.b_n]s(q_1')$, mas $[1, x] = 1$ em $Br(\mathrm{K})$, para todo $x \in \dot{\mathrm{K}}$. Assim, $s(q') = s(q_1')$.

Provemos por indução que se $dim(q) = dim(q_1)$, $d(q) = d(q_1)$ e $s(q) = s(q_1)$ então $q \simeq q_1$.

Suponhamos válido para formas quadráticas com dimensão até n e provemos que vale para formas quadráticas de dimensão $n+1$.

Pela hipótese de indução, $q' \simeq q'_1$, e portanto $q \simeq \langle 1 \rangle \perp q' \simeq \langle 1 \rangle \perp q'_1 \simeq q_1$. Logo $q \simeq q_1$.

□

Capítulo 4

Corpos Locais

Definição 4.0.2 *Dados um corpo* K *e uma aplicação* $v : \mathrm{K} \longrightarrow \mathbb{Z}$*, dizemos que* v *é uma valorização não arquimediana de* K *se:*

(i) $v(x.y) = v(x) + v(y)$*;*

(ii) $v(x+y) \geq min\{v(x), v(y)\}$*, para todos* $x, y \in \dot{\mathrm{K}}$*, com* $y \neq -x$*.*

Desde que os grupos aditivos $\mathbb{Z}$ e $m\mathbb{Z}$, $m \neq 0$ são isomorfos podemos assumir sem perda de generalidade, que v é sobrejetora. Estendemos a adição de $\mathbb{Z}$ para $\mathbb{Z} \cup \{\infty\}$ por $a + \infty = \infty + a = \infty = \infty + \infty$, para todo $a \in \mathbb{Z}$ e definimos $v(0) = \infty$ e $\infty > a$, para todo $a \in \mathbb{Z}$.

O conjunto $\mathrm{A}_v = \{x \in \mathrm{K} \mid v(x) \geq 0\}$ é um subanel de K, dito *anel de valorização* de K. A_v tem um único ideal maximal $\mathcal{P} = \{x \in \mathrm{K} \mid v(x) \geq 1\}$, que é um ideal principal gerado por qualquer elemento π tal que $v(\pi) = 1$. Os geradores de $\mathcal{P}$ são determinados a menos de unidades do anel A_v e são ditos *uniformizadores* de A_v, ou de K.

De fato: • A_v é um anel, pois:

(a) $v(1) = v((-1)(-1)) = v(-1) + v(-1)$ e $v(1) = v(1.1) = v(1) + v(1)$. Logo $2v(-1) = 2v(1)$, ou $v(1) = v(-1)$. De $v(1) = 2v(1)$, segue que $v(1) = 0 = v(-1)$. Assim, $1 \in \mathrm{A}_v$. Logo $\mathrm{A}_v \neq \emptyset$.

(b) Sejam $x, y \in \mathrm{A}_v$. Como $v(1) = v(-1)$, temos que $v(-y) = v(-1) + v(y) = v(y)$. Então $v(x-y) \geq min\{v(x), v(-y)\} = min\{v(x), v(y)\} \geq 0$. Portanto $x - y \in \mathrm{A}_v$.

(c) De $v(xy) = v(x) + v(y) \geq 0$, para todos $x, y \in \mathrm{A}_v$, segue que $xy \in \mathrm{A}_v$.

Logo A_v é fechado para subtração e multiplicação. Como A_v está contido em K, A_v é

um domínio.

• $\mathcal{P}$ é um ideal maximal de A_v.

(a) $\mathcal{P} \neq \emptyset$, pois $0 \in \mathcal{P}$, desde que $v(0) = \infty \geq 1$.

(b) Sejam $x, y \in \mathcal{P}$, como $v(x) = v(-x)$ temos, $v(x-y) \geq min\{v(x), v(-y)\} = min\{v(x), v(y)\} \geq 1$. Portanto, $x - y \in \mathcal{P}$.

(c) Se $x \in \mathrm{A}_v$ e $y \in \mathcal{P}$ então $v(x.y) = v(x) + v(y) \geq 1$. Logo, $xy \in \mathcal{P}$. Portanto $\mathcal{P}$ é um ideal de A_v.

(d) O *grupo das unidades* de A_v é dado por $\mathcal{U}(\mathrm{A}_v) = \{x \in \mathrm{A}_v \mid x \notin \mathcal{P}\} = \{x \in \dot{\mathrm{K}} \mid v(x) = 0\}$ (também representamos $\mathcal{U}(\mathrm{A}_v)$ por $\mathcal{U}$).

De fato, isto segue da igualdade $\mathcal{P} = \mathrm{A}_v - \mathcal{U}(\mathrm{A}_v)$ e para verificar esta igualdade, basta demonstrarmos que $\mathcal{U}(\mathrm{A}_v) = \{x \in \dot{\mathrm{K}} \mid v(x) = 0\}$. Seja $x \in \dot{\mathrm{K}}$ tal que $v(x) = 0$. De $1 = xx^{-1}$ em K, segue que $0 = v(x) + v(x^{-1})$. Logo $v(x^{-1}) = 0$ e então $x^{-1} \in \mathrm{A}_v$. Assim $x \in \mathcal{U}(\mathrm{A}_v)$. Se $x \in \mathcal{U}(\mathrm{A}_v)$ então existe $x^{-1} \in \mathrm{A}_v$ tal que $1 = xx^{-1}$. Como $v(x) = 0$ temos que $0 = v(1) = v(x) + v(x^{-1}) = v(x^{-1})$.

(e) $\mathcal{P}$ é o único ideal maximal de A_v, e é principal.

(i)Seja J um ideal de A_v tal que $\mathcal{P} \subsetneq \mathrm{J} \subset \mathrm{A}_v$, então por (d) $\mathrm{J} \cap \mathcal{U}(\mathrm{A}_v) \neq \emptyset$. Portanto $\mathrm{J} = \mathrm{A}_v$ e $\mathcal{P}$ é maximal.

(ii) $\mathcal{P}$ é único.

Suponhamos I um ideal maximal de A_v, então I não contém unidades, ou seja, $\mathrm{I} \cap \mathcal{U}(\mathrm{A}_v) = \emptyset$. Logo $\mathrm{I} \subseteq \mathcal{P} \subsetneq \mathrm{A}_v$. Como I é maximal, $\mathrm{I} = \mathcal{P}$.

(iii) $\mathcal{P}$ é principal.

Como v é sobrejetora, existe $\pi \in \mathrm{A}_v$ tal que $v(\pi) = 1$. Portanto, para todo $x \in \mathcal{P}, v(x) = \alpha = v(\pi^\alpha)$. Logo $v(x\pi^{-\alpha}) = 0$ e portanto $x\pi^{-\alpha} = u \in \mathcal{U}(\mathrm{A}_v)$, assim $x = u\pi^\alpha$. Logo x pertence ao ideal principal $\pi\mathrm{A}_v$.

Além disso, como qualquer gerador de $\mathcal{P}$ tem valorização 1, eles diferem por uma unidade.

Nota 4.0.1 (1) *Notemos que todo $y \in \dot{\mathrm{K}}$ pode ser escrito (unicamente) na forma $y = u\pi^{v(y)}$, onde $u \in \mathcal{U}$. Basta ver que se $y \in \dot{\mathrm{K}}$, existe $r \in \mathbb{Z}$ tal que $v(y) = r$ então $v(y) = v(\pi^r)$. Isto implica que $v(y\pi^{-r}) = 0$ e então $y\pi^{-r} = u \in \mathcal{U}(\mathrm{A}_v)$. Assim $y = u\pi^r = u\pi^{v(y)}$.*

(2) *Para todo* $x \in \dot{\mathrm{K}}$*, tem-se que* $x \in \mathrm{A}_v$ *ou* $x^{-1} \in \mathrm{A}_v$*. Consequentemente* $\mathrm{K} = Cfr(\mathrm{A}_v)$ *(onde* $Cfr(\mathrm{A}_v)$ *é o corpo de frações de* A_v *).*

De fato, de (1) temos que para todo $x \in \dot{\mathrm{K}}$, $x = u\pi^m$ com $m \in \mathbb{Z}$ e $u \in \mathcal{U}(\mathrm{A}_v)$. Se $m > 0$ então $x \in \mathrm{A}_v$. Se $m < 0$ então $x^{-1} = u^{-1}\pi^{-m} \in \mathrm{A}_v$ (pois $u^{-1} \in \mathcal{U}(\mathrm{A}_v)$ e $-m > 0$).

Temos uma sequência de ideais encaixados:

$$\mathrm{A}_v \supset \mathcal{P} \supset \mathcal{P}^2 \supset \cdots \supset \{0\}, \text{ com} \cap \mathcal{P}^i = \{0\}.$$

O corpo $\overline{\mathrm{K}} = \dfrac{\mathrm{A}_v}{\mathcal{P}}$ é dito o *corpo de resíduos* de K (relativo à valorização v), e a projeção de A_v em $\overline{\mathrm{K}}$ é expressado por $a \longrightarrow \overline{a} = a + \mathcal{P}$.

Definição 4.0.3 *Um corpo local é um par* (K, v) *como acima, onde* K *é completo relativamente à valorização.*

Temos que toda valorização induz numa métrica , e dizer que K é completo significa que na métrica $d(x, y) = e^{-v(x-y)}$, toda sequência de Cauchy converge em K. Observe que nesta métrica, dois elementos x, y estão próximos se, e somente se, $x - y$ pertence a uma potência $\mathcal{P}^n$, para $n \in \mathbb{N}$, suficientemente grande.

Suponha $x_1, \ldots, x_n$ uma sequência em A_v tal que $x_{i+1} \equiv x_i (mod \mathcal{P}^i)$, para todo i. Então A_v contém um elemento $x (= limx_i)$ tal que $x \equiv x_i (mod \mathcal{P}^i)$, para todo i. Esta propriedade caracteriza o completamento.

Exemplos de corpos locais são os corpos de séries de potências formais $\mathrm{K} = \mathrm{F}(t)$, sobre um corpo F. Os elementos de K são da forma $g = \sum_{i=m}^{\infty} a_i t^i = t^m(a_m + a_{m+1}t + \cdots)$, com $a_i \in \mathrm{F}$ e $m \in \mathbb{Z}$.

Definição 4.0.4 *O corpo local* (K, v) *é dito* $\mathcal{P}$*-ádico se* $\overline{\mathrm{K}}$ *é um corpo finito.*

Definição 4.0.5 *Um corpo* $\mathcal{P}$*-ádico* (K, v) *é dito diádico se* $2 \in \mathcal{P}$*. Em outras palavras,* (K, v) *é diádico se, e somente se,* $v(2) \geq 1$ *e isto ocorre quando* $car(\overline{\mathrm{K}}) = 2$*. Caso contrário, ou seja se* $2 \notin \mathcal{P}$*,* (K, v) *é dito não diádico.*

Os completamentos p-ádicos do corpo $\mathbb{Q}$, denotado por $\mathbb{Q}_p$ é outro exemplo. Temos que $(\mathbb{Q}_p, v_p)$ são corpos p-ádicos para cada primo p em $\mathbb{Z}$ tal que seus elementos se escrevem como acima, trocando t por p e $0 \leq a_i < p$, com $a_i \in \mathbb{Z}$. Também como exemplo, tomemos F um corpo global, isto é, uma extensão finita de $\mathbb{Q}$ (dita um corpo de números) , ou de $\mathbb{K}_q(t)$ (dita um corpo de funções de uma variável sobre $\mathbb{K}_q$). O completamento de F por uma valorização não arquimediana é um corpo local que tem um corpo de resíduos finito.

Lema 4.0.1 *Sejam* (K, v) *um corpo local com* $car(\overline{\mathrm{K}}) \neq 2$ *e* $u \in \mathcal{U}$. *Temos que* u *é um quadrado em* K *(ou em* $\mathcal{U}$*) se, e somente se,* $\overline{u}$ *é um quadrado em* $\overline{\mathrm{K}}$.

Demonstração: ($\Longrightarrow$) Se $u = \alpha^2, \alpha \in \mathrm{K}$, então $\overline{u} = \overline{\alpha}^2 \in \overline{\mathrm{K}}^2$.

($\Longleftarrow$) Seja $\overline{u} = \overline{b}^2, \quad \overline{b} \in \overline{\mathrm{K}}$.

Precisamos construir uma sequência (b_i) em $\mathcal{U}$ tal que $b_i^2 \equiv u(mod\mathcal{P}^i)$ e $b_{i+1} \equiv b_i(mod\mathcal{P}^i)$, para todo i. Se tivermos tal sequência, ela é de Cauchy pois $b_{i+1} - b_i \in \mathcal{P}^i$. Logo (b_i^2) é de Cauchy e fazendo $b = \lim_{i \longrightarrow \infty} b_i$, tem-se que $b^2 - u = \lim_{i \longrightarrow \infty} b_i^2 - u = \lim_{i \longrightarrow \infty} (b_i^2 - u) = 0$. Assim, $b^2 = u$ e $u \in \mathrm{K}^2$, pois K é completo.

