INVARIANTES DE FORMAS QUADRÁTICAS E MENORES PRINCIPAIS DE MATRIZES

Marcele Tavares

Centro de Ciências Exatas

Universidade Estadual de Maringá

Programa de Pós-Graduação em Matemática

(Mestrado)

Orientadora: Rosali Brusamarelo

Maringá - Pr

2006

INVARIANTES DE FORMAS QUADRÁTICAS E MENORES PRINCIPAIS DE MATRIZES

Marcele Tavares

Tese submetida ao corpo docente do Programa de Pós-Graduação em Matemática da Universidade Estadual de Maringá - UEM-Pr, como parte dos requisitos necessários à obtenção do grau de Mestre.

Aprovada por:

Prof^a. PhD. Rosali Brusamarello - UEM .....
(Orientadora)

Prof. Dr. Marcelo E. Hernandes - UEM .....

Prof^a. Dr^a Ires Dias - USP .....

Maringá

10 de Março

Aos meus pais com todo amor

e ao meu amor sempre companheiro, Rafael.

Agradecimentos

São muitas as pessoas que gostaria de agradecer, não apenas por este trabalho, mas por terem tido participação na minha formação e na minha vida.

Agradeço a minha **mãe** por tantas coisas! Mas principalmente por me dar a certeza de que apesar da distância, ela sempre esteve comigo. Por acreditar nos meus sonhos e fazer deles os seus. E não posso esquecer de agradecer as tantas novenas e orações.

Agradeço ao meu **pai** pela certeza de que tudo vai dar certo. Pela sabedoria de vida, pela calma e paciência mesmo quando já não a tinha. E principalmente pelo amor que dedica a nossa família.

Agradeço ao meu grande amor, **Rafa**, por ter sido tão companheiro. Por ter me dado força em cada momento de angústia, por entender minhas horas de estudo e por ter sido muito, mas muito mais que um simples namorado.

Agradeço a minha orientadora, Prof^a. Dr^a. **Rosali Brusamarello**, pelo apoio, incentivo, paciência, amizade e dedicação na realização deste trabalho.

Agradeço aos meus irmãos, **Martinha** e **Marquinho**, que almejaram muito que este dia chegasse.

Agradeço a todos meus amigos que estiveram ao meu lado estes 2 anos, mas em especial ao meu amigo **João Lorin** que esteve em momentos difíceis e que tentou de tudo para me ver feliz.

Agradeço à **CAPES** por parte do apoio financeiro.

Agradeço à **Lucia** por sua eficiência, paciência e amizade.

Agradeço **aos professores** do Departamento de Matemática da UEM que contribuíram com a minha formação.

E enfim, agradeço a **Deus** que apesar de não lhe dar a devida atenção sempre esteve comigo abençoando minhas decisões.

Resumo

Neste trabalho iremos caracterizar as matrizes de Hankel finitas e mostraremos que tais matrizes surgem naturalmente como representação matricial de formas traço e traço escalares de extensão de corpos separáveis. Iremos ainda utilizar o método dos menores principais de matrizes para calcular a assinatura e o invariante de Hasse de formas quadráticas.

Palavras chaves: Matrizes de Hankel; formas quadráticas; formas traço; menores.

Abstract

In this work we give a characterization of finite Hankel matrices and we show that such matrices arise naturally as matrix representations of scaled trace forms of separables extensions of fields. We also use the principal minor method to calculate the signature and the Hasse invariant of quadratic forms.

Keywords: Hankel matrices; quadratic forms; trace forms; minors.

Sumário

Introdução

A teoria de formas quadráticas como é estudada atualmente foi sistematizada por Ernst Witt em 1937. Porém as formas quadráticas já eram estudadas muito antes, provavelmente surgiram na Babilônia. Trabalhando essencialmente sobre os corpos dos números reais e complexos, os matemáticos do século XIX já se preocupavam com os invariantes das formas quadráticas. Eles sabiam como calcular a assinatura de formas quadráticas usando os menores principais das matrizes simétricas que representam estas formas, contanto que não houvesse muitos sucessivos menores principais nulos. Podemos citar os trabalhos de Sylvester [11], Jacobi [6], Gundelfinger [3], Frobenius [1]. Na verdade Frobenius mostrou que a condição sobre os menores nulos pode ser removida quando a forma é representada por uma matriz de Hankel. Mais tarde, o método dos menores principais foi adaptado para calcular o invariante de Hasse de formas quadráticas sobre corpos locais, ver [7].

Um dos objetivos deste trabalho é apresentar o método dos menores principais na linguagem moderna de formas quadráticas, inclusive para o caso de matrizes de Hankel. Isto está feito no Capítulo 4.

Um segundo objetivo é o estudo das matrizes de Hankel, pois estas surgem naturalmente como uma representação matricial da formas traço e traço escalares de extensões de corpos separáveis. Fizemos isto no Capítulo 3.

Para atingir os dois objetivos citados acima foi necessário um estudo dos fundamentos da teoria de formas quadráticas (feito no Capítulo 1) e um estudo das álgebras centrais simples visando definir o invariante de Hasse (feito no Capítulo 2).

Capítulo 1

Preliminares

Durante este capítulo faremos uma introdução à teoria de formas quadráticas, apresentando alguns resultados que fundamentam esta teoria. Neste trabalho F denotará um corpo com característica diferente de 2 e os espaços vetoriais sobre F serão sempre de dimensão finita. O grupo multiplicativo dos elementos não nulos de F denotaremos por $\dot{F}$.

1.1 Espaços Bilineares e Quadráticos

Iniciamos recordando os conceitos de forma bilinear e forma quadrática vistos nos cursos de Álgebra Linear.

Definição 1.1. Seja V um espaço vetorial sobre F. Uma *forma bilinear simétrica* sobre F é uma aplicação $B : V \times V \to F$ que satisfaz as propriedades:

(1) $B(x + y, z) = B(x, z) + B(y, z)$, para todo $x, y, z \in V$;

(2) $B(\alpha x, y) = \alpha B(x, y) = B(x, \alpha y)$, para todo $x, y \in V$ e $\alpha \in F$;

(3) $B(x, y) = B(y, x)$, para todo x, $y \in V$.

Definição 1.2. Seja V um espaço vetorial sobre F. A aplicação $q : V \to F$ é chamada de *forma quadrática sobre* V se satisfaz as seguintes propriedades:

(1) $q(\alpha x) = \alpha^2 q(x)$, para todo $x \in V, \alpha \in F$;

(2) $B_q : V \times V \to F$ definida por $B_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$, para todo $x, y \in V$, é uma forma bilinear simétrica .

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

Dada uma forma bilinear simétrica B sobre um espaço vetorial V, podemos definir $q_B : V \to F$ por $q_B(x) = B(x, x)$. A função q_B definida é uma forma quadrática e é chamada *forma quadrática associada à* B. Quando não houver perigo de confusão usaremos apenas q para denotar q_B e apenas B para denotar B_q.

Observação 1.3. Sejam $\mathcal{B} = \{e_1, ..., e_n\}$ uma base do espaço vetorial V e $x = \sum_{i=1}^{n} x_i e_i$, $y = \sum_{j=1}^{n} y_j e_j$ elementos de V. Se B é uma forma bilinear sobre F, então

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

Definição 1.4. A matriz $M_B = (B(e_i, e_j))$ é chamada *matriz da forma bilinear* B em relação à base $\mathcal{B}$.

Deste modo, temos

$$B(x, y) = (x_1 \ x_2 \ ... \ x_n) \begin{pmatrix} B(e_1, e_1) & \dots & B(e_1, e_n) \\ \vdots & \ddots & \vdots \\ B(e_n, e_1) & \dots & B(e_n, e_n) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = [x]_{\mathcal{B}}^t M_B [y]_{\mathcal{B}},$$

onde $[x]_B$ é o vetor coordenadas.

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

$$M_q = M_{B_q} \text{ e } q(x) = B_q(x, x) = [x]_{\mathcal{B}}^t M_{B_q} [x]_{\mathcal{B}}.$$

Definição 1.5. Um *espaço bilinear* é um par (V, B), onde V é um espaço vetorial sobre F e B é uma forma bilinear simétrica sobre V. Chamamos (V, q) *de espaço quadrático*, onde q é uma forma quadrática sobre V.

A verificação de que as correspondências $q \to B_q$ e $B \to q_B$ (ou $(V,q) \to (V,B_q)$ e $(V,B) \to (V,q_B)$) são inversas uma da outra é imediata desde que $q_{B_q} = q$ e $B_{q_B} = B$. Ou seja, podemos identificar formas quadráticas com formas bilineares. Assim, conceitos e propriedades de espaços quadráticos (ou formas quadráticas) podem ser transmitidos para espaços bilineares (ou formas bilineares) e vice-versa.

Vale ressaltar que esta correspondência biunívoca não ocorre se o corpo F for de característica 2 ou se estivermos trabalhando com formas bilineares sobre anéis em que 2 não é inversível.

Definição 1.6. Sejam $(V,B),(V',B')$ dois espaços bilineares. Dizemos que eles são *isométricos* se existe um isomorfismo linear $\tau : V \to V'$ tal que $B'(\tau(u),\tau(v)) = B(u,v)$, para todo $u,v \in V$ (ou $q_{B'}(\tau(u)) = q_B(u)$, para todo $u \in V$).

Notação $(V,B) \cong (V',B')$, $B \cong B'$, $q \cong q'$.

Ser isométrico é uma relação de equivalência onde a classe de equivalência $(q) = \{q' \mid q' \cong q\}$ é chamada *classe de isometria*.

Proposição 1.7. *Sejam (V,B), (V',B') espaços bilineares. Então $(V,B) \cong (V',B')$ se, e somente se, M_B é congruente a $M_{B'}$.*

Demonstração: Se existe um isomorfismo $\tau : V \to V'$, então $\dim V = \dim V'$. Considere $\{e_1,...,e_n\}$ e $\{e'_1,...,e'_n\}$ bases de V e V', respectivamente. Agora, se $C = (c_{ij})$ é a matriz da tranformação linear τ, então $\tau\ (e_i) = \sum_{k=1}^{n} c_{ki}e'_k$. Assim,

$$\begin{aligned} M_B &= (B(e_i,e_j)) = (B'(\tau(e_i),\tau(e_j))) \\ &= (B'(\sum_{k=1}^{n} c_{ki}e'_k, \sum_{l=1}^{n} c_{lj}e'_l)) \\ &= (\sum_{k,l=1}^{n} c_{ki}B'(e'_k,e'_l)c_{lj}) = C^t M_{B'} C. \end{aligned}$$

Portanto, M_B é congruente a $M_{B'}$.

Reciprocamente, temos que $M_B = C^t M_{B'} C$, para alguma matriz $C \in GL_n(F)$. Seja $\tau : V \to V'$ com $\tau(u) = C[u]$, onde $[u]$ são as coordenadas de u em ter-

mos de uma base de V. É claro que τ é um isomorfismo. Então $B'(\tau(u), \tau(v)) = (\tau(u))^t M_{B'}(\tau(v)) = (C[u])^t M_{B'}(C[v]) = [u]^t C^t M_{B'} C[v] = [u]^t M_B[v] = B(u, v)$. Portanto, $(V, B) \cong (V', B')$. $\square$

Definição 1.8. Seja (V, B) um espaço bilinear. Dois vetores $x, y \in V$ são *ortogonais se* $B(x, y) = 0$. Denotamos por $x \perp y$.