Temos que b_1 existe, pois $\overline{u} = \overline{b}^2 \in \overline{\mathrm{K}}^2 = \dfrac{\mathrm{A}_v^2}{\mathcal{P}^2}$. Como $u \in \mathcal{U}$, também $b_1 = b \in \mathcal{U}$. Assim, $b_1^2 \equiv u(mod\mathcal{P})$.

Suponhamos que existam $b_i \in \mathcal{U}, \quad i \geq 1$, tais que $b_i^2 \equiv u(mod\mathcal{P}^i)$ e $b_i \equiv b_{i-1}(mod\mathcal{P}^{i-1})$. Precisamos encontrar $b_{i+1} \in \mathcal{U}$ tal que $b_{i+1}^2 \equiv u(mod\mathcal{P}^{i+1})$ e $b_{i+1} \equiv b_i(mod\mathcal{P}^i)$, isto é, $b_{i+1} = b_i + z\pi^i$, para algum $z \in \mathrm{A}_v$.

Seja $b_{i+1} = b_i + \alpha\pi^i$, com $\alpha \in \mathrm{A}_v$. Então, $b_{i+1} \equiv b_i(mod\mathcal{P}^i)$, para todo $\alpha \in \mathrm{A}_v$.

Como $b_i^2 - u = \beta\pi^i, \quad \beta \in \mathrm{A}_v$, temos que $b_{i+1}^2 - u = (b_i + \alpha\pi^i)^2 - u = (b_i^2 - u) + 2\alpha b_i\pi^i + \alpha^2\pi^{2i} \equiv \pi^i(\beta + 2\alpha b_i)(mod\mathcal{P}^{i+1})$. Como $2b_i \in \mathcal{U}$ (pois $car(\overline{\mathrm{K}}) \neq 2$) e $u \in \mathcal{U}$, basta encontrar $\alpha \in \mathrm{A}_v$ tal que $\beta + 2\alpha b_i = \pi$. Fazendo $\alpha = (\pi - \beta)(2b_i)^{-1} \in \mathrm{A}_v$, concluimos que $b_{i+1} \in \mathcal{U}$ e $b_{i+1} \equiv b_i(mod\mathcal{P}^i)$. □

Teorema 4.0.3 *(Levantamento de raízes)*
Sejam (K, v) *um corpo local com* $car(\overline{\mathrm{K}}) \neq 2$ *e* $f(x) = ax^2 + bx + c \in \mathrm{K}[x]$. *Se existe uma raiz* $\overline{u}$ *de* $\overline{f}(x) = \overline{a}x^2 + \overline{b}x + \overline{c}$ *em* $\overline{\mathrm{K}}$, *então existe uma raiz* u *de* $f(x)$ *em* K.

Demonstração: Fazendo a mudança de variável x para $y - \dfrac{b}{2a}$ em $f(x)$, obtemos $g(y) =$

$ay^2 - \dfrac{b^2-4ac}{4a}$. Temos que x_0 é raiz de f se, e somente se, $y_0 = x_0 + \dfrac{b}{2a}$ é raiz de g. Porém, y_0 é raiz de $g(y)$ se, e somente se, $h(y) = \dfrac{1}{a}g(y)$ tem raiz y_0. Dessa forma, o cálculo de raízes de um polinômio de grau dois se reduz ao cálculo de quadrados. Assim basta verificarmos que se $\overline{h}(x) = x^2 + \overline{d} \in \overline{\mathrm{K}}[x]$ tem uma raiz $\overline{u} \in \overline{\mathrm{K}}$, então $h(x) = x^2 + d$ tem uma raiz u em K, e isto segue do Lema 4.0.1. □

Corolário 4.0.1 *Seja* (K, v) *um corpo local com* $car(\overline{\mathrm{K}}) \neq 2$. *Um elemento* $u\pi^m \in \dot{\mathrm{K}}$, *com* $u \in \mathcal{U}$ *e* $m \in \mathbb{Z}$, *é um quadrado em* K *se, e somente se,* m *é par e* $\overline{u} \in \dot{\overline{\mathrm{K}}}^2$. *Em particular, se* $\overline{u} = 1$ *então* $u \in \mathcal{U}^2$.

Com isto, podemos construir uma sequência exata. Definimos um homomorfismo i de $\dfrac{\dot{\overline{\mathrm{K}}}}{\dot{\overline{\mathrm{K}}}^2}$ em $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$ por $i(\overline{u}\dot{\overline{\mathrm{K}}}^2) = u\dot{\mathrm{K}}^2$, onde $u \in \mathcal{U}$ é um levantamento de $\overline{u}$. Este homomorfismo está bem definido pois se w é outro levantamento de $\overline{u}$, então $\overline{uw^{-1}} = \overline{1}$, isto é, $\overline{uw^{-1}} \in \dot{\overline{\mathrm{K}}}^2$. Logo $uw^{-1} \in \dot{\mathrm{K}}^2$ (pelo Corolário 4.0.1). Assim, $u\dot{\mathrm{K}}^2 = w\dot{\mathrm{K}}^2$, ou seja, $i(\overline{u}\dot{\overline{\mathrm{K}}}^2) = i(\overline{w}\dot{\overline{\mathrm{K}}}^2)$.

Corolário 4.0.2 *Seja* (K, v) *um corpo local com* $car(\overline{\mathrm{K}}) \neq 2$. *Então a sequência*

$$1 \longrightarrow \frac{\dot{\overline{\mathrm{K}}}}{\dot{\overline{\mathrm{K}}}^2} \xrightarrow{\ i\ } \frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} \xrightarrow{\ \overline{v}\ } \frac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow 0, \textit{ é exata e se fatora.}$$

Demonstração: Temos que i é injetora pois se $i(\overline{u}\dot{\overline{\mathrm{K}}}^2) = 1\dot{\mathrm{K}}^2$, então $u\dot{\mathrm{K}}^2 = \dot{\mathrm{K}}^2$. Logo $u \in \dot{\mathrm{K}}^2$. Pelo Corolário 4.0.1 $\overline{u} \in \dot{\overline{\mathrm{K}}}^2$ e assim $\overline{u}\dot{\overline{\mathrm{K}}}^2 = \overline{1}\dot{\overline{\mathrm{K}}}^2$. A função $\overline{v} : \dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} \longrightarrow \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ tal que $\overline{v}(x\dot{\mathrm{K}}^2) = v(x) + 2\mathbb{Z}$ está bem definida pois se $x\dot{\mathrm{K}}^2 = y\dot{\mathrm{K}}^2$, então $xy^{-1} \in \dot{\mathrm{K}}^2$. Logo $v(xy^{-1}) \in 2\mathbb{Z}$. Daí, $v(x) - v(y) \in 2\mathbb{Z}$, equivalentemente $v(x) + 2\mathbb{Z} = v(y) + 2\mathbb{Z}$. Assim $\overline{v}(x\dot{\mathrm{K}}^2) = \overline{v}(y\dot{\mathrm{K}}^2)$.

Também $\overline{v}$ é claramente sobrejetora e $(\overline{v} \circ i)(\overline{u}\dot{\overline{\mathrm{K}}}^2) = \overline{v}(u\dot{\mathrm{K}}^2) = v(u) + 2\mathbb{Z} = 2\mathbb{Z} = \overline{0}$. Logo, $Im(i) \subset Ker(\overline{v})$.

Se $x\dot{\mathrm{K}}^2 \in Ker(\overline{v})$, então $\overline{v}(x\dot{\mathrm{K}}^2) = v(x) + 2\mathbb{Z} = \overline{0}$, ou seja, $v(x) \in 2\mathbb{Z}$. Logo existe $y \in \dot{\mathrm{K}}$ tal que $v(x) = v(y^2)$ o que implica que $\dfrac{x}{y^2} = u \in \mathcal{U}$. Assim $x = uy^2$, o que resulta que $x\dot{\mathrm{K}}^2 = u\dot{\mathrm{K}}^2 = i(\overline{u}\dot{\overline{\mathrm{K}}}^2)$. Portanto $Ker(\overline{v}) \subset Im(i)$.

Para a fatoração, definimos $\varphi : \dfrac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow \dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$ por $\varphi(1) = \pi\dot{\mathrm{K}}^2$ e $\varphi(0) = \dot{\mathrm{K}}^2$. Então $(\overline{v} \circ \varphi) = id_{\frac{\mathbb{Z}}{2\mathbb{Z}}}$. Uma das equivalências da fatoração é

$$\frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} \overset{\theta}{\approx} \frac{\dot{\overline{\mathrm{K}}}}{\dot{\overline{\mathrm{K}}}^2} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$$

com $\theta(u\pi^\alpha) = \left(\overline{u}\dot{\overline{\mathrm{K}}}^2, \overline{\alpha}\right)$. □

Nota 4.0.2 *A Nota 4.0.1(2), garante que para todo $x \in \dot{\mathrm{K}}$, $x \in \mathrm{A}_v$ ou $x^{-1} \in \mathrm{A}_v$. Como $x\dot{\mathrm{K}}^2 = x^{-1}\dot{\mathrm{K}}^2$, trocando x por x^{-1} se necessário (veja Lema 1.2.4 (ii)), podemos tomar qualquer diagonalização $\langle a_1, \ldots, a_n\rangle$ de uma forma quadrática com $a_i \in \dot{\mathrm{A}}_v$. Além disso pelo Corolário 4.0.1, $a_i = u$ ou $a_i = u\pi$, com $u \in \mathcal{U}(\mathrm{A}_v)$.*

Proposição 4.0.2 *Seja (K, v) um corpo local, com $car(\overline{\mathrm{K}}) \neq 2$.*

(i) *Se $q = \langle u_1, \ldots, u_r\rangle$, onde $u_i \in \mathcal{U}$, então q é anisotrópica sobre K se, e somente se, $\overline{q} = \langle \overline{u}_1, \ldots, \overline{u}_r\rangle$ é anisotrópica sobre $\overline{\mathrm{K}}$;*

(ii) *Suponhamos $q = q_1 \perp \langle\pi\rangle q_2$, onde $q_1 = \langle u_1, \ldots, u_r\rangle$, $q_2 = \langle u_{r+1}, \ldots, u_n\rangle$ $(u_i \in \mathcal{U})$. Então q é anisotrópica sobre K se, e somente se, $\overline{q}_1$ e $\overline{q}_2$ são anisotrópicas sobre $\overline{\mathrm{K}}$.*

Demonstração: **(i)** $(\Longrightarrow)$ Suponhamos $\overline{q}$ isotrópica, logo existe $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_r) \in \overline{\mathrm{K}}$, não nulo tal que $\overline{q}(\overline{x}) = 0$, ou seja, $\displaystyle\sum_{i=1}^{r} \overline{u}_i\overline{x}_i^2 = 0$. Supondo $\overline{x}_1 \neq 0$, temos que $\overline{x}_1$ é raiz da equação $\overline{u}_1 t^2 + \overline{b} = 0$, onde $b = u_2x_2^2 + \cdots + u_rx_r^2$. Pelo Teorema 4.0.3, segue que x_1 é raiz de $u_1t^2 + b = 0$, ou seja, $q(x_1) = 0$, com $x_1 \neq 0$. Logo q é isotrópica, contradizendo a hipótese. Portanto $\overline{q}$ é anisotrópica.

$(\Longleftarrow)$ Suponhamos q isotrópica e $x = (x_1, \ldots, x_r) \neq 0$ tal que $q(x) = 0$. Logo $\displaystyle\sum_{i=1}^{r} u_ix_i^2 = 0$. Como $x_i = v_i\pi^{\alpha_i}$, com $\alpha_i \in \mathbb{Z}$ e v_i : unidade, se tivermos $\alpha_i > 0$, consideraremos o mínimo dos $\alpha_i's$. Consideremos que α_1 seja o mínimo (reordenando se necessário). Daí, $\pi^{2\alpha_1}(u_1v_1^2 + u_2v_2^2\pi^{2(\alpha_2-\alpha_1)} + \cdots + u_rv_r^2\pi^{2(\alpha_r-\alpha_1)}) = 0$. Logo, fazendo $\beta_i = \alpha_i - \alpha_1$, temos $u_1v_1^2 + u_2v_2^2\pi^{2\beta_2} + \cdots + u_rv_r^2\pi^{2\beta_r} = 0$ e $\overline{x} = (\overline{v}_1, \overline{v_2\pi^{\beta_2}}, \ldots, \overline{v_r\pi^{\beta_r}}) \neq 0$. Dessa forma, se $q(x) = 0$ com $x \neq 0$, então $\overline{q}(\overline{x}) = 0$ com $\overline{x} \neq 0$. Portanto $\overline{q}$ é isotrópica, o que é um absurdo.