Se X e Y são subconjuntos de V, dizemos que X é *ortogonal* a Y se $B(x, y) = 0$, para todo $x \in X$ e para todo $y \in Y$. Denotamos por $X \perp Y$.

Definição 1.9. Sejam (V, B) um espaço bilinear e S um subconjunto de V. *O complemento ortogonal* de S é definido por

$$S^{\perp} = \{x \in V \mid B(x, S) = 0\}.$$

O complemento ortogonal de V é chamado de *radical* de (V, B), denotado por $V^{\perp} = rad\, V$.

Observação 1.10. **(1)** Claramente se $S \subset T$, então $T^{\perp} \subset S^{\perp}$. É fácil ver também que $S \subset (S^{\perp})^{\perp}$.

(2) Se W é um subespaço de V, então $(W, B|_{W \times W})$ é um espaço bilinear.

Proposição 1.11. *Sejam (V, B) um espaço bilinear, $\mathcal{B}$ uma base de V e M a matriz simétrica associada a forma bilinear B. São equivalentes*

(1) *M é não singular;*

(2) *$x \to B(x, -)$ define um isomorfismo $V \to V^{\star}$, onde $V^{\star}$ denota o espaço dual de V;*

(3) *Se $B(x, y) = 0$, para todo $y \in V$, então $x = 0$. Ou seja, $V^{\perp} = \{0\}$.*

Demonstração: (1) $\Rightarrow$ (2) Suponhamos que M é uma matriz não singular, isto é, inversível. Como M é inversível, temos que $[x]_B^t M \neq [y]_B^t M$, para todo $x, y \in V$, com $x \neq y$. Logo $B(x, -) \neq B(y, -)$, para todo $x \neq y$. Ou seja, $x \to B(x, -)$ é

uma aplicação injetiva e ainda $\dim V = \dim V^*$. Portanto $x \to B(x, -)$ define um isomorfismo de $V \to V^\star$.

(2) $\Rightarrow$ (3) Seja $\sigma : V \to V^\star$ o isomorfismo dado por $\sigma(x)(-) = B(x, -)$. Tomemos $x \in V$ de modo que $B(x, y) = 0$, para todo $y \in V$. Isto implica que $\sigma(x)(y) = 0$, para todo $y \in V$. Logo $\sigma(x) = 0$. Como σ é um isomorfismo, temos $x = 0$.

(3) $\Rightarrow$ (1) Usemos o fato de que M é inversível se, e somente se, $\det M \neq 0$.

Seja $M = (b_i j)$. Se $\det M = 0$, então $M.[y]_B = 0$ tem solução não nula, ou seja, existe $y' = (y_1, ..., y_n) \in V$, com $y_i \neq 0$ para algum i, tal que

$$\begin{cases} b_{11}y_1 + ... + b_{1n}y_n = 0 \\ \vdots \\ b_{n1}y_1 + ... + b_{nn}y_n = 0. \end{cases}$$

Assim, para todo $x \in V$ não nulo, temos $x^t M y' = 0$. Portanto $y' \in V^\perp$, ou seja, $V^\perp \neq \{0\}$, o que contradiz a hipótese (3). $\square$

Definição 1.12. Se uma das sentenças acima for verdadeira, dizemos que (V, B) é um *espaço bilinear regular*, ou equivalentemente, que q_B é uma *forma quadrática regular*.

Observação 1.13. Observe que (V, B) é regular se, e somente se, $\text{rad } V = 0$. E se (V, B) é regular, os subespaços de V não são necessariamente regulares.

Proposição 1.14. *Sejam (V, B) um espaço bilinear regular e W um subespaço de V. Então,*

(1) $\dim W + \dim W^\perp = \dim V$.

(2) $(W^\perp)^\perp = W$.

Demonstração: (1) Seja $\sigma : V \to V^\star$ o isomorfismo definido na proposição anterior. A projeção canônica $V^\star \to W^\star$ dada por $f \to f|_W$ é claramente sobrejetora.

Como o núcleo da composição $V \to V^\star \to W^\star$ é $W^\perp$, temos pelo Teorema do núcleo e imagem da álgebra linear o resultado desejado.

(2) Aplicando **(1)** para o subespaço $W^\perp$, obtemos $\dim\,(W^\perp)^\perp + \dim\,W^\perp = \dim V$. Logo $\dim\,(W^\perp)^\perp = \dim\,V - \dim\,W^\perp = \dim\,V - (\dim\,V - \dim\,W) = \dim\,W$. Como $W \subset (W^\perp)^\perp$, segue que $(W^\perp)^\perp = W$. $\square$

1.2 Diagonalização de Formas Quadráticas

Definição 1.15. Se (V, B) e (V', B') são dois espaços bilineares, então escrevemos $(V, B)\perp(V', B')$ para o espaço bilinear $(V \oplus V', B\perp B')$, onde

$$(B\perp B')((x, x'), (y, y')) = B(x, y) + B'(x', y').$$

O espaço $(V, B)\perp(V', B')$ é chamado de *soma ortogonal de* (V, B) *e* (V', B'). A soma ortogonal de espaços bilineares induz naturalmente uma soma ortogonal de espaços quadráticos $(V, q_B)\perp(V', q'_B) = (V \oplus V', q_B\perp q'_B)$, onde

$$(q_B\perp q_{B'})(x, x') = q_B(x) + q_{B'}(x').$$

Observação 1.16. De modo análogo, definimos soma ortogonal para n espaços quadráticos. Dados os espaços quadráticos (V_i, q_i), $i = 1, ..., n$ $(n \geq 2)$. Sejam $V = V_1 \oplus ... \oplus V_n$ e $q : V \to F$ definida por $q(x_1, ..., x_n) = \sum_{i=1}^{n} q_i(x_i)$. O par (V, q) é um espaço quadrático denotado por $(V, q) = (V_1, q_1)\perp ...\perp(V_n, q_n)$, chamado soma ortogonal dos espaços $(V_1, q_1), ..., (V_n, q_n)$. Observe que a forma bilinear associada a q é dada pela aplicação $B : V \times V \to F$ definida por

$$B((x_1, ..., x_n), (y_1, ..., y_n)) = B_1(x_1, y_1) + ... + B_n(x_n, y_n).$$

Quando o contexto for claro usaremos também a notação, $V_1\perp ...\perp V_n$ ou $q_1\perp ...\perp q_n$.

Proposição 1.17. *Sejam* (V_i, B_i) *espaços bilineares com* $i = 1, 2, 3$ *e* 4. *Então*

(1) $(V_1, B_1)\perp(V_2, B_2) \cong (V_2, B_2)\perp(V_1, B_1)$*;*

(2) $((V_1, B_1)\perp(V_2, B_2))\perp(V_3, B_3) \cong (V_1, B_1)\perp((V_2, B_2)\perp(V_3, B_3))$*;*

(3) *Se* $(V_1, B_1) \cong (V_2, B_2)$ *e* $(V_3, B_3) \cong (V_4, B_4)$*, então* $(V_1, B_1)\perp(V_3, B_3) \cong (V_2, B_2)$ $\perp(V_4, B_4)$*;*

(4) $(V_1, B_1)\perp(V_2, B_2)$ *é regular se, e somente se,* (V_1, B_1) *e* (V_2, B_2) *são regulares;*

(5) *Se* M_1 *é a matriz de* B_1 *na base* $\mathcal{B}_1$ *de* V_1 *e* M_2 *é a matriz de* B_2 *na base* $\mathcal{B}_2$ *de* V_2*, então a soma ortogonal* $B_1\perp B_2$ *tem a matriz* $\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$ *na base* $\mathcal{B}_1 \cup \mathcal{B}_2$ *de* $V_1 \oplus V_2$*.*

Demonstração: Imediata. □

Definição 1.18. Sejam (V, q) um espaço quadrático sobre F e $d \in \dot{F}$. Dizemos que q *representa* d se existe $v \in V$ tal que $q(v) = d$. Note que v é automaticamente um vetor não nulo. Denotaremos por $D_F(q)$ o conjunto formado pelos elementos de $\dot{F}$ que são representados por q, ou seja,

$$D_F(q) = \{d \in \dot{F} \mid \exists\ v \in V \text{ tal que } q(v) = d\}.$$

Quando não houver perigo de confusão usaremos $D(V)$ para denotar $D_F(q)$.

Definição 1.19. Uma forma quadrática é chamada *universal* se ela representa todos os elementos não nulos de F, isto é, $D_F(q) = \dot{F}$.

Observe que se $a, d \in \dot{F}$, então $d \in D(q_B)$ se, e somente, se $a^2 d \in D(q_B)$. Assim, $D(q_B)$ consiste de uma união de classes de $\dot{F}$ módulo $\dot{F}^2$.

Nosso objetivo agora é mostrar que todo espaço quadrático é isométrico a uma soma ortogonal de espaços unidimensionais. A classe de isometria de um espaço quadrático unidimensional (Fv, q), com $q(v) = d \in \dot{F}$, será denotada por $\langle d\rangle$. Claramente, $\langle d\rangle$ é regular se, e somente se, $d \in \dot{F}$.

Teorema 1.20. ***(Critério da Representação)*** *Seja* (V, q) *um espaço quadrático e* $d \in \dot{F}$*. Então* $d \in D(V)$ *se, e somente se,* $V \cong \langle d\rangle\perp V'$*, onde* (V', q') *é outro espaço quadrático.*

Demonstração: Se $V \cong \langle d\rangle \perp V'$, então $d \in D(\langle d\rangle \perp V') = D(V)$. Portanto $d \in D(V)$.

Reciprocamente, vamos primeiro reduzir ao caso em que V é regular. Para isso tomemos W o subespaço de V tal que $V = \text{rad } V \oplus W = \text{rad } V \perp W$. Assim $D(V) = D(\text{rad } V) + D(W) = D(W)$ e W é claramente regular. Logo, sem perda de generalidade, podemos supor que V é regular.

Suponha $d \in D(V)$, então existe $v \in V$ tal que $q(v) = d$. O subespaço quadrático (Fv, q) é isométrico a $\langle d\rangle$ e como $V = Fv \oplus (Fv)^{\perp}$ temos $(Fv) \cap (Fv)^{\perp} = \{0\}$. Como $\dim V = \dim Fv + \dim (Fv)^{\perp}$, temos $V \cong \langle d\rangle \perp (Fv)^{\perp}$. $\square$

A primeira consequência do Critério da Representação é a existência de uma base ortogonal em qualquer espaço quadrático. Em outras palavras, todo espaço quadrático é isométrico a uma soma ortogonal de espaços unidimensionais.

Corolário 1.21. *Se (V, q) é um espaço quadrático sobre F, então existem escalares $d_1, ..., d_n \in \dot{F}$ tais que $V \cong \langle d_1\rangle \perp ... \perp \langle d_n\rangle$.*

Demonstração: Se $D(V) = \varnothing$, então $B \equiv 0$ e V é isométrico a soma de $\langle 0\rangle's$.

Se existe algum $d_1 \in D(V)$, pelo teorema anterior $V \cong \langle d_1\rangle \perp V'$, para algum subespaço (V', B'). Aplicando o teorema anterior novamente com (V', B'), obtemos $V \cong \langle d_1\rangle \perp \langle d_2\rangle \perp V''$, para algum subespaço (V'', B'') e $d_2 \in \dot{F}$. Como V é de dimensão finita, após um número finito de passos obtemos o resultado. $\square$

Notação: $\langle d_1\rangle \perp ... \perp \langle d_n\rangle = \langle d_1, ..., d_n\rangle$ e $\langle d\rangle \perp ... \perp \langle d\rangle = n\langle d\rangle$.

Corolário 1.22. *Se (V, B) é um espaço bilinear e W um subespaço regular, então*

(1) $W \perp W^{\perp} = V$;

(2) *Se U é um subespaço de V tal que $V = W \perp U$, então $U = W^{\perp}$.*

Demonstração: Mostremos que **(1)** $\Rightarrow$ **(2)** e depois provemos a afirmação **(1)**. Se $V = W \perp U$, então claramente $U \subseteq W^{\perp}$ por **(1)**. Pela Proposição 1.14 $\dim U = \dim V - \dim W = \dim W^{\perp}$. Portanto $U = W^{\perp}$.

(1) Como $W \cap W^{\perp} = \text{rad } W = \{0\}$, é suficiente mostrar que $V = W + W^{\perp}$. Pelo Corolário 1.21, W tem uma base $\{x_1, ..., x_p\}$ ortogonal e pela regularidade de W, temos $B(x_i, x_i) \neq 0$, para todo i. Dado $z \in V$, considere o vetor

$$y = z - \sum_{i=1}^{p} \frac{B(z, x_i)}{B(x_i, x_i)} x_i.$$

Assim

$$\begin{aligned} B(y, x_j) &= B(z, x_j) - \sum_{i=1}^{p} \frac{B(z, x_i)}{B(x_i, x_i)} B(x_i, x_j) \\ &= B(z, x_j) - \frac{B(z, x_j)}{B(x_j, x_j)} B(x_j, x_j) \\ &= 0. \end{aligned}$$

Como y é ortogonal a todos os elementos de uma base de W, temos que $y \in W^{\perp}$.

Portanto, $z = \sum_{i=1}^{p} \frac{B(z,x_i)}{B(x_i,x_i)} x_i + y \in W \perp W^{\perp}$. $\square$

Corolário 1.23. *Seja (V, B) um espaço bilinear regular. Então o subespaço W é regular se, e somente se, existe $U \subseteq V$ tal que $V = W \perp U$.*

Demonstração: Pelo corolário anterior, basta tomar $U = W^{\perp}$. Reciprocamente, se $V = W \perp U$, então rad $W \subseteq$ rad $V = 0$. Portanto, W é regular. $\square$

Definição 1.24. O *determinante* de uma forma quadrática q não singular é definido por $d(q) = \det(M_q)\dot{F}^2$, onde M_q é a matriz simétrica associada a q.

Pela Proposição 1.7, se $q \cong q'$, então $M_q = C^t M_{q'} C$, para uma matriz não singular C. Assim $d(q) = \det(M_q).\dot{F}^2 = \det(M_{q'}).(\det C)^2.\dot{F}^2 = \det(M_{q'}).\dot{F}^2 = d(q')$. Ou seja, $d(q)$ é um invariante da classe de isometria de q.

Sejam $(V_1, q_1), (V_2, q_2)$ espaços quadráticos. Como visto o determinante de uma forma quadrática independe da base dada para expressá-la. Com isto, se M_1 é a

matriz de q_1 na base $\mathcal{B}_1$ de V_1 e M_2 é a matriz de q_2 na base $\mathcal{B}_2$ de V_2, então a soma ortogonal $q_1 \perp q_2$ tem determinante igual a $d(q_1 \perp q_2) = \det \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} = \det(M_1).\det(M_2).\dot{F}^2$. Se $V \cong \langle d_1, ..., d_n \rangle$ é uma diagonalização de V, então $d(q) = d_1 \cdots d_n \dot{F}^2$.

1.3 Espaços Isotrópicos e Hiperbólicos

Definição 1.25. Seja (V, B) um espaço bilinear. Um vetor não nulo $v \in V$ é chamado *isotrópico* se $B(v, v) = 0$ $(q(v) = 0)$. Se $B(v, v) \neq 0$ diz-se que v é *anisotrópico*. Dizemos que (V, B) é um *espaço isotrópico* se existe um vetor isotrópico em V. Caso contrário, se diz que (V, B) é um *espaço anisotrópico*. Finalmente, dizemos que (V, B) é um espaço *totalmente isotrópico* se todo vetor v não nulo de V é isotrópico, isto é, $B \equiv 0$.

O próximo teorema caracteriza um tipo especial de espaço quadrático bidimensional.

Teorema 1.26. *Seja (V, q) um espaço quadrático bidimensional. As afirmações seguintes são equivalentes:*

(1) *(V, q) é regular e isotrópico;*

(2) *(V, q) é regular, com $d(q) = -1\dot{F}^2$;*

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

Demonstração: (1) $\Rightarrow$ (2) Seja $\{x_1, x_2\}$ uma base ortogonal de V. Pela regularidade de V, temos $q(x_i) = d_i \neq 0$, $i = 1, 2$. Seja $ax_1 + bx_2$ um vetor isotrópico de V. Suponhamos, sem perda de generalidade, que $a \neq 0$. Logo, $0 = q(ax_1 + bx_2) = a^2 q(x_1) + b^2 q(x_2) = a^2 d_1 + b^2 d_2$. Segue que $d_1 = \frac{-b^2 d_2}{a^2}$. Como $d(q_B) = d_1 d_2 . \dot{F}^2$, temos $d(q_B) = -(\frac{b}{a})^2 d_2 d_2 \dot{F}^2 = -(\frac{b}{a})^2 {d_2}^2 \dot{F}^2 = -1\dot{F}^2$.

(2) $\Rightarrow$ **(3)** Novamente, consideremos $\{x_1, x_2\}$ uma base ortogonal de V e $q(x_i) = d_i \neq 0$, $i = 1, 2$. Assim, $q \cong \langle d_1, d_2 \rangle$. Como $d(q) = -1\dot{F}^2$, temos $d_1 d_2 = -1.\dot{F}^2$. Logo $d_2 \equiv -d_1 (\text{mod } F^2)$. Ou seja, $q \cong \langle d_1, -d_1 \rangle$, com $d_1 \in \dot{F}$.

Considere agora o espaço quadrático (V, q') com $q'(x, y) = d_1 xy$ e $\sigma : V \to V$ definida por $\sigma(x, y) = (x-y, x+y)$. É fácil ver que σ é um isomorfismo e que $q' \circ \sigma = \langle -d_1, d_1 \rangle$. Ou seja, $q' \cong q$. Claramente q' é universal. Pela isometria, q também é universal. Em particular, (V, q) representa 1. Pelo Critério da Representação 1.20, temos que $q \cong \langle 1, c \rangle$. Como $d(q) = -1\dot{F}^2$, temos $c \equiv -1 (\text{mod } \dot{F}^2)$, ou seja, $q \cong \langle 1, -1 \rangle$.

(3) $\Rightarrow$ **(1)** Como $\langle 1, -1 \rangle$ é isotrópica e regular, q também é. $\square$

Definição 1.27. A classe de isometrias de um espaço bidimensional satisfazendo as condições do teorema anterior é dito *plano hiperbólico*. O plano hiperbólico será denotado por $\mathbb{H}$. Observe que $\mathbb{H} \cong \langle 1, -1 \rangle$. Uma soma ortogonal de planos hiperbólicos é chamado *espaço hiperbólico*.

Teorema 1.28. *Seja (V, B) um espaço bilinear regular. Então*

(1) *Todo espaço totalmente isotrópico, $U \subseteq V$, de dimensão r, está contido em um subespaço hiperbólico $T \subseteq V$ de dimensão $2r$;*

(2) *V é isotrópico se, e somente se, V contém um plano hiperbólico (como um somando ortogonal);*

(3) *Se V é isotrópico, então V é universal.*

Demonstração: Provemos **(1)** $\Rightarrow$ **(2)** $\Rightarrow$ **(3)** e depois provemos **(1)**.

(1) $\Rightarrow$ **(2)** Seja $v \in V$ um vetor isotrópico. Logo $U = Fv$ é um espaço totalmente isotrópico. Por **(1)** existe um subespaço hiperbólico $T \subseteq V$ de dimensão 2, ou seja, V contém um plano hiperbólico. Reciprocamente, se V contém um plano hiperbólico, então pelo teorema anterior V possui um vetor isotrópico.

(2) $\Rightarrow$ **(3)** Sendo V isotrópico, temos pela hipótese **(2)** que V contém um plano hiperbólico. Como o plano hiperbólico é universal, então V é universal.

(1) Provemos por indução sobre r. Seja $\{x_1, ..., x_r\}$ uma base de U e seja S o espaço gerado por $x_2, ..., x_r$. É claro que $U^\perp \subseteq S^\perp$.

Como V é regular, podemos usar a Proposição 1.14, então $\dim S^\perp = \dim V - \dim S > \dim V - \dim U = \dim U^\perp$. Isto significa que existe um vetor y_1, que é ortogonal a $x_2, ..., x_r$, mas não é ortogonal a x_1. Pelo Corolário 1.21 e pelo fato que V é regular podemos supor que $q(y_1) \neq 0$. Em particular, $\{x_1, y_1\}$ é linearmente independente. De fato, suponha $ax_1 + by_1 = 0$, com $a, b \in F$. Assim $0 = q(ax_1 + by_1) = a^2q(x_1) + b^2q(y_1)$. Como U é totalmente isotrópico, temos $q(x_1) = 0$. Logo $b^2q(y_1) = 0$. Segue que $b = 0$ e assim $a = 0$, pois $x_1 \neq 0$.

O subespaço $H_1 = Fx_1 + Fy_1$ tem determinante

$$d(H_1) = \begin{pmatrix} 0 & B(x_1, y_1) \\ B(x_1, y_1) & B(y_1, y_1) \end{pmatrix} .\dot{F}^2 = -1\dot{F}^2,$$

então $H_1 \cong \mathbb{H}$ pelo Teorema 1.26. E assim $V = \mathbb{H} \perp V'$, onde $V' = {H_1}^\perp$. Como V' é regular e contém x_2, ..., x_r, então V' contém um subespaço totalmente isotrópico U' de dimensão $r - 1$. Por indução $U' \subseteq T'$, onde T' é um subespaço hiperbólico de V' de dimensão $2(r - 1) = 2r - 2$. Como $\{x_1, ..., x_r\}$ é uma base de U, podemos concluir que U está contido no espaço hiperbólico $\mathbb{H} \perp T'$ de dimensão $2r$. $\square$

Corolário 1.29. *(**Primeiro Teorema da Representação**) Seja q uma forma quadrática regular e $d \in \dot{F}$. Então $d \in D(q)$ se, e somente se, $q \perp \langle -d \rangle$ é isotrópica.*

Demonstração: Se existe $v \in V$ tal que $q(v) = d$, então $q(v) - d = 0$, assim a forma $q \perp \langle -d \rangle$ é isotrópica.

Reciprocamente, seja $v \oplus w$ um vetor isotrópico de $q \perp \langle -d \rangle$, então $q(v) - da^2 = 0$, ou seja, $q(v) = da^2$. Se $a \neq 0$, basta tomar $u = \frac{1}{a}v$ e teremos que $q(u) = \frac{1}{a^2}q(v) = d \in D(q)$. Se $a = 0$, então v é um vetor isotrópico para q. Pelo Teorema 1.28(3), temos que $D(q) = \dot{F}$. Portanto $d \in D(q)$. $\square$

Corolário 1.30. *Para r um inteiro positivo, as afirmações são equivalentes:*

(1) *Qualquer forma quadrática regular de dimensão r é universal;*

(2) *Qualquer forma quadrática de dimensão $r+1$ é isotrópica.*

Demonstração: Segue imediatamente do corolário anterior. □

1.4 Teorema do Cancelamento de Witt e Teorema da Decomposição

Para provarmos o Teorema do Cancelamento de Witt precisamos primeiro da noção de reflexões.