(ii) ($\Longrightarrow$) Se q é anisotrópica, então q_1 e q_2 também são anisotrópicas. Assim, $\overline{q}_1$ e $\overline{q}_2$ são anisotrópicas sobre $\overline{\mathrm{K}}$ (por (i)).

($\Longleftarrow$) Suponhamos $q = q_1 \perp \langle\pi\rangle q_2$ isotrópica, assim $q \supseteq \mathbb{H} = \langle 1, -1\rangle$. Dessa forma, q_1 é isotrópica ou q_2 é isotrópica, pois caso contrário $\mathbb{H}$ seria isométrico a $\langle u, \pi v\rangle$, com u, v unidades, o que é um absurdo pois $det(\mathbb{H}) = -1$. Logo pelo item (i), $\overline{q}_1$ ou $\overline{q}_2$ é isotrópica, absurdo pela hipótese. Portanto q é anisotrópica. □

Corolário 4.0.3 *Seja* (K, v) *um corpo local, com* $car(\overline{\mathrm{K}}) \neq 2$.

(i) *Se toda forma quadrática de dimensão* $n+1$ *sobre* $\overline{\mathrm{K}}$ *é isotrópica, então toda forma quadrática de dimensão* $2n+1$ *sobre* K *é isotrópica;*

(ii) *Se* $\overline{\mathrm{K}}$ *tem uma forma quadrática anisotrópica de dimensão* n*, então* K *tem uma forma quadrática anisotrópica de dimensão* $2n$*.*

Demonstração: Consequência da proposição anterior. □

Teorema 4.0.4 *Sejam* (K, v) *um corpo* $\mathcal{P}$*-ádico, não diádico e* $u \in \mathcal{U}$ *tal que* $\overline{u} \notin \dot{\overline{\mathrm{K}}}^2$*. Então:*

(i) $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$ *consiste de quatro conjuntos representados por* $1, u, \pi, u\pi$*;*

(ii) *Existe uma única forma quadrática anisotrópica de dimensão 4 sobre* K*, a menos de isometria, a forma* $q = \langle 1, -u, -\pi, u\pi\rangle = \langle 1, -u\rangle \otimes \langle 1, -\pi\rangle$*;*

(iii) *Existe uma única álgebra de quatérnios com divisão sobre* K*, a menos de isomorfismo, que é* $\left(\dfrac{u, \pi}{\mathrm{K}}\right)$.

Demonstração: **(i)** Como $|\dot{\overline{\mathrm{K}}}|$ é finito, temos que $\dfrac{\dot{\overline{\mathrm{K}}}}{\dot{\overline{\mathrm{K}}}^2} = \{\overline{1}, \overline{u}\}$, com $\overline{u} \notin \dot{\overline{\mathrm{K}}}^2$. Pelo Corolário 4.0.2 temos que $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} \approx \dfrac{\dot{\overline{\mathrm{K}}}}{\dot{\overline{\mathrm{K}}}^2} \oplus \dfrac{\mathbb{Z}}{2\mathbb{Z}}$. Pelo Corolário 4.0.1, segue o resultado.

(ii) Seja $q = \langle u_1, \ldots, u_r\rangle \perp \langle\pi\rangle\langle u_{r+1}, \ldots, u_4\rangle$ uma forma quadrática anisotrópica sobre K. Pela Proposição 4.0.2 (ii), temos que $\overline{q}_1 = \langle \overline{u}_1, \ldots, \overline{u}_r\rangle$ e $\overline{q}_2 = \langle \overline{u}_{r+1}, \ldots, \overline{u}_4\rangle$ são anisotrópicas sobre $\overline{\mathrm{K}}$. Logo pela Proposição 2.2.2 e pelo Corolário 1.4.2 $dim(\overline{q}_1) = dim(\overline{q}_2) = 2$. Pela Proposição 2.2.2, temos $\overline{q}_1 = \langle \overline{1}, \overline{-u}\rangle \simeq \langle \overline{-1}, \overline{u}\rangle = \overline{q}_2$. Portanto $q \simeq \langle 1, -u, -\pi, u\pi\rangle$.

(iii) Segue de (ii) e pelo fato que toda álgebra de quatérnios com divisão, está em correspondência 1 a 1 com sua forma norma (veja Proposição 2.1.3). □

Observação 4.0.2 *Temos que* $\langle 1, -u, -\pi, u\pi\rangle$ *é universal.*

De fato: Se existe $w \in \dot{\mathrm{K}}$ tal que $w \notin D(\langle 1, -u, -\pi, u\pi\rangle)$, então $\langle 1, -u, -\pi, u\pi\rangle \perp \langle -w\rangle$ é anisotrópica. Logo $\langle 1, -u, -\pi, -w\rangle$ e $\langle -u, -\pi, u\pi, -w\rangle$ são subformas anisotrópicas de $\langle 1, -u, -\pi, u\pi, -w\rangle$ e não são isométricas pois têm determinantes distintos (o que é um absurdo pelo item (ii) do Teorema 4.0.4).

Corolário 4.0.4 *Seja* K *um corpo* $\mathcal{P}$*-ádico, não diádico.*

(i) *Se* $q = \langle 1, -a, -b, ab\rangle$ *é uma forma quadrática sobre* K*, então* $s(q) = [a, b]$;

(ii) *Para quaisquer álgebras* $\mathrm{A}_1 = \left(\frac{a,b}{\mathrm{K}}\right)$, $\mathrm{A}_2 = \left(\frac{c,d}{\mathrm{K}}\right)$ *existem* $e, z, t \in \dot{\mathrm{K}}$ *tais que* $\mathrm{A}_1 \approx \left(\frac{e,z}{\mathrm{K}}\right)$, $\mathrm{A}_2 \approx \left(\frac{e,t}{\mathrm{K}}\right)$.

Demonstração: **(i)** Desde que $[1, x] = 1$, por linearidade temos que $s(q) = [-a, -b].[-a, ab].[-b, ab] = [-a, -ab^2].[-b, ab] = [-a, -a].[-b, a].[-b, b] = [-1, -a].[a, -a].[-b, b].[-b, a]$. Pelo Corolário 2.1.3 ficamos com $s(q) = [-1, -a].[-b, a] = [-1, -1].[-1, a].[-b, a] = [-1, -1].[b, a]$. Pelo Teorema 4.0.4(ii) a forma norma de $\left(\frac{-1,-1}{\mathrm{K}}\right)$, $4\langle 1\rangle$ é isotrópica. Do Teorema 2.1.1 segue que $s(q) = [b, a] = [a, b]$.

(ii) Se A_1 e A_2 são álgebras com divisão, pelo Teorema 4.0.4 elas são isomorfas. Consequentemente pela Proposição 2.1.3 $\langle 1, -a, -b, ab\rangle \simeq \langle 1, -c, -d, cd\rangle$. Logo $\langle -a, -b, ab\rangle \simeq \langle -c, -d, cd\rangle$. Daí $-a \in D(\langle -c, -d, cd\rangle)$ e pelo Critério da Representação existem $x, y \in \dot{\mathrm{K}}$ tais que $\langle -c, -d, cd\rangle \simeq \langle -a, x, y\rangle$. Calculando o determinante encontramos $1 = -axy$ o que implica que $y = -ax$. Daí $\langle -c, -d, cd\rangle \simeq \langle -a, x, -ax\rangle$. Isto implica que $-ax = y(-ax)^2$, e portanto $\langle 1, -c, -d, cd\rangle \simeq \langle 1, -a, x, -ax\rangle$. Segue que $\left(\frac{c,d}{\mathrm{K}}\right) \approx \left(\frac{a,-x}{\mathrm{K}}\right)$. Logo $e = a$.

Se A_1 (ou A_2) se fatora então $\langle 1, -a, -b, ab\rangle \simeq \langle 1, -1, 1, -1\rangle$. Logo $\langle -a, -b, ab\rangle \simeq \mathbb{H} \perp \langle -1\rangle$. Assim $\langle -a, -b, ab\rangle$ é universal e portanto representa $-c$. Repetindo o raciocínio anterior conclui-se que $\mathrm{A}_1 \approx \left(\frac{c,z}{\mathrm{K}}\right)$ e $\mathrm{A}_2 = \left(\frac{c,d}{\mathrm{K}}\right)$, ou seja $e = c$. □

Pelo Corolário anterior podemos concluir que $s(q)$ em $Br(\mathrm{K})$ é representado por uma

classe de álgebra de quatérnios $\left(\frac{a,b}{\mathrm{K}}\right)$. Como só existem duas álgebras de quatérnios sobre K, a menos de isomorfismo, uma se fatora e a outra é com divisão podemos redefinir o invariante de Hasse neste caso por

Definição 4.0.6 *Seja* K *um corpo $\mathcal{P}$-ádico (não diádico). Para cada forma quadrática $q = \langle a_1, a_2, \ldots, a_n\rangle$ definimos o invariante de Hasse de q dado por $s(q) = [a, b]$, por:*

$$s(q) = \begin{cases} 1, & se \left(\frac{a,b}{\mathrm{K}}\right) \ se \ fatora \\ -1, & se \left(\frac{a,b}{\mathrm{K}}\right) \ não \ se \ fatora. \end{cases}$$

Teorema 4.0.5 *Seja* (K, v) *um corpo $\mathcal{P}$-ádico, não diádico. Então toda forma quadrática de dimensão 5 sobre* K *é isotrópica.*

Demonstração: Considere $q \simeq \langle a, b, c, d, e\rangle$.

Se $\langle a, b, c, d\rangle$ é isotrópica, então q é isotrópica.

Se $q_1 = \langle a, b, c, d\rangle$ é anisotrópica, então $q_1 \simeq \langle 1, -u, -\pi, u\pi\rangle$ (pois esta é a única forma anisotrópica de dimensão 4 sobre um corpo local). Mas $\langle 1, -u, -\pi, u\pi\rangle$ é universal, logo $-e \in \mathrm{D}(q_1)$. Pelo Teorema da Representação, $q \simeq q_1 \perp \langle e\rangle$ é isotrópica. □

Corolário 4.0.5 *As formas quadráticas sobre um corpo $\mathcal{P}$-ádico* K *são classificadas por dimensão, determinante e invariante de Hasse.*

Demonstração: Segue do Teorema 3.2.2. □

4.1 Corpos p-Ádicos $\mathbb{Q}_p$

Fixado um número primo $p \in \mathbb{Z}$ $p \neq 2$, todo número racional x não nulo se escreve de modo único na forma $x = p^m \frac{a}{b}$ com $m,\ a,\ b \in \mathbb{Z},\ b \neq 0$ e p não divide ab. A valorização p-ádica é definida sobre $\mathbb{Q}$ por $v_p(x) = m$ e $v_p(0) = \infty$. Denota-se por $\mathbb{Q}_p$ é o completamento p-ádico de $\mathbb{Q}$ segundo a valorização p-ádica de $\mathbb{Q}$. Assim

$$\mathbb{Q}_p = \left\{ p^m \left(\sum_{i=0}^{\infty} a_i p^i \right), \quad a_i \in \mathbb{Z}, \quad 0 \leq a_i < p \right\}.$$

O anel de valorização de v_p é:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\} = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \mathbb{Z}, \quad 0 \leq a_i < p \right\},$$

o grupo das unidades de $\mathbb{Q}_p$ é dado por

$$\mathcal{U}_p = \{x \in \mathbb{Q}_p \mid v_p(x) = 0\} = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \mathbb{Z}, \quad 0 \leq a_i < p, \quad a_0 \neq 0 \right\},$$

e o ideal maximal de $\mathbb{Z}_p$ é

$$\mathcal{P} = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 1\} = \left\{ p\left(\sum_{i=0}^{\infty} a_i p^i \right), \quad a_i \in \mathbb{Z}, \quad 0 \leq a_i < p \right\}.$$

Podemos escrever todo elemento não nulo x de $\mathbb{Q}_p$ de modo único na forma $x = up^m$, onde $m = v_p(x) \in \mathbb{Z}$ e u é uma unidade.

O par $(\mathbb{Q}_p, v_p)$ é um corpo local e é p-ádico, pois $\overline{\mathbb{Q}}_p = \dfrac{\mathbb{Z}_p}{\mathcal{P}} \approx \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ (corpo finito). De fato, basta considerarmos a aplicação $\varphi : \mathbb{Z}_p \longrightarrow \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ definida por $\varphi(x) = a_0 + p\mathbb{Z}$, que induz um isomorfismo $\overline{\mathbb{Q}}_p \approx \dfrac{\mathbb{Z}}{p\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$.

Observemos que no caso de $\mathbb{Q}_p$, teremos $\dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2} = \{1, u, p, up\}$, já que $v_p(p) = 1$ e π era tomado tal que $v(\pi) = 1$.