Definição 1.31. Seja V um espaço vetorial não nulo. Um *hiperplano* de V é um subespaço próprio W tal que se W' for um subespaço de V satisfazendo $W \subseteq W' \subseteq V$, então $W = W'$ ou $W' = V$.

Lema 1.32. *Seja (V, B) um espaço bilinear, $x \in V$ um vetor anisotrópico e $W = (Fx)^{\perp}$. Defina $\tau_x : V \to V$ por $\tau_x(y) = y - 2\frac{B(x,y)}{q(x)}x$, para todo $y \in V$. Então,*

(1) *$\tau_x(x) = -x$ e $\tau_x|_W = id_W$;*

(2) *τ_x é uma isometria de (V, B);*

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

Demonstração: **(1)** Se aplicarmos τ_x em x temos

$$\tau_x(x) = x - 2\frac{B(x,x)}{q(x)}x = x - 2x = -x.$$

Se $y \in (Fx)^{\perp}$, então $B(x, y) = 0$ e $\tau_x(y) = y$. Portanto, $\tau|_W = id_W$.

(2) τ_x é um endomorfismo. De fato, considere $x_1, x_2 \in V$ e $\lambda \in F$, segue que

$$\tau_x(x_1 + \lambda\, x_2) \;=\; (x_1 + \lambda\, x_2) - 2\frac{B(x, x_1 + \lambda\, x_2)}{q(x)}x$$

$$
\begin{aligned}
&= x_1 + \lambda\, x_2 - 2\frac{B(x,x_1)}{q(x)}x - 2\lambda\,\frac{B(x,x_2)}{q(x)}x \\
&= x_1 - 2\frac{B(x,x_1)}{q(x)}x + \lambda\,(x_2 - 2\frac{B(x,x_2)}{q(x)}x) \\
&= \tau_x(x_1) + \lambda\,\tau_x(x_2).
\end{aligned}
$$

Pode-se mostrar que τ_x é um isomorfismo. Ainda

$$
\begin{aligned}
B(\tau_x(x_1),\tau_x(x_2)) &= B(x_1 - 2\frac{B(x,x_1)}{q(x)}x, x_2 - 2\frac{B(x,x_2)}{q(x)}x) \\
&= B(x_1,x_2) + \frac{4B(x_1,x)B(x_2,x)B(x,x)}{q(x)^2} - \frac{4B(x_1,x)B(x_2,x)}{q(x)} \\
&= B(x_1,x_2).
\end{aligned}
$$

Portanto τ_x é uma isometria.

(3) Seja $\{e_2,...,e_n\}$ uma base de W onde tomemos $e_1 = x$ e teremos que $e_1, e_2, ..., e_n$ é uma base para V. A matriz de τ_x com relação a esta base é

$$
\begin{pmatrix}
-1 & 0 & \dots & 0 \\
0 & 1 & \dots & 0 \\
\vdots & & \ddots & \vdots \\
0 & 0 & \dots & 1
\end{pmatrix}.
$$

Portanto, $\det(\tau_x) = -1$. $\square$

Definição 1.33. A aplicação τ_x como descrita no lema anterior é chamada *reflexão ortogonal à x segundo o hiperplano W.*

Lema 1.34. *Sejam (V,B) um espaço bilinear e $x, y \in V$ tais que $q(x) = q(y) \neq 0$. Então existe uma isometria $\tau : V \to V$ tal que $\tau(x) = y$.*

Demonstração: Inicialmente vamos mostrar que podemos assumir que $x - y$ é anisotrópico. Pela lei do paralelogramo, temos $q(x+y) + q(x-y) = 2q(x) + 2q(y) = 4q(x) \neq 0$. Assim, $q(x+y)$ e $q(x-y)$ não são simultaneamente nulos. Podemos assumir que $q(x-y) \neq 0$ (se necessário trocamos y por $-y$, pois se acharmos uma isometria τ tal que $\tau(x) = -y$, basta tomar $-\tau$).

Como $q(x-y) \neq 0$, podemos considerar a reflexão segundo o hiperplano $(F(x-y))^{\perp} = W$. Aplicando a reflexão τ_{x-y} à x temos

$$\tau_{x-y}(x) = x - 2\frac{B(x, x-y)}{q(x-y)}(x-y).$$

Mas $q(x-y) = 2B(x, x-y)$, logo $\tau_{x-y}(x) = x - (x-y) = y$. $\square$

Teorema 1.35. *(**Teorema do Cancelamento de Witt**) Sejam q, q_1, q_2 formas quadráticas arbitrárias. Se $q \perp q_1 \cong q \perp q_2$, então $q_1 \cong q_2$.*

Demonstração: Passo 1: O teorema é verdadeiro se q é totalmente isotrópica e q_1 regular. De fato, sejam M_1, M_2 as matrizes simétricas associadas a q_1, q_2, respectivamente. Por hipótese temos $\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix}$ congruente à $\begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$, isto é, existe uma matriz em blocos $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_n(F)$ tal que

$$\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^t \cdot \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} C^t M_2 C & C^t M_2 D \\ D^t M_2 C & D^t M_2 D \end{pmatrix}$$

Em particular, $M_1 = D^t M_2 D$. Como M_1 é não singular, D é não singular e assim M_1 é congruente a M_2. Portanto, $q_1 \cong q_2$.

Passo 2: O teorema é válido se q é totalmente isotrópica. De fato, diagonalizemos q_1, q_2 e vamos assumir que q_1 tem exatamente r zeros na diagonalização e que q_2 tem r zeros ou mais.

Assim, $q \perp r\langle 0\rangle \perp {q_1}' \cong q \perp r\langle 0\rangle \perp {q_2}'$. Como $q \perp r\langle 0\rangle$ é totalmente isotrópica e ${q_1}'$ é regular, temos pelo passo 1 que ${q_1}' \cong {q_2}'$. Por fim, adicionando os r termos de $\langle 0\rangle$, obtemos $q_1 \cong r\langle 0\rangle \perp {q_1}' \cong r\langle 0\rangle \perp {q_2}' \cong q_2$.

Passo 3: Seja q uma forma quadrática e $\langle a_1, ..., a_n\rangle$ uma diagonalização de q. Vamos provar por indução sobre n.

Para $n = 1$, $\langle a_1\rangle \perp q_1 \cong \langle a_1\rangle \perp q_2$. Se $a_1 = 0$ já está provado no passo 2.

Se $a_1 \neq 0$, sejam $(V, q_3) = \langle a_1\rangle \perp q_1$ e $(V', q_4) = \langle a_1\rangle \perp q_2$ e consideremos $\sigma : V \to V'$ tal que $q_3 = q_4 \circ \sigma$. Como $a_1 \in D(q_3) \cap D(q_4)$, existem $z \in V$ e $y \in V'$, tais que

$q_3(z) = a_1 = q_4(y)$. Se $x \in V'$ é tal que $\sigma(z) = x$, então $a_1 = q_3(z) = q_4(\sigma(z)) = q_4(x)$. Segue que $q_4(y) = q_4(x) \neq 0$. Pelo Lema 1.34, existe $\tau : V \to V$ tal que $\tau(x) = y$ $(q_4 \circ \tau = q_4)$. Como $q_3 = q_4 \circ \sigma = q_4 \circ \tau \circ \sigma$, temos

$$q_3(z) = (q_4 \circ \tau \circ \sigma)(z) = q_4((\tau \circ \sigma)(z)) = q_4(y).$$

Logo $(\tau \circ \sigma)|_{(Fz)^\perp} : (Fz)^\perp \to (Fy)^\perp$ é um isomorfismo tal que $q_4|_{(Fy)^\perp}(\tau \circ \sigma)|_{(Fz)^\perp} = q_3|_{(Fz)^\perp}$, ou seja, $q_2 \circ (\tau \circ \sigma) = q_1$. Assim $q_1 \cong q_2$. O restante segue por indução. □

Teorema 1.36. *(**Teorema da Decomposição de Witt**) Um espaço quadrático (V, q) pode ser escrito como soma ortogonal $(V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$, onde V_t é totalmente isotrópico, V_h é hiperbólico (ou zero) e V_a é anisotrópico. E a menos de isometria V_t,V_h e V_a são unicamente determinados.*

Demonstração: (Existência) Seja V_0 um subespaço de V tal que $V = \text{rad } V \oplus V_0$. Então $V_t = \text{rad } V$ é totalmente isotrópico e V_0 é um subespaço regular.

Se V_0 é isotrópico, então pelo Teorema 1.28, temos que $V_0 = H_1 \perp V_1$, onde $H_1 \cong \mathbb{H}$. Se V_1 é isotrópico, então podemos novamente fazer $V_1 \cong H_2 \perp V_2$, onde $H_2 \cong \mathbb{H}$. Após um número finito de passos, obtemos

$$V = V_t \perp H_1 \perp ... \perp H_r \perp V_a, r \geq 0,$$

onde V_a é anisotrópico. Tomando $V_h = H_1 \perp ... \perp H_r$, obtemos o desejado.

(Unicidade) Suponha V com outra decomposição de Witt $V = V_t' \perp V_h' \perp V_a'$. Então V_t' é totalmente isotrópico e $V_h' \perp V_a'$ é regular. Assim, rad V = rad $V_t' \perp$rad $(V_h' \perp V_a') = V_t'$, então $V_t = V_t'$. Pelo Teorema do Cancelamento de Witt 1.35, $V_h \perp V_a \cong V_h' \perp V_a'$.

Tomando $V_h = m\mathbb{H}$ e $V_h' = m'\mathbb{H}$, temos $m\mathbb{H} \perp V_a \cong m'\mathbb{H} \perp V_a'$. Como V_a, V_a' são anisotrópicos, temos $m = m'$. Logo $V_h \cong V_h'$. Novamente pelo Teorema do Cancelamento de Witt, temos que $V_a = V_{a'}$. □

Definição 1.37. O inteiro m $(= \frac{1}{2}\dim V_h)$ unicamente determinado na decomposição de Witt é chamado de *índice de Witt do espaço quadrático* (V, q).

Corolário 1.38. *Se (V, q) é regular, o índice de Witt de V é igual a dimensão de qualquer subespaço totalmente isotrópico maximal de V.*

Demonstração: Seja U um subespaço totalmente isotrópico maximal de V, com $\dim U = r$. Pelo Teorema 1.28(1) U está contido em um espaço hiperbólico T, onde $\dim T = 2r$. Como T é um espaço hiperbólico, temos T regular. Logo $V = T \perp T^{\perp}$ (Corolário 1.22). Observe que $T^{\perp}$ é anisotrópico, pois se existe $0 \neq x \in T^{\perp}$ tal que $B(x, x) = 0$, então $U + Fx$ é um subespaço totalmente isotrópico de V que contém U, o que contradiz a maximalidade de U. Pelo Teorema da Decomposição de Witt 1.35 $T \cong V_h$, mas $m = \frac{1}{2}\dim V_h = \frac{1}{2}(2r) = r = \dim U$. $\square$

Proposição 1.39. *Sejam $q = \langle a, b\rangle$, $q' = \langle c, d\rangle$ formas quadráticas binárias regulares. Então $q \cong q'$ se, e somente se, $d(q) = d(q')$, e q, q' representam um elemento $e \in \dot{F}$ em comum.*

Demonstração: Como $q \cong q'$, sabemos que $M_q = C^t M_{q'} C$, para algum $C \in GL_n(F)$. Então $d(q) = \det\ M_q\, \dot{F}^2 = \det\ C^t . \det\ M_{q'} . \det\ C . \dot{F}^2 = \det\ M_{q'} . \dot{F}^2 = d(q')$. É certo que $a \in D(q)$. Como $q' \cong \langle a\rangle \perp \langle b\rangle$ temos pelo Critério da Representação 1.20 que $a \in D(q')$.