Consideremos $p \neq 2$ e assim $car(\overline{\mathbb{Q}}_p) \neq 2$. Logo os corpos $\mathbb{Q}_p$ satisfazem todos os resultados obtidos para corpos locais e corpos p-ádicos. Em particular $\mathrm{A} = \left(\dfrac{u, p}{\mathbb{Q}_p}\right)$ é a única álgebra de quatérnios com divisão sobre $\mathbb{Q}_p$ e $s(\langle 1, -u, -p, up\rangle) = -1_{Br}$.

Capítulo 5

Forma Traço Sobre Algumas Extensões Galoisianas de Corpos p-Ádicos

Este é o principal capítulo da dissertação. Nele vamos considerar extensões galoisianas F de $\mathbb{Q}_p$ ($p \neq 2$) de graus 2, 3 e 4 e vamos determinar, em cada caso, os invariantes da forma traço vistos anteriormente, a saber: a dimensão da forma quadrática, que é o grau $[\mathrm{F} : \mathbb{Q}_p]$; o determinante da forma quadrática, que é exatamente o discriminante da extensão F sobre $\mathbb{Q}_p$; e o invariante de Hasse. Estes três invariantes caracterizam a forma quadrática traço $\mathrm{T} : \mathrm{F} \longrightarrow \mathbb{Q}_p$, $\mathrm{T}(x) = tr(x^2)$ ou sua forma bilinear associada $b_{\mathrm{T}} : \mathrm{F} \times \mathrm{F} \longrightarrow \mathbb{Q}_p$, $b_{\mathrm{T}}(x, y) = tr(xy)$, a menos de isometria. Especialmente para extensões de grau 4 o discriminante do corpo F é de grande ajuda e por isso vamos precisar de alguns resultados preparatórios.

Lema 5.0.1 *Seja* $\langle 1, a\rangle$ *uma forma quadrática sobre o corpo* K. *Então* $D(\langle 1, a\rangle)$ *é um subgrupo de* $\dot{\mathrm{K}}$ *ou de* $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$.

Demonstração: Seja $\mathrm{F} = \mathrm{K}(\sqrt{-a})$. Para $x = \alpha + \beta\sqrt{-a} \in \mathrm{F}$, a norma de x é definida por $N(x) = x\overline{x} = \alpha^2 + a\beta^2$. Assim temos que $D(\langle 1, a\rangle) = \{\alpha^2 + a\beta^2 \in \dot{\mathrm{K}},\ \alpha, \beta \in \mathrm{K}\} = \{N(x) \in \dot{\mathrm{K}},\ x \in \mathrm{F}\}$. Agora a demonstração deste Lema é análoga a demonstração da Proposição 2.1.2. □

Lema 5.0.2 *Se $\langle 1, a\rangle$ é anisotrópica sobre $\mathbb{Q}_p$, então $|D(\langle 1, a\rangle)| = 2$. Em particular, se a é uma unidade, então $D(\langle 1, a\rangle) = \{1, u\}$, onde $\dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2} = \{1, u, p, up\}$.*

Demonstração: Suponhamos $\dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2}$ representado por $\{1, u, p, up\}$ (veja Teorema 4.0.4(i)).

Se $a = p$, temos que $D(\langle 1, p\rangle) = \{s = x^2 + py^2 \in \dot{\mathbb{Q}}_p, \text{com } x, y \in \mathbb{Q}_p\}$. Se $x = 0$ então $s \equiv p(mod\ \dot{\mathbb{Q}}_p^2)$. Se $x \neq 0$, então $s = x^2\left(1 + p\,(y/x)^2\right)$. Como $1 + pz^2 \in \mathrm{A}_{v_p}$, segue que $\overline{1 + pz^2} = \overline{1} \in \overline{\dot{\mathbb{Q}}_p}^2$ e pelo Lema 4.0.1, temos que $1 + pz^2 \in \dot{\mathbb{Q}}_p^2$. Logo $s = 1$ em $\dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2}$. Portanto $D(\langle 1, p\rangle) = \{1, p\}$. Analogamente prova-se que $D(\langle 1, up\rangle) = \{1, up\}$, com $u \in \mathcal{U}$.

Agora suponhamos que $a = u$, com $u \in \mathcal{U}$. Como $\langle 1, u\rangle$ é anisotrópica, $u \neq -1$. Evidentemente $D(\langle 1, u\rangle) \supset \{1, u\}$. Suponhamos que $p \in D(\langle 1, u\rangle)$, então $p = x^2 + uy^2$ e assim $-uy^2 = x^2 - p1^2$. Como $y \neq 0$ (pois p não é um quadrado) obtemos $-u = (x/y)^2 - p\,(1/y)^2 \in D(\langle 1, -p\rangle) = \{1, -p\}$. Logo $u = -1$, absurdo. Analogamente se demonstra que $up \notin D(\langle 1, u\rangle)$. Assim $D(\langle 1, u\rangle) = \{1, u\}$. Finalmente suponhamos que $\dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2}$ é representado por $\{1, -1, p, -p\}$ e demonstremos que $D(\langle 1, 1\rangle) = \{1, -1\}$. Como $D(\langle 1, 1\rangle) \subseteq \mathcal{U}\dot{\mathbb{Q}}_p^2$ resta demonstrar que $D(\langle 1, 1\rangle) \neq \dot{\mathbb{Q}}_p^2$. Façamos por absurdo. Se $x^2 + y^2 = z^2$, para todos $x, y \in \mathbb{Q}_p$, então por indução em $n = dim(n\langle 1\rangle)$ temos $D(n\langle 1\rangle) = \dot{\mathbb{Q}}_p^2$, para todo $n \geq 1$. Em particular, $D(5\langle 1\rangle) = \dot{\mathbb{Q}}_p^2$. Mas pelo Teorema 4.0.5 a forma quadrática $5\langle 1\rangle$ é isotrópica, logo universal pelo Corolário 1.25 (ii), absurdo. Portanto $D(\langle 1, 1\rangle) = \{1, -1\}\dot{\mathbb{Q}}_p^2$. □

Seja F uma extensão de K de grau n e seja $r : \mathrm{F} \longrightarrow \mathrm{K}$ um funcional linear não nulo (logo sobrejetor). Se (V, q) é um espaço quadrático sobre F definimos $r_*q : \mathrm{V} \longrightarrow \mathrm{K}$ por $(r_*q)(x) = r(q(x))$. Então r_*q é uma forma quadrática cuja bilinear associada é definida de $\mathrm{V} \times \mathrm{V}$ em K por $b_{r_*q}(x, y) = \dfrac{1}{2}\left[(r_*q)(x + y) - (r_*q)(x) - (r_*q)(y)\right] = \dfrac{1}{2}\left[r\left(q(x + y)\right) - r\left(q(x)\right) - r\left(q(y)\right)\right]$. Assim temos um novo espaço quadrático (V, r_*q) sobre K.

Podemos notar que $b_{r_*q} = r(b_q)$ e vamos denotar b_{r_*q} por r_*b_q.

Agora consideremos a forma quadrática $q = \langle c\rangle$, com $c \in \dot{\mathrm{F}}$. Como q tem dimensão 1, segue que o espaço vetorial $\mathrm{V} = \mathrm{F}.e_1$, onde $q(e_1) = c$. Temos que $r_*\langle c\rangle : \mathrm{F}.e_1 \longrightarrow \mathrm{K}$ é dada por $(r_*\langle c\rangle)(x) = r(cx^2)$ e a forma bilinear sobre F associada a forma quadrática $\langle c\rangle$ é $b_{\langle c\rangle}(x, y) = \dfrac{1}{2}(\langle c\rangle(x + y) - \langle c\rangle(x) - \langle c\rangle(y)) = cxy$.

Para $\mathrm{F} = \mathrm{K}(\sqrt{a})$, temos que $\{1, \sqrt{a}\}$ é base para o K-espaço vetorial F. Temos que $r_* b_q : \mathrm{V} \times \mathrm{V} \longrightarrow \mathrm{K}$ é dada por $(r_* b_q)(x, y) = r(b_q(x, y))$. Considerando o funcional linear definido por $r(1) = 0$ e $r(\sqrt{a}) = 1$ temos que $\mathrm{M}_{r_*\langle c\rangle} = \mathrm{M}_{r_* b_{\langle c\rangle}} = \begin{pmatrix} r(b_{\langle c\rangle}(1,1)) & r(b_{\langle c\rangle}(1,\sqrt{a})) \\ r(b_{\langle c\rangle}(\sqrt{a},1)) & r(b_{\langle c\rangle}(\sqrt{a},\sqrt{a})) \end{pmatrix}$ $= \begin{pmatrix} r(c) & r(c\sqrt{a}) \\ r(c\sqrt{a}) & r(ac) \end{pmatrix}$. Fazendo $c = \alpha + \beta\sqrt{a}$, com $\alpha, \beta \in \mathrm{K}$, temos $\mathrm{M}_{r_*\langle c\rangle} = \begin{pmatrix} \beta & \alpha \\ \alpha & \beta a \end{pmatrix}$, cujo determinante é $-\alpha^2 + a\beta^2 = -(\alpha^2 - a\beta^2) = -N(c)$. Seja $r_*\langle c\rangle \simeq \langle a_1, a_2\rangle$. Como o determinante é um invariante por isometria temos que $a_1 a_2 = -N(c)$, e então $a_1^2 a_2 = -N(c)a_1$. Logo $r_*\langle c\rangle \simeq \langle a_1, a_2\rangle \simeq \langle a_1, a_2 a_1^2\rangle \simeq \langle a_1, -N(c)a_1\rangle \simeq \langle a_1\rangle\langle 1, -N(c)\rangle$. Portanto, $r_*\langle c\rangle \simeq \langle a_1\rangle\langle 1, -N(c)\rangle$, com $a_1 \in D(r_*\langle c\rangle)$.

Teorema 5.0.1 *Seja* $\mathrm{F} = \mathrm{K}(\sqrt{a})$*, com* $a \notin \dot{\mathrm{K}}^2$*. Então a sequência*

$$\dot{\mathrm{K}}^2 \longrightarrow \left\{\dot{\mathrm{K}}^2, a\dot{\mathrm{K}}^2\right\} \longrightarrow \frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2} \xrightarrow{\bar{i}} \frac{\dot{\mathrm{F}}}{\dot{\mathrm{F}}^2} \xrightarrow{\overline{n}} \frac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$$

é exata, onde $\bar{i}$ *é induzida pela inclusão* $\mathrm{K} \hookrightarrow \mathrm{F}$ *e* $\overline{n}$ *é definida por* $\overline{n}(a\dot{\mathrm{F}}^2) = N(a)\dot{\mathrm{K}}^2$*, onde* N *é norma de* F *em* K*.*

Demonstração: (i) Verifiquemos a exatidão em $\dfrac{\dot{\mathrm{K}}}{\dot{\mathrm{K}}^2}$. Seja $\beta\dot{\mathrm{K}}^2$ um elemento de $Ker(\bar{i})$. Então $\beta\dot{\mathrm{F}}^2 = \dot{\mathrm{F}}^2$, ou seja, $\beta \in \dot{\mathrm{F}}^2$. Assim, $\beta = (x + y\sqrt{a})^2$, com $x, y \in \mathrm{K}$ e desenvolvendo o quadrado temos $\beta = x^2 + ay^2 + 2xy\sqrt{a}$. Desde que $\beta \in \mathrm{K}$, segue-se que $xy = 0$. Se $x = 0$, temos $\beta = ay^2 \in a\dot{\mathrm{K}}^2$ e se $y = 0$ temos $\beta = x^2 \in \dot{\mathrm{K}}^2$. Logo $Ker(\bar{i}) = \left\{\dot{\mathrm{K}}^2, a\dot{\mathrm{K}}^2\right\}$.

(ii) Verifiquemos a exatidão em $\dot{\mathrm{F}}/\dot{\mathrm{F}}^2$.

Temos que $\overline{n}(\bar{i}(\alpha\dot{\mathrm{K}}^2)) = \overline{n}(\alpha\dot{\mathrm{F}}^2) = N(\alpha)\dot{\mathrm{K}}^2 = \alpha^2\dot{\mathrm{K}}^2 = \dot{\mathrm{K}}^2$. Portanto $Im(\bar{i}) \subset Ker(\overline{n})$.

Seja $x\dot{\mathrm{F}}^2$ tal que $N(x)\dot{\mathrm{K}}^2 = \dot{\mathrm{K}}^2$, ou seja, $N(x) \in \dot{\mathrm{K}}^2$. Consideremos o funcional linear $r : \mathrm{F} \longrightarrow \mathrm{K}$ definido por $r(1) = 0$ e $r(\sqrt{a}) = 1$. Como vimos anteriormente $r_*\langle x\rangle \simeq \langle y\rangle\langle 1, -N(x)\rangle$, com $y \in \dot{\mathrm{K}}$. Como $N(x) \in \dot{\mathrm{K}}^2$, tem-se $r_*\langle x\rangle \simeq \mathbb{H}$. Seja $z \in \dot{\mathrm{F}}$ um vetor isotrópico para $r_*\langle x\rangle$. Então $(r_*\langle x\rangle)(z) = 0$, ou seja, $r(xz^2) = 0$. Fazendo $z = z_1 + z_2\sqrt{a}$ e $x = \alpha + \beta\sqrt{a}$, então $xz^2 = (\alpha + \beta\sqrt{a})(z_1^2 + az_2^2 + 2z_1z_2\sqrt{a})$. Como $r(xz^2) = 2\alpha z_1 z_2 + \beta(z_1^2 + az_2^2) = 0$, segue-se que $xz^2 = (\alpha(z_1^2 + az_2^2) + 2\beta a z_1 z_2) + (2\alpha z_1 z_2 + \beta(z_1^2 + az_2^2)\sqrt{a}) \in \dot{\mathrm{K}}$. Logo $x\dot{\mathrm{F}}^2 = xz^2\dot{\mathrm{F}}^2 = \bar{i}(xz^2\dot{\mathrm{K}}^2)$. Portanto $Ker(\overline{n}) \subset Im(\bar{i})$. □

Corolário 5.0.1 *Seja* $\mathrm{F} = \mathbb{Q}_p(\sqrt{a})$*, com* $a \in \dot{\mathbb{Q}}_p \smallsetminus \dot{\mathbb{Q}}_p^2$*. Então* $\left|\dot{\mathrm{F}}/\dot{\mathrm{F}}^2\right| = 4$.

Demonstração: Como a não é um quadrado em $\mathbb{Q}_p$ temos que a forma quadrática $\langle 1, -a\rangle$ é anisotrópica. Pelo Lema 5.0.2 temos que $|D(\langle 1, -a\rangle)| = 2$. Desde que $\dfrac{\dot{\mathrm{F}}/\dot{\mathrm{F}}^2}{Ker(\overline{n})} \approx Im(\overline{n})$, segue do Teorema 5.0.1 que $\left|\dfrac{\dot{\mathrm{F}}/\dot{\mathrm{F}}^2}{Im\ (\bar{i})}\right| = |D(\langle 1, -a\rangle)| = 2$. Logo $\dfrac{\left|\dot{\mathrm{F}}/\dot{\mathrm{F}}^2\right|}{2} = 2$ o que implica que $\left|\dot{\mathrm{F}}/\dot{\mathrm{F}}^2\right| = 4$. □

Definição 5.0.1 *Sejam* $\mathrm{F} = \mathbb{Q}_p(\theta)$ *uma extensão Galoisiana de grau* n *de* $\mathbb{Q}_p$ *e* $A = \{\alpha_1, \ldots, \alpha_n\}$ *uma* $\mathbb{Q}_p$*-base de* F. *O discriminante de* A *é definido como sendo*

$$\Delta[A] = \{det(\sigma_i(\alpha_j))\}^2,$$

onde σ_i *são* $\mathbb{Q}_p$*-automorfismos de* F.

Notação: $\Delta[A]$.

Se tomarmos outra $\mathbb{Q}_p$-base de F, $B = \{\beta_1, \ldots, \beta_n\}$, temos que o discriminante das bases A e B diferem apenas por um fator quadrático, ou seja, $\Delta[B] = \Delta[A].c^2,\ c \in \dot{\mathbb{Q}}_p$.

De fato: Para todo $\beta_k \in B$, $\beta_k = \sum_{j=1}^{n} a_{kj}\alpha_j$, com $a_{kj} \in \mathbb{Q}_p$. Assim, (a_{kj}) é a matriz de mudança da base A para a base B. Portanto, $\Delta[B] = \{det(\sigma_i(\beta_k))\}^2 = \left\{det\left(\sum_{j=1}^{n} a_{kj}\sigma_i(\alpha_j)\right)\right\}^2$ $= \{det[(a_{kj}).(\sigma_i(\alpha_j))]\}^2 = \{det(a_{kj})\}^2.\{det(\sigma_i(\alpha_j))\}^2 = \{det(a_{kj})\}^2.\Delta[A]$.

Considerando o discriminante de uma base A de um corpo F como elemento de $\dot{\mathbb{Q}}_p/\dot{\mathbb{Q}}_p^2$ temos que ele é um invariante (por mudança de base) do corpo F e será denotado por δF.

Proposição 5.0.1 *Seja* $A = \{\alpha_1, \ldots, \alpha_n\}$ *uma* $\mathbb{Q}_p$*-base de* $\mathrm{F} = \mathbb{Q}_p(\theta)$. *Então* $\delta\mathrm{F} = det(tr(\alpha_i\alpha_j))$, *onde* $tr(x) = \sum_{i=1}^{n} \sigma_i(x)$ *é o traço do elemento* $x \in \mathrm{F}$.

Demonstração: Denotemos a matriz $(\sigma_i(\alpha_j))$ por M. Então $\delta\mathrm{F} = \{det(\sigma_i(\alpha_j))\}^2 = det\mathrm{M}^t.det\mathrm{M} = det(\mathrm{M}^t\mathrm{M}) = det\{(\sigma_j(\alpha_i)).(\sigma_i(\alpha_j))\} = det\left(\sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j)\right) = det\left(\sum_{r=1}^{n} \sigma_r(\alpha_i\alpha_j)\right) = det(tr(\alpha_i\alpha_j))$. □

Teorema 5.0.2 *Sejam* $\mathrm{F} \supset \mathbb{Q}_p$ *uma extensão galoisiana de grau* $n = [\mathrm{F} : \mathbb{Q}_p] \leq 4$ *e* $\delta = \delta\mathrm{F}$. *Então:*

(i) *Se* $n = 2$ *ou* $n = 4$ *e* $Gal(\mathrm{F} : \mathbb{Q}_p)$ *é cíclico, então* $\delta \notin \dot{\mathbb{Q}}_p^2$ *e* $\mathbb{Q}_p(\sqrt{\delta})$ *é a única extensão de grau* 2 *de* $\mathbb{Q}_p$ *contida em F;*

(ii) *Se* $n = 3$, *ou* $n = 4$ *e* $Gal(\mathrm{F} : \mathbb{Q}_p)$ *é o grupo de Klein então* $\delta \in \dot{\mathbb{Q}}_p^2$.

Demonstração: Sejam $\mathrm{G} = Gal(\mathrm{F} : \mathbb{Q}_p) = \{\sigma_1, \ldots, \sigma_n\}$ e $\{e_1, \ldots, e_n\}$ uma base de F sobre $\mathbb{Q}_p$. Pela Proposição 5.0.1, $\delta = det(tr_{\mathrm{F}/\mathbb{Q}_p}(e_i e_j)) = \{det(\sigma_i(e_j))\}^2$. Assim, $\delta \in \mathbb{Q}_p \cap \dot{\mathrm{F}}^2$.

Pelo Teorema do Elemento Primitivo temos que $\mathrm{F} = \mathbb{Q}_p(\theta)$, com $\theta \in \mathrm{F} \setminus \mathbb{Q}_p$.

Se $n = 2$, então $\{1, \theta\}$ é uma base para F e como $\theta^2 \in \mathrm{F}$ existem $a_1,\ a_2 \in \mathbb{Q}_p$ tais que $\theta^2 = a_1\theta + a_2$. Logo θ é uma das raízes de $f(x) = x^2 - a_1 x - a_2 \in \mathbb{Q}_p[x]$, a saber: $\theta_i = \dfrac{a_1 \pm \sqrt{a_1^2 + 4a_2}}{2}$. Portanto $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(2\theta - a_1) = \mathbb{Q}_p(\sqrt{a_1^2 + 4a_2})$. Resta demonstrar que $\delta = a_1^2 + 4a_2$.

Por definição $\delta = \begin{vmatrix} 1 & \theta_1 \\ 1 & \theta_2 \end{vmatrix}^2 = (\theta_2 - \theta_1)^2$ e em F temos que $x^2 - a_1 x - a_2 = (x - \theta_1)(x - \theta_2) = x^2 - (\theta_1 + \theta_2)x + \theta_1\theta_2$. Logo $\theta_1 + \theta_2 = a_1$ e $\theta_1\theta_2 = -a_2$, o que implica que $a_1^2 + 4a_2 = (\theta_1 + \theta_2)^2 - 4\theta_1\theta_2 = (\theta_2 - \theta_1)^2$. Portanto $\mathrm{F} = \mathbb{Q}_p\left(\sqrt{\delta}\right)$ e então $\delta \notin \dot{\mathbb{Q}}_p^2$.

Se $n = 3$, pelo Teorema da multiplicidade dos graus de extensões temos que não existe extensão de grau 2 de $\mathbb{Q}_p$ contida em F. Assim para todo $\beta \in \mathrm{F}$ tal que $\beta^2 \in \mathbb{Q}_p$, segue que $\beta \in \mathbb{Q}_p$ e portanto $\beta^2 \in \dot{\mathbb{Q}}_p^2$. Mas como $\delta = \{det(\sigma_i(e_j))\}^2$ e $\delta \in \mathbb{Q}_p \cap \dot{\mathrm{F}}^2$, temos que $\delta \in \dot{\mathbb{Q}}_p^2$. Resta estudar os casos de $n = 4$.

Se $n = 4$, sejam $\mathrm{F} = \mathbb{Q}_p(\theta)$, $p(x) = Irr(\theta, \mathbb{Q}_p) \in \mathbb{Q}_p[x]$ de grau 4 e $\theta = \theta_1, \theta_2, \theta_3, \theta_4$ as raízes de $p(x)$. Temos dois casos a considerar:

(i) Para $\mathrm{G} = Gal(\mathrm{F} : \mathbb{Q}_p)$ cíclico, $\mathrm{G} = \langle\sigma\rangle = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4 = id\}$, onde $\sigma_i = \sigma^i$ e as raízes são ordenadas de forma que $\sigma(\theta_1) = \theta_2,\ \sigma^2(\theta_1) = \theta_3,\ \sigma^3(\theta_1) = \theta_4,\ \sigma^4(\theta_1) = \theta_1$. Considerando a base $\{1, \theta, \theta^2, \theta^3\}$ da extensão $\mathrm{F} \supseteq \mathbb{Q}_p$ temos:

$\delta = \delta\mathrm{F} = \{det(\sigma_i(\theta^j))\}^2$. Logo $\sqrt{\delta} = \begin{vmatrix} 1 & \theta_2 & \theta_2^2 & \theta_2^3 \\ 1 & \theta_3 & \theta_3^2 & \theta_3^3 \\ 1 & \theta_4 & \theta_4^2 & \theta_4^3 \\ 1 & \theta_1 & \theta_1^2 & \theta_1^3 \end{vmatrix} =$

$$\begin{vmatrix} 1 & \theta_2-\theta_1 & \theta_2(\theta_2-\theta_1) & \theta_2^2(\theta_2-\theta_1) \\ 1 & \theta_3-\theta_1 & \theta_3(\theta_3-\theta_1) & \theta_3^2(\theta_3-\theta_1) \\ 1 & \theta_4-\theta_1 & \theta_4(\theta_4-\theta_1) & \theta_4^2(\theta_4-\theta_1) \\ 1 & 0 & 0 & 0 \end{vmatrix} = \begin{vmatrix} \theta_2-\theta_1 & \theta_2(\theta_2-\theta_1) & \theta_2^2(\theta_2-\theta_1) \\ \theta_3-\theta_1 & \theta_3(\theta_3-\theta_1) & \theta_3^2(\theta_3-\theta_1) \\ \theta_4-\theta_1 & \theta_4(\theta_4-\theta_1) & \theta_4^2(\theta_4-\theta_1) \end{vmatrix} =$$

$$(\theta_2-\theta_1)(\theta_3-\theta_1)(\theta_4-\theta_1)\begin{vmatrix} 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \\ 1 & \theta_4 & \theta_4^2 \end{vmatrix} =$$

$$(\theta_2-\theta_1)(\theta_3-\theta_1)(\theta_4-\theta_1).\begin{vmatrix} 1 & \theta_2-\theta_4 & \theta_2(\theta_2-\theta_4) \\ 1 & \theta_3-\theta_4 & \theta_3(\theta_3-\theta_4) \\ 1 & 0 & 0 \end{vmatrix} =$$

$$= (\theta_2-\theta_1)(\theta_3-\theta_1)(\theta_4-\theta_1)(\theta_2-\theta_4)(\theta_3-\theta_4)(\theta_3-\theta_2) = \prod_{1\le i<j\le 4}(\theta_j-\theta_i).$$

Temos que $\sqrt{\delta} \in \mathbb{Q}_p$ se, e somente se, G fixa $\sqrt{\delta}$. Mas $\sigma(\sqrt{\delta}) = \sigma\left(\prod_{1\le i<j\le 4}(\theta_j-\theta_i)\right) = \prod_{1\le i<j\le 4}(\sigma(\theta_j)-\sigma(\theta_i)) = \prod_{1\le i<j\le 3}(\sigma(\theta_j)-\sigma(\theta_i))\,[(\sigma(\theta_4)-\sigma(\theta_1))(\sigma(\theta_4)-\sigma(\theta_2))(\sigma(\theta_4)-\sigma(\theta_3))]$
$= \prod_{1\le i<j\le 3}(\theta_{j+1}-\theta_{i+1})[(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_1-\theta_4)] = \prod_{2\le i<j\le 4}(\theta_j-\theta_i)[(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_1-\theta_4)] =$
$-\prod_{2\le i<j\le 4}(\theta_j-\theta_i)[(\theta_2-\theta_1)(\theta_3-\theta_1)(\theta_4-\theta_1)] = -\prod_{1\le i<j\le 4}(\theta_j-\theta_i) = -(det(\sigma_i(\theta^j)))$. Logo $\sqrt{\delta} \notin \mathbb{Q}_p$, o que implica que $\delta \notin \mathbb{Q}_p^2$ e $\mathbb{Q}_p(\sqrt{\delta})$ é uma extensão quadrática de $\mathbb{Q}_p$ contida em F. Para a unicidade note que toda extensão intermediária L de $\mathbb{Q}_p$ é galoisiana e o grupo de Galois da extensão $L_{|\mathbb{Q}_p}$ é do tipo G/N, onde N é subgrupo normal de G. Mas o único subgrupo normal de G com $|G/N| = 2$ é $N = \langle\sigma^2\rangle = \{id, \sigma^2\}$ e $L = \mathbb{Q}_p(\sqrt{\delta})$, pois $\sigma(\sqrt{\delta}) = -\sqrt{\delta}$ e disto segue que σ^2 fixa $\sqrt{\delta}$.