Reciprocamente, assuma que $d(q) = d(q') \in \frac{\dot{F}}{\dot{F}^2}$ e $e \in D(q) \cap D(q')$. Pelo Critério da Representação 1.20, $q \cong \langle e, e'\rangle$, para algum $e' \in \dot{F}$. Calculando o determinante obtemos $d(q) = a.b.\dot{F}^2 = e.e'.\dot{F}^2$. Analogamente, $d(q') = c.d.\dot{F}^2 = e.e''.\dot{F}^2$, para algum $e'' \in \dot{F}$. Segue que $q \cong \langle e, abe\rangle$ e $q' \cong \langle e, cde\rangle$, mas $a.b.\dot{F}^2 = c.d.\dot{F}^2$ e assim, $q \cong q'$. $\square$

1.5 Equivalência por Cadeia

Nesta seção vamos estudar a equivalência por cadeia de formas quadráticas e veremos que é uma outra forma de analisarmos se duas formas são isométricas.

Definição 1.40. Duas formas quadráticas diagonalizadas $q = \langle a_1, ..., a_n \rangle$ e $q_1 = \langle b_1, ..., b_n \rangle$ são de *equivalência simples* se existirem i, j tais que :

(1) $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$;

(2) $a_k = b_k$ sempre que k é diferente de i e j.

Definição 1.41. Dizemos que duas formas quadráticas diagonalizadas q e q' são *equivalentes por cadeia* se existe uma sequência de formas quadráticas diagonalizadas $q_0, ..., q_m$, tais que $q_0 = q$ e $q_m = q'$ e q_i, q_{i+1} são de equivalência simples para $i = 0, ..., m-1$. Notação $q \approx q'$ (q é equivalente por cadeia a q').

Observação 1.42. A equivalência por cadeia é claramente uma relação de equivalência sobre o conjunto de todas formas quadráticas sobre F.

Observe que se $q \approx q'$, então $q \cong q'$. O teorema a seguir mostra que a recíproca deste fato também é verdadeira. Assim, como já dito, poderemos verificar se duas formas são isométricas pela equivalência por cadeia.

Teorema 1.43. *(**Teorema de Equivalência por Cadeia**) Sejam q,q' duas formas quadráticas arbitrárias. Se $q \cong q'$, então $q \approx q'$.*

Demonstração: Sejam $q = \langle a_1, ..., a_n \rangle$ e $q' = \langle b_1, ..., b_n \rangle$. Note que se σ é uma permutação dos índices $\{1, 2, ..., n\}$ e $q^\sigma = \langle a_{\sigma(1)}, ..., a_{\sigma(n)} \rangle$, então $q \approx q^\sigma$, pois o grupo das permutações é gerado por transposições.

Seja $q \cong q'$, então q e q' têm o mesmo número de zeros em suas diagonalizações. Ou seja, é suficiente verificarmos que as partes regulares de q e q' são equivalentes por cadeia. Logo, podemos assumir que q e q' são formas quadráticas regulares.

Façamos por indução sobre n. Se $n = 1, 2$ o resultado é direto, então consideremos $n \geqslant 3$. Dentre todas as formas quadráticas diagonais que são equivalentes por cadeia a q, vamos escolher uma $q_1 = \langle c_1, ..., c_n \rangle$ tal que $\langle c_1, ..., c_p \rangle$ represente b_1, sendo p o menor número natural possível.

Vamos mostrar que $p = 1$. Suponhamos que $b_1 = c_1 e_1^2 + ... + c_p e_p^2$ com $p \geqslant 2$, então para todo $m \geqslant 1$ e $m \leqslant p$, $c_1 e_1^2 + ... + c_m e_m^2 \neq 0$. Pois caso contrário iria contradizer a minimalidade de p. Em particular, $d = c_1 {e_1}^2 + c_2 {e_2}^2 \neq 0$. Pelo Teorema 1.39, $\langle c_1, c_2 \rangle \cong \langle d, c_1 c_2 d \rangle$. Deste modo, $q \approx q_1 = \langle c_1, ..., c_n \rangle \approx \langle d, c_1 c_2 d, c_3, ..., c_p ...., c_n \rangle \approx \langle d, c_3, ..., c_p, ..., c_n, c_1 c_2 d \rangle$ e $b_1 = d + c_3 {e_3}^2 + ... + c_p {e_p}^2$ é representado por $\langle d, c_3, ..., c_p \rangle$ que tem dimensão $p - 1$, contradizendo a escolha de p. Logo, $p = 1$.

Consequentemente $\langle c_1 \rangle = \langle b_1 \rangle$, e assim $q \approx \langle b_1, c_2, ..., c_n \rangle$. Segue que $\langle b_1, c_2, ..., c_n \rangle \cong \langle b_1, ..., b_n \rangle$ e pelo Teorema do Cancelamento de Witt 1.35 $\langle c_2, ..., c_n \rangle \cong \langle b_2, ..., b_n \rangle$. Por hipótese de indução, tem-se $\langle c_2, ..., c_n \rangle \approx \langle b_2, ..., b_n \rangle$. Portanto, $q \approx \langle b_1, c_2, ..., c_n \rangle \approx \langle b_1, ..., b_n \rangle = q'$. $\square$

1.6 Produto de Kronecker de Espaços Quadráticos

Já foi definido soma ortogonal de espaços quadráticos. Agora definiremos produto de espaços quadráticos. Para tanto, vamos utilizar, o produto tensorial entre espaços vetoriais definido no Apêndice.

Definição 1.44. Sejam $(V_1, q_1), (V_2, q_2)$ espaços quadráticos sobre F de dimensão m e n, e $V = V_1 \otimes V_2$, o produto tensorial entre V_1 e V_2. Definimos o *produto tensorial* de q_1 por q_2 como sendo a forma quadrática $q : V \to F$ dada por $q(x_1 \otimes x_2) = q(x_1).q(x_2)$, para todo $x_1 \in V_1$, $x_2 \in V_2$. Observe que a forma bilinear associada ao produto tensorial é $B(x_1 \otimes x_2, y_1 \otimes y_2) = B_1(x_1 \otimes y_1).B_2(x_2 \otimes y_2)$, onde B_i é a forma associada a q_i, $i = 1, 2$. Denotaremos q por $q_1 \otimes q_2$. Note que dim $(q_1 \otimes q_2) =$ dim q_1.dim q_2.

Sejam $\{e_1, ..., e_m\}$ base de V_1, $\{{e_1}', ..., {e_n}'\}$ base de V_2. Assim $A = (a_{ij}) =$

$(B_1(e_i, e_j))$ e $B = (b_{kl}) = (B_2(e'_k, e'_l))$ são as matrizes de q_1 e q_2 nestas bases. No conjunto gerador $\{e_1 \otimes e'_1, e_1 \otimes e'_2, ..., e_1 \otimes e'_n, ..., e_m \otimes e'_1, ..., e_m \otimes e'_n\}$ de V, a matriz de $q_1 \otimes q_2$ é

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

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

Proposição 1.45. (1) $q_1 \otimes q_2 \cong q_2 \otimes q_1$ *(lei comutativa);*

(2) $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$*(lei associativa);*

(3) $q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$*(lei distributiva).*

Demonstração: (1) Seja $\sigma : V = V_1 \otimes V_2 \to V_2 \otimes V_1$ dada por $\sigma(x \otimes y) = y \otimes x$. É fácil mostrar que σ é um isomorfismo. E mais $(q_2 \otimes q_1)(\sigma(x \otimes y)) = (q_2 \otimes q_1)(y \otimes x) = q_2(y).q_1(x) = q_1(x).q_2(y) = (q_1 \otimes q_2)(x \otimes y)$. Portanto, $q_1 \otimes q_2 \cong q_2 \otimes q_1$.

(2) Seja $\sigma : (V_1 \otimes V_2) \otimes V_3 \to V_1 \otimes (V_2 \otimes V_3)$, onde $\sigma((x \otimes y) \otimes z) = x \otimes (y \otimes z)$. É fácil ver que σ é um isomorfismo. E mais $(q_1 \otimes (q_2 \otimes q_3))(\sigma((x \otimes y) \otimes z)) = (q_1 \otimes (q_2 \otimes q_3))(x \otimes (y \otimes z)) = q_1(x) \otimes (q_2 \otimes q_3)(y \otimes z) = q_1(x) \otimes q_2(y) \otimes q_3(z) = (q_1 \otimes q_2)(x \otimes y) \otimes q_3(z) = ((q_1 \otimes q_2) \otimes q_3)((x \otimes y) \otimes z)$. Portanto, $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$.

(3) Seja $\sigma : V \otimes (V_1 \perp V_2) \to (V \otimes V_1) \perp (V \otimes V_2)$ definida por $\sigma(x \otimes (y_1 + y_2)) = (x \otimes y_1) + (x \otimes y_2)$. É fácil ver que σ é um isomorfismo que satisfaz $((q \otimes q_1) \perp (q \otimes q_2))(\sigma x \otimes (y_1 + y_2)) = ((q \otimes q_1) \perp (q \otimes q_2))((x \otimes y_1) + (x \otimes y_2)) = (q \otimes q_1)(x \otimes y_1) + (q \otimes q_2)(x \otimes y_2) = q(x)(q_1 \perp q_2)(y_1 + y_2) = q \otimes (q_1 \perp q_2)(x \otimes (y_1 + y_2))$. Logo $q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$. $\square$

Observação 1.46. (1) Pela lei distributiva tem-se:

$$\langle a_1, ..., a_m \rangle \otimes \langle b_1, ..., b_n \rangle \cong \langle a_1b_1, a_1b_2, ..., a_1b_n, ..., a_mb_1, ..., a_mb_n \rangle;$$

(2) Se q é regular então $q \otimes \mathbb{H} \cong (\dim(q)).\mathbb{H}$;

1.7 Corpos Ordenados e Assinatura

Definição 1.47. Uma *ordem* de um corpo F é um subconjunto P de $\dot{F}$ tendo as seguintes propriedades:

(1) Para $x, y \in P$, temos que $x + y \in P$;

(2) Para $x, y \in P$, temos que $x.y \in P$;

(3) $P \cup (-P) = F^*$, onde $-P = \{-x : x \in P\}$.

Um corpo com uma ordem é chamado um *corpo ordenado*. Os elementos de P são chamados *elementos positivos*, os elementos de $-P$ são chamados *elementos negativos*.

Definição 1.48. Seja X um conjunto qualquer. Uma relação de *ordem parcial* sobre X, que denotaremos por $\prec$, é uma relação que satisfaz:

(1) $x \prec x$ para cada $x \in X$;

(2) $x \prec y$ e $y \prec z$, com $x, y, z \in X$, implica $x \prec z$;

(3) $x \prec y$ e $y \prec x$, com $x, y \in X$, implica $x = y$.

Uma relação de *ordem total* sobre X é uma relação de ordem parcial $\prec$ sobre X com a propriedade adicional que para quaisquer x, y em X se $x \neq y$, então $x \prec y$ ou $y \prec x$.

Uma ordem P em um corpo F define uma relação $>$ de ordem total sobre F da seguinte forma: $x > y \Leftrightarrow (x - y) \in P$. Se $x > y$ também denotamos $y < x$.