(ii) Se G é o grupo de Klein podemos supor, a menos de isomorfismo, que G está contido no grupo das permutações pares, ou seja: $G = \{id, (\theta_1\,\theta_2)(\theta_3\,\theta_4), (\theta_1\,\theta_3)(\theta_2\,\theta_4),\ (\theta_1\,\theta_4)(\theta_3\,\theta_2)\}$. Logo $\sigma(\sqrt{\delta}) = \sqrt{\delta}$, para todo $\sigma \in G$. Como a extensão é galoisiana, vem que $\sqrt{\delta} \in \mathbb{Q}_p$ e então $\delta \in \dot{\mathbb{Q}}_p^2$. □

Corolário 5.0.2 *Seja* F *uma extensão galoisiana cíclica de* $\mathbb{Q}_p$ *(*$p \neq 2$*), de grau* 4 *com discriminante* δ*. Então* δ *é uma soma de dois quadrados.*

Demonstração: Sejam $\mathrm{L} = \mathbb{Q}_p\left(\sqrt{\delta}\right)$, a única extensão quadrática de $\mathbb{Q}_p$ contida em F, e $\mathrm{F} = \mathbb{Q}_p\left(\sqrt{\alpha+\beta\sqrt{\delta}}\right)$. Denote por $\mathrm{G} = \langle\sigma\rangle$ o grupo de Galois de F sobre $\mathbb{Q}_p$, e $e = \sqrt{\alpha+\beta\sqrt{\delta}}$. Como L é o corpo fixo de $\{id, \sigma^2\}$ e $e^2 \in \mathrm{L}$ temos que $(\sigma^2(e))^2 = \sigma^2(e^2) = e^2$. Logo $\sigma^2(e) = \pm e$ e como $e \notin \mathrm{L}$ vem que $\sigma^2(e) = -e$. Desde que $\sigma_{|\mathrm{L}} \in Gal(\mathrm{L}, \mathbb{Q}_p)$ e $\sigma \neq id$ temos que $\sigma(\alpha+\beta\sqrt{\delta}) = \alpha - \beta\sqrt{\delta}$, ou, $\sigma(e^2) = \alpha - \beta\sqrt{\delta}$. Consequentemente, $\alpha^2 - \delta\beta^2 = e^2\sigma(e^2) = (e\sigma(e))^2 \in \mathbb{Q}_p \cap \mathrm{F}^2$. Então, $\mathbb{Q}_p(e\sigma(e))$ é uma extensão quadrática contida em F. Pelo Teorema 5.0.2(i), $\mathbb{Q}_p(e\sigma(e)) = \mathrm{L}$. Segue-se que $\alpha^2 - \delta\beta^2 = (e\sigma(e))^2 \in \mathbb{Q}_p \cap \mathrm{L}^2$. Pelo Teorema 5.0.1 vem que $\alpha^2 - \delta\beta^2 = x^2,\ x \in \mathbb{Q}_p,$ ou $\alpha^2 - \delta\beta^2 = \delta x^2,\ x \in \mathbb{Q}_p$. No primeiro caso $e\sigma(e) = \sqrt{\alpha^2 - \delta\beta^2} \in \mathbb{Q}_p$ e portanto $\sigma(e)\sigma^2(e) = \sigma(e\sigma(e)) = e\sigma(e)$. Logo $\sigma^2(e) = e$, o que contradiz o fato de que $\sigma^2(e) = -e$. Então $\alpha^2 - \delta\beta^2 = \delta x^2$.

Se $\alpha = 0$ então $-1 \equiv 1\left(mod\ \dot{\mathbb{Q}}_p^2\right)$. Daí, $\langle 1,1\rangle \simeq \mathbb{H}$ e $\delta \in D(\langle 1,1\rangle$.

Se $\alpha \neq 0$ então $1 = \delta\left(\frac{x}{\alpha}\right)^2 + \delta\left(\frac{\beta}{\alpha}\right)^2$. Multiplicando por δ, temos que $\delta = 1\left(\frac{\delta x}{\alpha}\right)^2 + 1\left(\frac{\delta\beta}{\alpha}\right)^2 \in D(\langle 1,1\rangle)$. □

Seja F uma extensão galoisiana de $\mathbb{Q}_p$ e $\sigma \in \mathrm{G} = Gal(\mathrm{F}, \mathbb{Q}_p)$. Para cada espaço bilinear (V, b) sobre F definimos um novo espaço bilinear $(\mathrm{V}^\sigma, b^\sigma)$, onde V^σ tem a mesma estrutura de espaço vetorial de V e a multiplicação por escalar é definida por $\alpha * x = \sigma(\alpha)x$. A forma bilinear $b^\sigma : \mathrm{V}^\sigma \times \mathrm{V}^\sigma \longrightarrow \mathrm{F}$ é definida por $b^\sigma(x,y) = \sigma^{-1}(b(x,y))$. De fato b^σ é uma forma bilinear pois, para todo $\alpha \in \mathrm{F}$ e $x,\ y,\ z \in \mathrm{V}$ temos que $b^\sigma(\alpha * x + y, z) = \sigma^{-1}(b(\sigma(\alpha)x + y, z)) = \sigma^{-1}(\sigma(\alpha)b(x,z) + b(y,z)) = \alpha\sigma^{-1}(b(x,z)) + \sigma^{-1}(b(y,z)) = \alpha b^\sigma(x,z) + b^\sigma(y,z)$. Fixada uma base de V podemos denotar $b(x,y)$ por $b(x,y) = \sum_{i,j=1}^{n} a_{ij}x_iy_j$. Daí

$$b^\sigma(x,y) = \sigma^{-1}(b(x,y)) = \sigma^{-1}\left(\sum_{i,j=1}^{n} a_{ij}x_iy_j\right) = \sum_{i,j=1}^{n} \sigma^{-1}(a_{ij})\sigma^{-1}(x_i)\sigma^{-1}(y_j).$$

Podemos definir também $q^\sigma : \mathrm{V}^\sigma \longrightarrow \mathrm{F}$, onde $q : \mathrm{V} \longrightarrow \mathrm{F}$ é uma forma quadrática. Um modo de fazer isto é considerar $b_q^\sigma : \mathrm{V}^\sigma \times \mathrm{V}^\sigma \longrightarrow \mathrm{F}$ como definido anteriormente e daí faça $q^\sigma(x) = b_q^\sigma(x,x)$.

Se $r : \mathrm{F} \longrightarrow \mathrm{K}$ é um funcional linear não nulo e q uma forma quadrática sobre F já temos definido $r_*q : \mathrm{V} \longrightarrow \mathrm{K}$. Quando $r = tr_{\mathrm{F|K}}$ (que não é o funcional nulo) denotaremos r_*q por $tr(q)$.

Notemos também que toda forma quadrática q (ou bilinear) sobre K pode ser vista como uma forma quadrática (bilinear) sobre F que denotaremos por q^{F}. De fato, dada $q : \mathrm{V} \longrightarrow \mathrm{K}$, defina $q^{\mathrm{F}} : \mathrm{F} \otimes_{\mathrm{K}} \mathrm{V} \longrightarrow \mathrm{F}$ por $q^{\mathrm{F}}(\alpha \otimes x) = \alpha^2 q(x)$. Assim, se na base $B = \{e_1, \ldots, e_n\}$ q tem matriz (α_{ij}), na base $B_1 = \{1 \otimes e_1, \ldots, 1 \otimes e_n\}$ q^{F} tem matriz (α_{ij}).

Proposição 5.0.2 *Se* (V, q) *é um espaço quadrático regular sobre* F*, então* (V, r_*q) *é um espaço quadrático regular sobre* K*.*

Demonstração: Suponhamos que (V, r_*q) não é um espaço quadrático regular. Então existe um vetor não nulo $x \in \mathrm{V}$, tal que $(r_*b_q)(x, y) = r(b_q(x, y)) = 0$, para todo $y \in \mathrm{V}$. Como (V, q) é regular, existe $y' \in \mathrm{V}$ tal que $b_q(x, y') \neq 0$. Para $\alpha \in \mathrm{F}$, temos $b_q\left(x, \dfrac{\alpha}{b_q(x,y')}y'\right) = \dfrac{\alpha}{b_q(x,y')}.b_q(x, y') = \alpha \in \mathrm{F}$. Aplicando o funcional r, temos $r(\alpha) = (r_*b_q)\left(x, \dfrac{\alpha}{b_q(x,y')}y'\right) = 0$, contradizendo o fato de $r : \mathrm{F} \to \mathrm{K}$ ser um funcional linear não nulo. □

Teorema 5.0.3 *Seja* $\mathrm{F} \supset \mathrm{K}$ *uma extensão galoisiana finita, com grupo de Galois* $\mathrm{G} = Gal(\mathrm{F} : \mathrm{K})$*. Então para toda forma quadrática* q *sobre* F*, existe uma isometria*

$$tr(q)^{\mathrm{F}} \simeq \perp_{\sigma \in \mathrm{G}} q^{\sigma}.$$

Demonstração: Seja (V, q) um espaço quadrático sobre F. Temos que a forma quadrática $\perp_{\sigma \in \mathrm{G}} q^{\sigma}$ está definida do espaço quadrático $\perp_{\sigma \in \mathrm{G}} \mathrm{V}^{\sigma}$ em F, enquanto que a forma quadrática $tr_{\mathrm{F|K}}(q)$ está definida de V em K. Precisamos encontrar uma isometria $\varphi : \mathrm{F} \otimes_{\mathrm{K}} \mathrm{V} \longrightarrow \perp_{\sigma \in \mathrm{G}} \mathrm{V}^{\sigma}$, de modo que $b_{\perp q^{\sigma}}(\varphi(x \otimes y), \varphi(x' \otimes y')) = tr(b_q)^{\mathrm{F}}(x * y, x' * y')$. Seja $\varphi(x \otimes_{\mathrm{K}} y) = \sum_{\sigma \in \mathrm{G}} (x * y)$ e estenda φ a todo $\mathrm{F} \otimes_{\mathrm{K}} \mathrm{V}$ por linearidade .

A função φ está bem definida pois, dados $x\alpha \otimes y$ e $x \otimes \alpha y$, com $\alpha \in \mathrm{K}$, temos que $\varphi(x\alpha \otimes y) = \sum_{\sigma \in \mathrm{G}} x\alpha * y = \sum \sigma(x\alpha)y = \sum \sigma(x)\alpha y = \sum_{\sigma \in \mathrm{G}} x * (\alpha y) = \varphi(x \otimes \alpha y)$. Temos também que φ é F-linear, pois $\varphi(x'(x \otimes y)) = \varphi(x'x \otimes y) = \sum_{\sigma \in \mathrm{G}} x'x * y = \sum \sigma(x'x)y = \sum \sigma(x')\sigma(x)y = \sum \sigma(x')(\sigma(x)y) = \sum_{\sigma \in \mathrm{G}} x' * (x * y) = x' * \varphi(x \otimes y)$, para todos $x', x \in \mathrm{F}$ e

$y \in \mathrm{V}$. E mais, $b_{\perp q^\sigma}(\varphi(x \otimes y), \varphi(x' \otimes y')) = \sum_{\sigma \in \mathrm{G}} b_q^\sigma(x * y, x' * y') = \sum_{\sigma \in \mathrm{G}} \sigma^{-1} b_q(\sigma(x)y, \sigma(x')y') =$
$= \sum_{\sigma \in \mathrm{G}} \sigma^{-1}(\sigma(x)\sigma(x')b_q(y, y')) = xx' \sum_{\sigma \in \mathrm{G}} \sigma^{-1}(b_q(y, y')) = xx' tr(b_q(y, y')) = xx'(tr * b_q)(y, y') =$
$tr(b_q)^{\mathrm{F}}(x * y, x' * y')$.