Note que P e $-P$ são disjuntos, pois se $x \in P \cap (-P)$, então $-x \in P$ e isto nos leva a contradição $0 = (x - x) \in P$. Portanto nenhum elemento é positivo e negativo.

Se $x \neq 0$, então x ou $-x$ é positivo. Assim, $x^2 = (-x)^2$ é positivo em qualquer um dos casos. Isto mostra que $\dot{F}^2 \subset P$. Portanto, $1 \in P$ e então $1+1, 1+1+1, ... \in P$. Mostrando que um corpo ordenado tem característica 0 (zero).

Definição 1.49. Um corpo F é chamado *formalmente real* se -1 não é soma de quadrados em F.

Observação 1.50. Um corpo ordenado é formalmente real. De fato, -1 não é soma de quadrados em um corpo ordenado, pois se $-1 \in P$, então $1 - 1 = 0 \in P$.

Definição 1.51. Seja F um corpo ordenado. O espaço quadrático (V, q) é chamado *definido positivo* se $q(x) > 0$, para todo $x \neq 0$. E chamado *definido negativo* se $q(x) < 0$, para todo $x \neq 0$. Assim segue da definição que um espaço definido positivo (negativo) é regular.

Exemplo 1.52. Os produtos internos sobre o corpo dos reais são formas bilineares e as formas quadráticas associadas a eles são definidas positivas.

Em geral, um corpo admite muitas ordens diferentes. Claramente a definição de forma quadrática definida positiva e forma quadrática definida negativa depende da ordem considerada no corpo.

O próximo teorema nos mostra que toda forma quadrática sobre um corpo ordenado é uma soma ortogonal de uma forma definida positiva e uma forma definida negativa. Esta decomposição nos permitirá a definição de um novo invariante de formas quadráticas, a assinatura.

Teorema 1.53. *(**Teorema da Inércia de Jacobi e Sylvester**) Seja (V, q) um espaço quadrático sobre um corpo ordenado F. Então $V = V^+ \perp V^-$, onde (V^+, q_{V^+}) é definido positivo e (V^-, q_{V^-}) é definido negativo. A dimensão de V^+ e de V^- são independentes da escolha da decomposição ortogonal.*

Demonstração: Escolha uma base ortogonal $\{e_1, ..., e_n\}$ de V. Reordenando se necessário, podemos assumir que

$$q(e_i) > 0 \text{ para } i = 1, ..., m,$$
$$q(e_i) < 0 \text{ para } i = m+1, ..., n.$$

Sejam $V^+ = Fe_1 + ... + Fe_m$ e $V^- = Fe_{m+1} + ... + Fe_n$. Então $V = V^+ \perp V^-$ e V^+ é definida positiva pois

$$q(\sum_{i=1}^{m} \alpha_i e_i) = \sum_{i=1}^{m} {\alpha_i}^2 q(e_i) > 0.$$

Analogamente, V^- é definida negativa. Mostremos que a dimensão de cada um dos subespaços independe da decomposição escolhida. De fato, seja $V = W^+ \perp W^-$ outra decomposição do mesmo tipo. Então claramente, $W^+ \cap V^- = \{0\}$ e $W^- \cap V^+ = \{0\}$. Assim $W^+ \subseteq V^+$ e $W^- \subseteq V^-$. Consequentemente

$$\dim W^+ \leq \dim V - \dim V^- = \dim V^+$$
$$\dim W^- \leq \dim V - \dim V^+ = \dim V^-.$$

Como $\dim W^+ + \dim W^- = \dim V^+ + \dim V^-$ temos a igualdade. □

Definição 1.54. Seja P uma ordem de F e (V, q) um espaço quadrático sobre F. Definimos $\text{sign}_P\ (q) = \dim(V^+) - \dim(V^-)$. Pelo Teorema 1.53 este invariante está bem definido e é chamado de *assinatura de q*. Os invariantes $i^+(q) = \dim V^+$ e $i^-(q) = \dim V^-$ são chamados de *índice positivo* e *índice negativo*.

Proposição 1.55. *Sejam ϕ e φ duas formas quadráticas, então*

(1) $\text{sign}_P\ (\phi \perp \psi) = \text{sign}_P\ (\phi) + \text{sign}_P\ (\psi)$;

(2) $\text{sign}_P\ (\phi \otimes \psi) = \text{sign}_P\ (\phi).\text{sign}_P\ (\psi)$;

(3) $\text{sign}_P\ (\langle 1 \rangle) = 1$;

(4) $\text{sign}_P\ (\phi) = 0$, *se ϕ é hiperbólico .*

Demonstração: (1) Pelo Teorema 1.53, $\phi = \phi^+ \perp \phi^-$ e $\varphi = \varphi^+ \perp \varphi^-$ com $\phi^+,\ \varphi^+$ definidas positivas e $\phi^-,\ \varphi^-$ definidas negativas. Logo $\phi \perp \varphi = (\phi^+ \perp \varphi^+) \perp (\phi^- \perp \varphi^-)$, onde $\phi^+ \perp \varphi^+$ é definida positiva e $\phi^- \perp \varphi^-$ é definida negativa. Portanto, $\text{sign}_P\ (\phi \perp \varphi) = \dim\ (\phi^+ \perp \varphi^+) - \dim\ (\phi^- \perp \varphi^-) = (\dim\ \phi^+ - \dim\ \phi^-) + (\dim\ \varphi^+ - \dim\ \varphi^-) = sign_P\ (\phi) + \text{sign}_P\ (\varphi)$.

(2) Usando a propriedade distributiva do produto tensorial em relação a soma ortogonal (ver Lema 5.2), temos:

$$\begin{aligned} \phi \otimes \psi &= (\phi^+ \perp \phi^-) \otimes (\psi^+ \perp \psi^-) \\ &= [(\phi^+ \perp \phi^-) \otimes \psi^+] \perp [(\phi^+ \perp \phi^-) \otimes \psi^-] \\ &= [(\phi^+ \otimes \psi^+) \perp (\phi^- \otimes \psi^+)] \perp [(\phi^+ \otimes \psi^-) \perp (\phi^- \otimes \psi^-)]. \end{aligned}$$

De acordo com as observações feitas sobre produto tensorial no Apêndice podemos analisar cada um dos somandos:

- $(\phi^+ \otimes \psi^+)$ é definida positiva com dimensão igual a $\dim\ \phi^+.\dim\ \psi^+$;
- $(\phi^- \otimes \psi^+)$ é definida negativa com dimensão igual a $\dim\ \phi^-.\dim\ \psi^+$;
- $(\phi^+ \otimes \psi^-)$ é definida negativa com dimensão igual a $\dim\ \phi^+.\dim\ \psi^-$;
- $(\phi^- \otimes \psi^-)$ é definida positiva com dimensão igual a $\dim\ \phi^-.\dim\ \psi^-$.

Assim, $(\phi^+ \otimes \varphi^+) \perp (\phi^- \otimes \varphi^-)$ é definida positiva e $(\phi^- \otimes \varphi^+) \perp (\phi^+ \otimes \varphi^-)$ é definida negativa. Segue que

$$\begin{aligned} \text{sign}_P\ (\phi \otimes \psi) &= \dim\ \phi^+.\dim\ \psi^+ + \dim\ \phi^-.\dim\ \psi^- - \dim\ \phi^-.\dim\ \psi^+ - \dim\ \phi^+.\dim\ \psi^- \\ &= \dim\ \phi^+(\dim\ \psi^+ - \dim\ \psi^-) - \dim\ \phi^-(\dim\ \psi^+ - \dim\ \psi^-) \\ &= \dim\ \phi^+(\text{sign}_P\ \psi) - \dim\ \phi^-(\text{sign}_P\ \psi) \\ &= (\dim\ \phi^+ - \dim\ \phi^-)\text{sign}_P\ \psi \\ &= \text{sign}_P\ \phi.\text{sign}_P\ \psi. \end{aligned}$$

(3) Imediata.

(4) Basta tomar a diagonalização de um espaço hiperbólico. □

Capítulo 2

Invariante de Hasse

No capítulo 1 estudamos três invariantes de formas quadráticas, a saber, a dimensão, o determinante e a assinatura. Neste capítulo iremos definir mais um importante invariante de formas quadráticas, conhecido como invariante de Hasse. Para definir este invariante iremos utilizar as álgebras de quatérnios, as quais são um caso particular de álgebras centrais simples.

2.1 Álgebras Centrais Simples e o Grupo de Brauer

Nesta seção iremos definir o Grupo de Brauer, o qual será formado por classes de equivalência de álgebras centrais simples. Iniciamos definindo álgebras centrais simples e explorando suas propriedades.

Definição 2.1. Seja F um corpo. Uma *F-álgebra* (ou uma *álgebra sobre F*) A é um anel tal que

(1) $(A, +)$ é um espaço vetorial de dimensão finita sobre F;

(2) $\lambda(ab) = (\lambda a)b$, para todo $\lambda \in F$ e $a, b \in A$.

Definição 2.2. Seja A uma F-álgebra. Para um subconjunto $S \subset A$, definimos o *centralizador* de S em A por

$$C_A(S) = \{x \in A \mid xs = sx, \text{ para todo } s \in S\}.$$

No caso em que $S = A$, $C_A(A)$ é chamado *centro* de A, e denotamos por $Z(A)$. Mostra-se facilmente que $C_A(S)$ é uma subálgebra de A.

Definição 2.3. (1) Uma F-álgebra A é dita *central* se $Z(A) = F$.

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

(3) Uma F- álgebra A é dita *central simples* se satisfaz **(1)** e **(2)**.

Exemplo 2.4. Para todo F-espaço vetorial V de dimensão n temos que a álgebra dos endomorfismos de V, isto é, $A = \text{End}\ (V) \simeq M_n(F)$, é sempre uma álgebra central simples.

O próximo teorema nos mostra que o produto tensorial é uma operação fechada no conjunto das álgebras centrais simples.

Proposição 2.5. (1) *Se A, B são F-álgebras e $A' \subset A$, $B' \subset B$ F-subálgebras, então $C_{A\otimes B}(A' \otimes B') = C_A(A') \otimes C_B(B')$. Em particular, se A, B são centrais, então $A \otimes B$ é central;*

(2) *Se A é uma álgebra central simples e B é uma álgebra simples, então $A \otimes B$ é simples;*

(3) *Se A, B são ambas álgebras centrais simples, então $A \otimes B$ também é.*

Demonstração: (1) Temos que $C_A(A') \otimes C_B(B') \subset C_{A\otimes B}(A' \otimes B')$. De fato, se $x \otimes y \in C_A(A') \otimes C_B(B')$, então $ax \otimes by = xa \otimes yb$, para todo $a \in A'$ e para todo $b \in B'$. Pelas propriedades de produto tensorial temos que $(a \otimes b)(x \otimes y) = (ax \otimes by) = (xa \otimes yb) = (x \otimes y)(a \otimes b)$. Logo $x \otimes y \subset C_{A\otimes B}(A' \otimes B')$. Portanto $C_A(A') \otimes C_B(B') \subset C_{A\otimes B}(A' \otimes B')$.

Por outro lado, seja $\{b_1, ..., b_n\}$ uma F-base de B e tome $x \in C_{A\otimes B}(A' \otimes B')$. Assim, $x = x_1 \otimes b_1 + ... + x_n \otimes b_n$, onde $x_i \in A$ são unicamente determinados. Para todo $a \in A'$, temos que $(a \otimes 1)x = x(a \otimes 1)$, logo

$$(ax_1) \otimes b_1 + ... + (ax_n) \otimes b_n = (x_1a) \otimes b_1 + ... + (x_na) \otimes b_n.$$

Pela unicidade da representação, temos que $x_i \in C_A(A')$.