Como $dim_{\mathrm{F}}(\mathrm{F} \otimes_{\mathrm{K}} \mathrm{V}) = dim_{\mathrm{K}}(\mathrm{V}) = [\mathrm{F} : \mathrm{K}].dim_{\mathrm{F}}(\mathrm{V})$ e $dim_{\mathrm{F}}(\perp_{\sigma \in \mathrm{G}} \mathrm{V}^\sigma) = |\mathrm{G}|.dim_{\mathrm{F}}(\mathrm{V}) = [\mathrm{F} : \mathrm{K}].dim_{\mathrm{F}}(\mathrm{V})$, para verificarmos que φ é um isomorfismo, resta demonstrar que φ é injetiva. Suponhamos que $\varphi(z) = 0$, com $z \in \mathrm{F} \otimes_{\mathrm{K}} \mathrm{V}$. Como φ preserva o produto interno, segue que $0 = b_{\perp q^\sigma}(\varphi(z), \varphi(x)) = tr(q)^{\mathrm{F}}(z, x)$, para todo $x \in \mathrm{F} \otimes_{\mathrm{K}} \mathrm{V}$, e portanto z pertence ao radical do espaço quadrático $(\mathrm{F} \otimes_{\mathrm{K}} \mathrm{V}, tr(q)^{\mathrm{F}})$. Mas pela Proposição 5.0.2, $(\mathrm{F} \otimes_{\mathrm{K}} \mathrm{V}, tr(q)^{\mathrm{F}})$ é regular, assim $z = 0$. Portanto φ é injetivo. □

Agora estamos em condições melhores e podemos começar o estudo da forma traço $\mathrm{T} : \mathrm{F} \longrightarrow \mathbb{Q}_p$, definida por $\mathrm{T}(x) = tr(x^2)$, onde F é uma extensão galoisiana de grau 2, 3 ou 4 de $\mathbb{Q}_p$.

5.1 Extensões Quadráticas e Cúbicas de $\mathbb{Q}_p$.

Seja F uma extensão quadrática de $\mathbb{Q}_p$. Pelo Teorema 5.0.2 (i) $\mathrm{F} = \mathbb{Q}_p(\sqrt{\delta})$, onde δ é o discriminante de F. Enunciemos

Teorema 5.1.1 *Seja* $\mathrm{F} = \mathbb{Q}_p(\sqrt{\delta})$ *uma extensão quadrática de* $\mathbb{Q}_p$ *e* $\mathrm{T} : \mathrm{F} \longrightarrow \mathbb{Q}_p$ *a forma traço* $\mathrm{T}(x) = tr(x^2)$ *(ou* $b_{\mathrm{T}} : \mathrm{F} \times \mathrm{F} \longrightarrow \mathbb{Q}_p$, $b_{\mathrm{T}}(x, y) = tr(xy)$*). Então*

$$s(\mathrm{T}) = [2, \delta] = \begin{cases} 1, \text{ se } \delta \in \mathcal{U} \text{ ou } \overline{2} \in \overline{\mathbb{Q}}_p^2 \\ -1, \text{ caso contrário.} \end{cases}$$

Demonstração: Seja $\mathrm{G} = Gal(\mathrm{F} : \mathbb{Q}_p) = \{id, \ \sigma\}$, onde $\sigma(\alpha + \beta\sqrt{\delta}) = \alpha - \beta\sqrt{\delta}$. Assim para todo $x = \alpha + \beta\sqrt{\delta}$, $y = \alpha_1 + \beta_1\sqrt{\delta}$ temos que $b_{\mathrm{T}}(x, y) = tr\left((\alpha\alpha_1 + \delta\beta\beta_1) + (\alpha\beta_1 + \alpha_1\beta)\sqrt{\delta}\right) = 2(\alpha\alpha_1 + \delta\beta\beta_1)$. Logo na base $\{1, \sqrt{\delta}\}$ a forma traço T se escreve na forma $\mathrm{T} \simeq \langle 2 \rangle \perp \langle 2\delta \rangle \simeq \langle 2, 2\delta \rangle$. Segue-se que $s(\mathrm{T}) = [2, 2][2, \delta]$. Como $2 \in D(\langle 1, 1 \rangle)$ pelo Teorema 1.3.1 temos que $\langle 1, 1 \rangle \simeq \langle 2, x \rangle$ e calculando o determinante encontramos $x = 2$. Logo $\langle 1, 1 \rangle \simeq \langle 2, 2 \rangle$. Consequentemente $1 \in D(\langle 2, 2 \rangle)$ e pelo Teorema 2.1.1 (6) vem que $[2, 2] = 1_{Br}$. Assim $s(\mathrm{T}) = [2, \delta]$. Como $\langle 2, \delta \rangle \simeq \langle 2 \rangle \langle 1, 2\delta \rangle$ se δ é uma

unidade então $D(\langle 2,\delta\rangle) = 2D(\langle 1,2\delta\rangle) = 2\{1,u\} = \{1,u\}$ ou $\dot{\mathbb{Q}}_p$ (veja Lema 5.0.2). Como $2 \in \mathcal{U}$, $D(\langle 2,\delta\rangle) = \{1,u\}$ ou $\dot{\mathbb{Q}}_p$. Logo $\langle 2,\delta\rangle$ representa 1, e novamente $[2,\delta] = 1$.

No caso em que $\overline{2} \in \dot{\overline{\mathbb{Q}}}_p^{\,2}$, então pelo Lema 4.0.1 $2 \in \dot{\mathbb{Q}}_p^2$. Logo $\langle 2,\delta\rangle \simeq \langle 1,\delta\rangle$ representa 1, e novamente $s(\mathrm{T}) = 1$.

Finalmente, se $2 \notin \dot{\mathbb{Q}}_p^2$ e δ não é uma unidade, então $\{1,2,\delta,2\delta\}$ é um conjunto de representantes das classes de quadrados de $\mathbb{Q}_p$. Dessa forma, $D(\langle 2,\delta\rangle) = 2D(\langle 1,2\delta\rangle) = 2\{1,2\delta\} = \{2,\delta\}$, ou seja, $\langle 2,\delta\rangle$ não representa 1. Portanto $s(\mathrm{T}) = -1$. □

Teorema 5.1.2 *Seja* $\mathrm{F} = \mathbb{Q}_p(\theta)$ *uma extensão cúbica da* $\mathbb{Q}_p$. *Então* $s(\mathrm{T}) = 1$.

Demonstração: A forma quadrática associada à forma bilinear $b(x,y) = xy$ é denotada por $q = \langle 1\rangle$. Logo $tr(\langle 1\rangle)_{\mathrm{F}} \simeq \perp_{\sigma\in \mathrm{G}} \langle 1\rangle^{\sigma} = \langle 1\rangle^{\sigma_1} \perp \langle 1\rangle^{\sigma_2} \perp \langle 1\rangle^{\sigma_3} = \langle \sigma_1^{-1}(1)\rangle \perp \langle \sigma_2^{-1}(1)\rangle \perp \langle \sigma_3^{-1}(1)\rangle = \langle 1\rangle \perp \langle 1\rangle \perp \langle 1\rangle = \langle 1,1,1\rangle$. Portanto $\mathrm{T} \simeq \langle 1,1,1\rangle$ em $\mathbb{Q}_p$. Assim, $s(\mathrm{T}) = [1,1][1,1][1,1] = [1,1]$. Como $\langle 1,1\rangle$ representa 1, pelo Teorema 2.1.1 temos que $s(\mathrm{T}) = 1$. □

5.1.1 Extensões Galoisianas de Grau 4

Como $\mathrm{G} = Gal(\mathrm{F},\mathbb{Q}_p)$ é um grupo cíclico ou o grupo de Klein, existe um subgrupo normal de G de ordem 2 e consequentemente uma extensão galoisiana intermediária L sobre $\mathbb{Q}_p$ tal que $\mathbb{Q}_p \subsetneq \mathrm{L} \subsetneq \mathrm{F}$. Como toda extensão quadrática é uma extensão radical, temos que $\mathrm{L} = \mathbb{Q}_p(\sqrt{a})$, com $a \in \mathbb{Q}_p \smallsetminus \dot{\mathbb{Q}}_p^2$ e $\mathrm{F} = \mathrm{L}(\sqrt{a_1})$, com $a_1 \in \mathrm{L} \smallsetminus \dot{\mathrm{L}}^2$.

Lema 5.1.1 *Sejam* $a \in \dot{\mathbb{Q}}_p \smallsetminus \dot{\mathbb{Q}}_p^2$, *com* $p \neq 2$ *e* $\mathrm{L} = \mathbb{Q}_p(\sqrt{a})$.

(i) *Se* $-a \notin \dot{\mathbb{Q}}_p^2$, *então* $\dfrac{\dot{\mathrm{L}}}{\dot{\mathrm{L}}^2} = \{1,\sqrt{a},\beta,\beta\sqrt{a}\}$, *onde* $\beta \in \dot{\mathbb{Q}}_p \smallsetminus \dot{\mathbb{Q}}_p^2$;

(ii) *Se* $-a \in \dot{\mathbb{Q}}_p^2$, *então* $\dfrac{\dot{\mathrm{L}}}{\dot{\mathrm{L}}^2} = \{1,p,\sqrt{-1},p\sqrt{-1}\}$.

Demonstração: Sejam $\dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2} = \{1,a,\beta,a\beta\}$ e $\mathrm{L} = \mathbb{Q}_p(\sqrt{a})$, demonstremos que $\beta\mathrm{L}^2 \neq \mathrm{L}^2$ e $\beta\sqrt{a}\mathrm{L}^2 \neq \mathrm{L}^2$.

Se $\beta = (x+y\sqrt{a})^2 \in \mathrm{L}^2$, então $\beta = x^2+ay^2+2xy\sqrt{a}$ em L. Logo $\beta = x^2+ay^2$ e $2xy = 0$. Como $\beta \notin \dot{\mathbb{Q}}_p^2$, temos que $y \neq 0$. Logo $x = 0$ e $\beta = ay^2$ em $\dot{\mathbb{Q}}_p$, o que é um absurdo. Portanto $\beta\mathrm{L}^2 \neq \mathrm{L}^2$.

Agora se $\beta\sqrt{a} \in \mathrm{L}^2$, então $\beta\sqrt{a} = (x + y\sqrt{a})^2$, ou seja, $\beta\sqrt{a} = x^2 + ay^2 + 2xy\sqrt{a}$. Daí, $x^2 + ay^2 = 0$ e $2xy = \beta$. Como $x \neq 0$ e $y \neq 0$, temos que $a = -\left(\frac{x}{y}\right)^2$.

Assim, se $-a \notin \dot{\mathbb{Q}}_p^2$, temos um absurdo e $\beta\sqrt{a} \notin \mathrm{L}^2$. Consequentemente, $\frac{\dot{\mathrm{L}}}{\dot{\mathrm{L}}^2} = \{1, \sqrt{a}, \beta, \beta\sqrt{a}\}$.

Se $-a \in \dot{\mathbb{Q}}_p^2$, ou seja, $a = -1$ em $\frac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2}$, então $\frac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2} = \{1, -1, \beta, -\beta\}$ e sem perda de generalidade, podemos supor $\beta = p$. Então temos $x^2 - y^2 = 0$ e $2xy = p$. Logo $y = x$ ou $y = -x$, e $2x^2 = p$ ou $-2x^2 = p$. Calculando as valorizações, obtemos $1 = v_p(p) = v_p(2) + 2v_p(x) = v_p(-2) + 2v_p(x)$, ou seja, $1 = 2v_p(x) \in \mathbb{Z}$, absurdo. Logo $p\sqrt{-1} \notin \dot{\mathrm{L}}^2$ e então temos as 4 classes de quadrados em L, $\frac{\dot{\mathrm{L}}}{\dot{\mathrm{L}}^2} = \{1, p, \sqrt{-1}, p\sqrt{-1}\}$. □

Lema 5.1.2 *Sejam* $\mathrm{L} = \mathbb{Q}_p(\sqrt{a})$ *e* $\mathrm{F} = \mathrm{L}(\sqrt{a_1})$, $a_1 = \alpha + \beta\sqrt{a} \in \mathrm{L} \setminus \dot{\mathrm{L}}^2$. *Se* $-a \notin {\mathbb{Q}_p}^2$, *então podemos considerar* $a_1 \in \mathbb{Q}_p$ *se, e somente se,* $Gal(\mathrm{F}, \mathbb{Q}_p)$ *é o grupo de Klein. Caso contrário* $a_1 = \beta\sqrt{a}$, *isto é,* $tr_{\mathrm{L}|\mathbb{Q}_p}(a_1) = 0$.