Agora considere $\{a_1, ..., a_k\}$ uma F-base de A. Assim, $x = a_1 \otimes y_1 + ... + a_k \otimes y_k$, onde $y_i \in B$ são unicamente determinados. Logo, para todo $b \in B'$, temos que $(1 \otimes b)x = x(1 \otimes b)$, ou seja,

$$a_1 \otimes (by_1) + ... + a_k \otimes (by_k) = a_1 \otimes (y_1b) + ... + a_k \otimes (y_kb).$$

Novamente $y_i \in C_B(B')$, pela unicidade da representação. Portanto $x \in C_A(A') \otimes C_B(B')$.

(2) Seja I um ideal bilateral não nulo de $A \otimes B$. Mostremos que $I = A \otimes B$. Vamos assumir que I contém um elemento $a \otimes b \neq 0$. O ideal bilateral de A gerado por a é A, já que A é central simples. Assim existem a_i's, a_i''s elementos de A tais que $\sum a_i a a_i' = 1$. Ou seja, $\sum (a_i \otimes 1)(a \otimes b)(a_i' \otimes 1) = 1 \otimes b \in I$. Repetindo o mesmo argumento à b temos que $1 \otimes 1 \in I$. Assim, neste primeiro caso $A \otimes B$ é simples.

Mais geralmente, vamos tomar $x \in I$ e uma representação $x = a_1 \otimes b_1 + ... + a_k \otimes b_k$, $a_i \in A$ e $b_i \in B$ tal que k é o menor possível. Como A é central simples podemos assumir sem perda de generalidade que $a_k = 1$.

Queremos mostrar que $k = 1$. Suponha, por absurdo, que $k > 1$. Então a_{k-1} e a_k são linearmente independentes, pois caso contrário $a_{k-1} = \lambda a_k$ e $a_{k-1} \otimes b_{k-1} + a_k \otimes b_k = a_k \otimes (\lambda b_{k-1} + b_k)$, acabando por tomar uma representação para x com k menor. Como A é central podemos considerar sem perda de generalidade que $a_{k-1} \notin Z(A)$. Assim, existe $a \in A$ tal que $aa_{k-1} - a_{k-1}a \neq 0$.

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

(3) É imediato de **(1)** e de **(2)**. □

Iremos definir agora uma relação de equivalência entre as álgebras centrais simples e em seguida mostrar que o conjunto das classes de equivalência forma um grupo.

Definição 2.6. Duas álgebras centrais simples A e A' são chamadas *similares* se existem espaços vetoriais V e V' de dimensões finitas sobre F tais que

$$A \otimes \text{End } (V) \simeq A' \otimes \text{End } (V')$$

como F-álgebras, onde $End\ (V)$ é a álgebra dos endomorfismos do espaço vetorial V. Denotaremos $A \sim A'$.

Proposição 2.7. *A relação de similaridade é uma relação de equivalência.*

Demonstração: Claramente temos que $A \sim A$ e se $A \sim B$, então $B \sim A$. Resta mostrar a transitividade. Para tanto iremos usar o fato de End $(V_1) \otimes$ End $(V_2) \simeq$ End $(V_1 \otimes V_2)$. Suponhamos que $A \sim B$ e $B \sim C$, logo existem espaços vetoriais V_1, V_2, V_3, V_4 sobre F tais que $A \otimes \text{End } (V_1) \simeq B \otimes \text{End } (V_2)$ e $B \otimes \text{End } (V_3) \simeq C \otimes \text{End } (V_4)$. Assim

$$\begin{aligned}
A \otimes \text{End } (V_1 \otimes V_3) &\simeq A \otimes (\text{End } (V_1) \otimes \text{End } (V_3)) \\
&\simeq (A \otimes \text{End } (V_1)) \otimes \text{End } (V_3) \\
&\simeq (B \otimes \text{End } (V_2)) \otimes \text{End } (V_3) \\
&\simeq B \otimes \text{End } (V_2 \otimes V_3) \\
&\simeq B \otimes (\text{End } (V_3) \otimes \text{End } (V_2)) \\
&\simeq (C \otimes \text{End } (V_4)) \otimes \text{End } (V_2) \\
&\simeq C \otimes \text{End } (V_4 \otimes V_2).
\end{aligned}$$

Logo $A \sim C$. Portanto similaridade é uma relação de equivalência. □

Notações: A classe de equivalência da álgebra central simples A será denotada por $[A]$ e o conjunto das classes de similaridade de álgebras centrais simples será denotado por $Br(F)$.

Observação 2.8. A operação $Br(F) \times Br(F) \to Br(F)$ dada por $[A_1].[A_2] = [A_1 \otimes A_2]$ está bem definida. De fato, sejam A_1, A'_1, A_2, A'_2 álgebras centrais simples tais que $A_1 \sim A'_1$ e $A_2 \sim A'_2$. Assim,

$$\begin{aligned} A_1 \otimes \text{End } (V_1) &\simeq A'_1 \otimes \text{End } (V'_1) \\ A_2 \otimes \text{End } (V_2) &\simeq A'_2 \otimes \text{End } (V'_2). \end{aligned}$$

Logo, $(A_1 \otimes \text{End } (V_1)) \otimes (A_2 \otimes \text{End } (V_2)) \simeq (A'_1 \otimes \text{End } (V'_1)) \otimes (A'_2 \otimes \text{End } (V'_2))$. Portanto, $(A_1 \otimes A_2) \otimes \text{End}\,(V_1 \otimes V_2) \simeq (A'_1 \otimes A'_2) \otimes \text{End}\,(V'_1 \otimes V'_2)$, isto é, $[A_1 \otimes A_2] = [A'_1 \otimes A'_2]$.

E ainda, como $A_1 \otimes (A_2 \otimes A_3) \simeq (A_1 \otimes A_2) \otimes A_3$ e $A_1 \otimes A_2 \simeq A_2 \otimes A_1$, o produto entre as classes é associativo e comutativo.

O elemento identidade deste produto é a classe $[M_n(F)] = [F]$, pois $[A].[M_n(F)] = [A \otimes M_n(F)] = [A]$, para qualquer álgebra central simples A.

Como já dito, estamos construindo uma estrutura de grupo, e para isso definiremos a álgebra oposta com a intenção de exibirmos um simétrico para cada elemento de $Br(F)$.

Definição 2.9. Seja A uma F-álgebra. A *álgebra oposta* de A, denotada por A^{op}, é a F-álgebra tal que como conjunto $A^{op} = A$, a multiplicação de A^{op} é dada por $a \odot b = ba$ e as outras operações permanecem as mesmas de A. Observe que $A^{op} = A$ como grupo abeliano aditivo.

Proposição 2.10. *Se A é uma F- álgebra central simples, então A^{op} também é.*

Demonstração: Primeiramente mostremos que $Z(A) = Z(A^{op})$. De fato, seja $a \in Z(A^{op})$, então $a \odot b = b \odot a$, para todo $b \in Z(A^{op})$. Por definição de álgebra oposta temos que $a \odot b = ba$ e da mesma forma $b \odot a = ab$, ou seja, $ba = ab$. Então, $a \in Z(A)$. Logo $Z(A^{op}) \subset Z(A)$. E analogamente, concluímos que $Z(A) \subset Z(A^{op})$. Portanto se A é central, temos A^{op} é central.

Se I é um ideal de A^{op}, então $\{a \in A \mid a^{op} \in I\}$ é um ideal de A. Portanto, se A é simples, temos A^{op} simples. $\square$

Teorema 2.11. *Seja A uma álgebra central simples. Então $A \otimes A^{op} \simeq End\ A$.*

Em particular, $Br(F)$ é um grupo multiplicativo, com $[A]^{-1} = [A^{op}]$.

Demonstração: Provemos que $A \otimes A^{op} \simeq End\ (A)$, onde A é considerado como um F-espaço vetorial. Vamos definir uma aplicação $\psi : A \times A^{op} \to \text{End } A$, dada por $\psi(a,b)(x) = axb$, para todo $x \in A$. É fácil mostrar que $\psi(a,b) \in \text{End } (A)$. Note que $\psi(a+b,c)(x) = (a+b)xc = axc + bxc = \psi(a,c)(x) + \psi(b,c)(x)$, para todo $x \in A$. Analogamente $\psi(a,b+c)(x) = \psi(a,b) + \psi(a,c)(x)$, para todo $x \in A$. Mais ainda, $\psi(\alpha a, b) = \psi(a, \alpha b)$, para todo $\alpha \in F$, pois $\psi(\alpha a, b)(x) = \alpha axb = ax\alpha b = \psi(a, \alpha b)(x)$, para todo $x \in A$. Assim ψ é uma aplicação linear mediana (ver Definição 5.4) e pela propriedade universal do produto tensorial (ver Teorema 5.5) existe uma única transformação linear $\psi : A \otimes A^{op} \to \text{End } (A)$.

Agora temos que ψ também é multiplicativa, pois

$\psi(ac, b \odot d)(x) = ac(x)b \odot d = a(cxd)b = \psi(a,b)(cxd) = \psi(a,b)(\psi(c,d)(x))$.

Assim, existe um homomorfismo de F-álgebras $\varphi : A \otimes A^{op} \to \text{End } A$. Como $\text{Ker}\,\varphi$ é um ideal de $A \otimes A^{op}$ e $A \otimes A^{op}$ é uma álgebra simples, segue que φ é injetivo. Como as dimensões de $A \otimes A^{op}$ e de End A coincidem, φ é sobrejetora. Portanto, $A \otimes A^{op} \simeq \text{End } A$. $\square$

Definição 2.12. O grupo $B_r(F)$ das classes de similaridade de álgebras centrais simples é chamado *Grupo de Brauer de F*.

Definição 2.13. Uma álgebra A é dita *álgebra com divisão* se todo elemento não nulo de A é inversível.

Proposição 2.14. *Seja F um corpo. Os elementos de $Br(F)$ estão em correspondência 1 a 1 com as classes de isomorfismos das F-álgebras centrais com divisão.*

Demonstração: Dado $[A] \in Br(F)$, pelo Teorema de Wedderburn (veja [10], Cap.8, Cor. 1.6), A é isomorfa a $M_n(D)$, onde D é uma F-álgebra central com divisão. Assim, $A \simeq M_n(D) \simeq D \otimes M_n(F)$, o que implica que $[A] = [D]$ em $Br(F)$. Ainda pelo teorema de Wedderburn temos que A é unicamente determinada por D. Dessa forma, se D e D' são álgebras centrais simples com divisão e $[D] = [D']$ em $Br(F)$, ou seja, existem $m, n \in \mathbb{N}$ tais $M_n(D) \simeq M_m(D')$. Portanto $D \simeq D'$ e $n = m$ (veja [10], Cap.8, Teo. 1.9). $\square$

2.2 Álgebras de Quatérnios

Nosso objetivo nesta seção é estudar as álgebras de quatérnios, pois é através delas que iremos definir o invariante de Hasse.

Definição 2.15. Sejam $a, b \in \dot{F}$, F um corpo. Definimos a *álgebra de quatérnios* $A = (\frac{a,b}{F})$ sendo a F-álgebra gerada por i, j, que satisfazem as seguintes relações $i^2 = a$, $j^2 = b$ e $ij = -ji = k$.

Observação 2.16. Seja $A = (\frac{a,b}{F})$ definida como acima.