Demonstração: Temos que $a_1 \in \dot{\mathbb{Q}}_p$ se, e somente se, $\beta = 0$. E neste caso, $a_1 = \alpha$. Como $\mathrm{F} = \mathrm{L}(\sqrt{a_1})$ é uma extensão de $\mathbb{Q}_p$ de grau 4 segue que $\mathbb{Q}_p(\sqrt{a}) = \mathrm{L} \neq \mathbb{Q}_p(\sqrt{a_1})$. Logo temos pelo menos duas extensões intermediárias entre $\mathbb{Q}_p$ e F. Pelo Teorema 5.0.2(i), $Gal(\mathrm{F}, \mathbb{Q}_p)$ é o grupo de Klein.

Reciprocamente, se $Gal(\mathrm{F}, \mathbb{Q}_p)$ é o grupo de Klein então temos três extensões quadráticas intermediárias correspondentes aos subgrupos normais de ordem 2 de $Gal(\mathrm{F}, \mathbb{Q}_p)$. São: $\mathbb{Q}_p(\sqrt{u})$, $\mathbb{Q}_p(\sqrt{p})$ e $\mathbb{Q}_p(\sqrt{up})$, onde $\frac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2} = \{1,\ u,\ p,\ up\}$, u uma unidade em $\mathbb{Q}_p$, tal que $\overline{u} \notin {\overline{\mathbb{Q}}_p}^2$. Consequentemente, $\sqrt{p} \notin \mathbb{Q}_p(\sqrt{u})$ e $\mathrm{F} = \mathbb{Q}_p(\sqrt{u}, \sqrt{p}) = \mathbb{Q}_p(\sqrt{u}, \sqrt{up})$. Logo podemos considerar $a_1 = u$, p, ou up, e portanto $a_1 \in \mathbb{Q}_p$.

Caso contrário, do Lema 5.1.1 segue que $a_1 = \sqrt{a}$ ou $a_1 = \beta\sqrt{a}$, para algum $\beta \in \dot{\mathbb{Q}}_p$, e neste caso $tr_{\mathrm{L}|\mathbb{Q}_p}(a_1) = 0$. □

Lema 5.1.3 *Sejam* F *uma extensão galoisiana de* $\mathbb{Q}_p$ *de grau quatro com* $G = Gal(\mathrm{F}, \mathbb{Q}_p)$, *e* L *uma extensão intermediária própria de* $\mathbb{Q}_p$ *contida em* F. *Então:*

(i) *Se* G *é o grupo de Klein então* $\mathrm{T} \simeq \langle 1, u, p, up \rangle$, *onde* $1,\ u,\ p,\ up$ *é um conjunto de representantes das classes de quadrados de* $\mathbb{Q}_p$;

(ii) *Se G é cíclico então* $\mathrm{T} \simeq \langle 1, \delta \rangle \perp \mathbb{H}$.

Demonstração:

(i) Vimos na demonstração do Lema 5.1.2 que $\mathrm{F} = \mathbb{Q}_p(\sqrt{u}, \sqrt{p})$ e $\mathrm{L} = \mathbb{Q}_p(\sqrt{u})$ ou $\mathbb{Q}_p(\sqrt{p})$, ou $\mathbb{Q}_p(\sqrt{up})$. Em qualquer caso, tomando a $\mathbb{Q}_p$-base $\{1, \sqrt{a}\}$ de $\mathrm{L} = \mathbb{Q}_p(\sqrt{a})$ completemos a $\mathbb{Q}_p$-base $B = \{1, \sqrt{u}, \sqrt{p}, \sqrt{up}\}$ de F. Vamos calcular o traço de cada elemento de B.

Seja $x = \sqrt{u}$. Então $X^2 - u = p(X)$ é o polinômio minimal de x sobre $\mathbb{Q}_p$. Logo o polinômio característico de x é $f_x(X) = p(X)^2 = X^4 - 2uX^2 + u^2$. Portanto $tr(\sqrt{u}) = 0$ (pois é o coeficiente de X^3 do polinômio $f_x(X)$). Do mesmo modo $tr(\sqrt{p}) = tr(\sqrt{up}) = 0$. Por definição a matriz da forma quadrática traço T na base B é a matriz da forma bilinear associada à T, portanto

$$(\mathrm{T})_B = (b_{\mathrm{T}})_B = \begin{pmatrix} tr(1) & tr(\sqrt{u}) & tr(\sqrt{p}) & tr(\sqrt{up}) \\ tr(\sqrt{u}) & tr(u) & tr(\sqrt{up}) & tr(u\sqrt{p}) \\ tr(\sqrt{p}) & tr(\sqrt{up}) & tr(p) & tr(p\sqrt{u}) \\ tr(\sqrt{up}) & tr(u\sqrt{p}) & tr(p\sqrt{u}) & tr(up) \end{pmatrix}.$$

Como o $tr : \mathrm{F} \longrightarrow \mathbb{Q}_p$ é uma função $\mathbb{Q}_p$-linear temos

$$(\mathrm{T})_B = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4u & 0 & 0 \\ 0 & 0 & 4p & 0 \\ 0 & 0 & 0 & 4up \end{pmatrix}.$$

Ou então $\mathrm{T} \simeq \langle 2^2, 2^2u, 2^2p, 2^2up \rangle \simeq \langle 1, u, p, up \rangle$.

(ii) Se G é um grupo cíclico então $\mathrm{L} = \mathbb{Q}_p(\sqrt{\delta})$ é a única extensão intermediária de grau dois de $\mathbb{Q}_p$ contida em F (Teorema 5.0.2(i)) e $\mathrm{F} = \mathrm{L}(\sqrt{a_1})$, com $tr_{\mathrm{L}|\mathbb{Q}_p}(a_1) = 0$ (ver Lema 5.1.2). Logo $a_1 = \beta\sqrt{\delta}$ com $\beta \in \mathbb{Q}_p$. Seja $B_1 = \left\{1, \sqrt{\delta}, \sqrt{\beta\sqrt{\delta}}, \sqrt{\delta}.\sqrt{\beta\sqrt{\delta}}\right\}$. É fácil demonstrar que B_1 é uma $\mathbb{Q}_p$-base de F. Para calcular a matriz da forma bilinear associada à quadrática traço na base B_1 precisamos calcular os traços dos elementos de B_1. Temos que $X^4 - \delta\beta^2$ é o polinômio característico de $\sqrt{\beta\sqrt{\delta}}$ e $(X^2 - \delta)^2 = X^4 - 2\delta X^2 - \delta^2$, $X^4 - \beta^2\delta^3$ são os polinômios característicos de $\sqrt{\delta}$ e $\sqrt{\delta\beta\sqrt{\delta}}$, respectivamente. Como nenhum deles tem

o termo X^3 temos que $tr\left(\sqrt{\beta\sqrt{\delta}}\right) = tr(\sqrt{\delta}) = tr\left(\sqrt{\delta\beta\sqrt{\delta}}\right) = 0$. Assim $(\mathrm{T})_{B_1} = (b_{\mathrm{T}})_{B_1}$ é dada por

$$(\mathrm{T})_{B_1} = \begin{pmatrix} tr(1) & tr(\sqrt{\delta}) & tr\left(\sqrt{\beta\sqrt{\delta}}\right) & tr\left(\sqrt{\beta\delta\sqrt{\delta}}\right) \\ tr(\sqrt{\delta}) & tr(\delta) & tr\left(\sqrt{\beta\delta\sqrt{\delta}}\right) & tr\left(\delta\sqrt{\beta\sqrt{\delta}}\right) \\ tr\left(\sqrt{\beta\sqrt{\delta}}\right) & tr\left(\sqrt{\beta\delta\sqrt{\delta}}\right) & tr(\beta\sqrt{\delta}) & tr(\beta\delta) \\ tr\left(\sqrt{\beta\delta\sqrt{\delta}}\right) & tr\left(\delta\sqrt{\beta\sqrt{\delta}}\right) & tr(\beta\delta) & tr(\beta\delta\sqrt{\delta}) \end{pmatrix}.$$

Como $tr : \mathrm{F} \longrightarrow \mathbb{Q}_p$ é $\mathbb{Q}_p$-linear temos

$$(\mathrm{T})_{B_1} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4\delta & 0 & 0 \\ 0 & 0 & 0 & 4\beta\delta \\ 0 & 0 & 4\beta\delta & 0 \end{pmatrix}.$$

Desde que $det\begin{pmatrix} 0 & 4\beta\delta \\ 4\beta\delta & 0 \end{pmatrix} = -1\dot{\mathbb{Q}}_p^2$, pelo Teorema 1.4.1 temos que $\mathrm{T} \simeq \langle 2^2, 2^2\delta\rangle \perp \mathbb{H} \simeq \langle 1, \delta\rangle \perp \mathbb{H}$. □

Teorema 5.1.3 *Sejam* F *uma extensão galoisiana de grau quatro de* $\mathbb{Q}_p$ *e* $G = Gal(\mathrm{F}, \mathbb{Q}_p)$. *Então*

(A) $-1 \in \dot{\mathbb{Q}}_p^2$,

(i) *Se* G *é o grupo de Klein, então* $\mathrm{T} \simeq \langle 1, u, p, up\rangle$ *é anisotrópica e* $s(\mathrm{T}) = -1$;

(ii) *Se G é cíclico, então* $\mathrm{T} \simeq \langle 1, \delta\rangle \perp \mathbb{H} \simeq 2\mathbb{H}$ *e* $s(\mathrm{T}) = 1$.

(B) $-1 \notin \dot{\mathbb{Q}}_p^2$, *então* $\mathrm{T} \simeq 2\mathbb{H}$ *e* $s(\mathrm{T}) = 1$.

Demonstração:

(i) Seja $\frac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2} = \{1, u, p, up\}$, com $u \notin \dot{\mathbb{Q}}_p^2$. Pelo Teorema 4.0.4(ii) $\langle 1, -u, -p, up\rangle$ é única forma quadrática anisotrópica de dimensão 4 sobre $\mathbb{Q}_p$ e $\left(\frac{u,p}{\mathbb{Q}_p}\right)$ a única álgebra de quatérnios

com divisão sobre $\mathbb{Q}_p$. Desde que $-1 \in \dot{\mathbb{Q}}_p^2$, pelo Lema 5.1.3(i) segue que $\mathrm{T} \simeq \langle 1, -u, -p, up\rangle$. Pelos Corolário 4.0.4 e Definição 4.0.6 segue que $s(\mathrm{T}) = -1$.

(ii) Se G é cíclico, segue do Lema 5.1.3 (ii) que $\mathrm{T} \simeq \langle 1, \delta\rangle \perp \mathbb{H} \simeq \langle 1, \delta, 1, -1\rangle \simeq \langle 1, \delta, 1, 1\rangle$ pois $1 = -1 \in \dfrac{\dot{\mathbb{Q}}_p}{\dot{\mathbb{Q}}_p^2}$. Daí, $s(\mathrm{T}) = [1, \delta]$. Como $\langle 1, \delta\rangle$ representa 1, segue-se que $s(\mathrm{T}) = 1$.

Para o caso (B) podemos considerar $1, -1, p, -p$ os representantes das classes de quadrados de $\mathbb{Q}_p$.

Se G é o grupo de Klein, pelo Lema 5.1.3(i) $\mathrm{T} \simeq \langle 1, -1, p, -p\rangle \simeq 2\mathbb{H}$. Pelo Corolário 4.0.4(i) $s(\mathrm{T}) = [1, -p] = 1$, pois a única álgebra de quatérnios com divisão sobre $\mathbb{Q}_p$ é $\left(\dfrac{-1, p}{\mathbb{Q}_p}\right)$ (veja Teorema 4.0.4(iii)).

Se G é cíclico, do Corolário 5.0.2 temos que $\delta \in D(\langle 1, 1\rangle)$. Como $D(\langle 1, 1\rangle) = \{1, -1\}\dot{\mathbb{Q}}_p^2$ e $\delta \notin \dot{\mathbb{Q}}_p^2$ temos que $\delta = -1$. Pelo Lema 5.1.3 (ii) $\mathrm{T} \simeq 2\mathbb{H}$. Logo $s(\mathrm{T}) = 1$ pelos Corolário 4.0.4 e Definição 4.0.6. □

Referências Bibliográficas

[G] GALLAGHER, V. P., *Local trace forms.* 1979, p.167-174. (Linear and Multilinear Algebra; 7).

[L] LAM, T. Y., *The algebraic theory of quadratic forms.* New York: W. A. Benjamin, 1980. (Mathematics Lecture Note Series).