(1) A quando considerado como espaço vetorial sobre F tem como base $\{1, i, j, k\}$.

(2) O quadrado de k também é um escalar em F. De fato, $k^2 = (ij)(ij) = i(ji)j = i(-ij)j = -i^2j^2 = -ab \in \dot{F}$.

(3) Os elementos $\{i, j, k\}$ são anticomutativos. Basta observar que $ij = -ji$, $ik = i\,ij = -iji = -ki$ e $jk = jij = -ijj = -kj$.

(4) Se considerarmos $F = \mathbb{R}$ e $a = b = -1$, então $(\frac{-1,-1}{\mathbb{R}})$ é o usual anel dos quatérnios.

Proposição 2.17. *A construção da álgebra de quatérnios é simétrica em relação aos escalares a e b, isto é,* $A = (\frac{a,b}{F}) \simeq (\frac{b,a}{F}) = A'$.

Demonstração: Sejam $i', j', k' \in A'$ tais que $i'^2 = b$, $j'^2 = a$, $-i'j' = j'i' = k'$. Defina $\varphi : A \to A'$ por $\varphi(1) = 1$, $\varphi(i) = j'$, $\varphi(j) = i'$ e $\varphi(k) = k'$ e estenda por linearidade. É fácil ver que φ é um homomorfismo de espaços vetoriais. Mais ainda, $\varphi(x\,y) = \varphi(x)\ \varphi(y)$. De fato, dados $x = \alpha+\beta i+\gamma j+\delta k$, $y = \alpha_1+\beta_1 i+\gamma_1 j+\delta_1 k \in A$, temos que $\varphi(xy) = \varphi(\alpha\alpha_1 + \alpha\beta_1 i + \alpha\gamma_1 j + \alpha\delta_1 k + \beta\alpha_1 i + \beta\beta_1 a + \beta\gamma_1 k + \beta\delta_1 aj + \gamma\alpha_1 j - \gamma\beta_1 k + \gamma\gamma_1 b - \gamma\delta_1 bi + \delta k\alpha_1 - \delta\beta_1 bi + \delta\gamma_1 bi - \delta\delta_1 ab)$. Pela linearidade de φ obtemos $\varphi(xy) = (\alpha\alpha_1 + \beta\beta_1 a + \gamma\gamma_1 b - \delta\delta_1 ab)\varphi(1) + (\alpha\beta_1 + \beta\alpha_1 - \gamma\delta_1 b + \delta\delta_1 b)\varphi(i) + (\alpha\gamma_1 + \beta\delta_1 a + \gamma\alpha_1)\varphi(j) + (\alpha\delta_1 + \beta\gamma_1 - \gamma\beta_1 + \delta\alpha_1)\varphi(k)$. Usando os valores de φ na base de A, temos que $\varphi(xy) = (\alpha\alpha_1 + \beta\beta_1 a + \gamma\gamma_1 b - \delta\delta_1 ab) + (\alpha\beta_1 + \beta\alpha_1 - \gamma\delta_1 b + \delta\delta_1 b)j' + (\alpha\gamma_1 + \beta\delta_1 a + \gamma\alpha_1)i' + (\alpha\delta_1 + \beta\gamma_1 - \gamma\beta_1 + \delta\alpha_1)k'$. Mas por outro lado, $\varphi(x).\varphi(y) = (\alpha\alpha_1 + \beta\beta_1 a + \gamma\gamma_1 b - \delta\delta_1 ab) + (\alpha\beta_1 + \beta\alpha_1 - \gamma\delta_1 b + \delta\delta_1 b)j' + (\alpha\gamma_1 + \beta\delta_1 a + \gamma\alpha_1)i' + (\alpha\delta_1 + \beta\gamma_1 - \gamma\beta_1 + \delta\alpha_1)k'$. Portanto temos um isomorfismo de F-álgebras. □

Proposição 2.18. (1) $(\frac{a,b}{F}) \simeq (\frac{ax^2,by^2}{F})$, *para todos* $a, b, x, y \in \dot{F}$;

(2) *O centro de* $(\frac{a,b}{F})$ *é* F, *para quaisquer* $a, b \in \dot{F}$;

(3) $(\frac{a,b}{F})$ *é uma álgebra simples, para todos* $a, b \in F$;

(4) $(\frac{1,-1}{F}) \simeq M_2(F)$, *a álgebra de matrizes* 2×2 *sobre* F.

Demonstração: (1) Seja $A = (\frac{a,b}{F})$, com base $\{1, i, j, k\}$ tal que $i^2 = a$, $j^2 = b$ e $ij = -ji = k$, e $A' = (\frac{ax^2,by^2}{F})$ com base $\{1, i', j', k'\}$ tal que $i'^2 = ax^2$ e $j'^2 = by^2$. Observe que

$$\begin{aligned} i'^2 &= ax^2 = x^2 i^2 = (xi)^2 \\ j'^2 &= by^2 = y^2 j^2 = (yj)^2 \\ k'^2 &= i'^2 j'^2 = abx^2 y^2 \\ (xi)(yj) &= (xy)(ij) = (xy)(-ji) = -(yj)(xi), \end{aligned}$$

logo $xi, yj \in A'$ e podemos definir $\varphi : A \to A'$ por $\varphi(i) = xi$, $\varphi(j) = yj$ e consequentemente $\varphi(k) = xyk = xiyj \in A'$. Estendendo por linearidade, temos um

isomorfismo de espaços vetoriais sobre F, pois $\dim A = \dim A'$. É fácil ver que $\varphi(x.y) = \varphi(x).\varphi(y)$, para todos $x, y \in A$. Portanto φ é um isomorfismo de álgebras sobre F.

(2) Seja $x = \alpha + \beta i + \gamma j + \delta k \in Z(A)$. Em particular $xi = ix$. Ou seja, $(\alpha+\beta i+\gamma j+\delta k)i = i(\alpha+\beta i+\gamma j+\delta k)$. Assim, $\alpha i+\beta a-\gamma k-\delta ja = \alpha i+\beta a+\gamma k+\delta ja$. O que nos fornece $2\gamma k + 2a\delta j = 0$. Como k, j são linearmente independente segue que $\gamma = \delta = 0$. Logo $x = \alpha + \beta i$. Usando agora que $xj = jx$. Ou seja, $(\alpha + \beta i)j = j(\alpha + \beta i)$. Temos $\alpha j + \beta k = j\alpha - \beta k$. Resultando em $2\beta k = 0$, ou seja, $\beta = 0$. Portanto, $x = \alpha \in F$, ou seja, $Z(A) = F$.

(3) Seja $J \subseteq A$ um ideal bilateral. Consideremos $J \neq \{0\}$ e $0 \neq x = \alpha + \beta i + \gamma j + \delta k \in J$. Suponhamos sem perda de generalidade que $\gamma \neq 0$. Como $xi, ix \in J$, temos que $y = xi - ix \in J$. Fazendo os cálculos obtemos que $y = -2a\delta j - 2\gamma k \in J$. Agora de $yj - jy \in J$, temos que $-4b\gamma i \in J$. Assim $-4b\gamma i.i = -4ab\gamma \in J$. Como $-4ab\gamma \neq 0 \in F$, segue que existe $\rho \in F$ tal que $-4ab\gamma\rho = 1$, ou seja, $1 \in J$. Portanto $A = J$.

(4) Sejam $i_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $j_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(F)$. É fácil ver que ${i_0}^2 = -Id$, ${j_0}^2 = Id$ e $i_0 j_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -j_0 i_0$. Assim existe um homomorfismo de álgebras $\varphi : (\frac{-1,1}{F}) \to M_2(F)$, onde $\varphi(1) = Id$, $\varphi(i) = i_0$, $\varphi(j) = j_0$, $\varphi(k) = i_0 j_0$. Como $\{Id, i_0, j_0, i_0 j_0\}$ é uma base para $M_2(F)$ temos um isomorfismo entre os F-espaços vetoriais $(\frac{-1,1}{F})$ e $M_2(F)$. É fácil ver que $\varphi(xy) = \varphi(x)\varphi(y)$, para todo $x, y \in (\frac{-1,1}{F})$. Logo φ é um isomorfismo de álgebras sobre F. □

Definição 2.19. Um elemento $x = \alpha+\beta i+\gamma j+\delta k \in A = (\frac{a,b}{F})$ é chamado *quatérnio puro* se $\alpha = 0$. O conjunto dos quatérnios puros será denotado por A_0.

O teorema abaixo mostra que o subconjunto A_0 dos quatérnios puros independe da base $\{1, i, j, k\}$.

Teorema 2.20. *Seja* $x \in A = (\frac{a,b}{F})$, $x \neq 0$. *Então* $x \in A_0$ *se, e somente se,* $x \notin F$ *e* $x^2 \in F$.

Demonstração: Seja $x = \alpha + \beta i + \gamma j + \delta k \in A$. Então calculando x^2 obtemos

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

Se $x \in A_0$, então $\alpha = 0$. Portanto $x^2 = a\beta^2 + b\gamma^2 - ab\delta^2 \in F$ e $x \notin F$. Reciprocamente, se $x \notin F$, então $\beta \neq 0$ ou $\gamma \neq 0$ ou $\delta \neq 0$. E consequentemente, como $x^2 \in F$ pela equação 2.1 devemos ter $\alpha = 0$. Portanto $x \in A_0$. □

Corolário 2.21. *Se* $A = (\frac{a,b}{F}), A' = (\frac{a',b'}{F})$ *e* $\varphi : A \to A'$ *é um isomorfismo de álgebras, então* $\varphi(A_0) = {A_0}'$.

Demonstração: Seja $x \in A_0$, então pelo teorema anterior $x \notin F$ e $x^2 \in F$. Considerando que $\varphi(F) = F$ (pois φ é um isomorfismo de anéis) e a injetividade de φ temos que $\varphi(x) \notin F$ e $\varphi(x)^2 = \varphi(x^2) \in F$. Logo $\varphi(x) \in {A_0}'$. Portanto, $\varphi(A_0) \subset {A_0}'$.

Por outro lado, pelo teorema acima, se $y \in {A_0}'$, então $y \notin F$ e $y^2 \in F$. Seja $x \in A$ tal que $\varphi(x) = y$. Como visto $\varphi(F) = F$, logo $x \notin F$. Pela injetividade de φ e de $\varphi(x^2) = \varphi(x)^2 = y^2 \in F$, segue que $x^2 \in F$. Novamente pelo teorema anterior, temos que $x \in A_0$, implicando ${A_0}' \subset \varphi(A_0)$. Obtendo a igualdade desejada. □

Definição 2.22. O *conjugado* de $x = \alpha + \beta i + \gamma j + \delta k \in A$ é definido como sendo $\overline{x} = \alpha - (\beta i + \gamma j + \delta k)$.

Observação 2.23. As seguintes propriedades seguem diretamente da definição de conjugado:

(1) $\overline{x + y} = \overline{x} + \overline{y}$;

(2) $\overline{xy} = \overline{y}\ \overline{x}$;

(3) $\overline{\overline{x}} = x$;

(4) $\overline{rx} = r\overline{x}, r \in F$;

(5) Se $x \in A_0$, então $\overline{x} = -x$;

(6) $x \in F$ se, e somente se, $\overline{x} = x$;

Definição 2.24. Dado $x \in A = (\frac{a,b}{F})$, definimos a *norma de* x por $N(x) = x\overline{x}$ e o *traço de* x por $T(x) = x + \overline{x}$.

Observação 2.25. Note que $N(x),\ T(x) \in F$, para todo $x \in A$. De fato, $\overline{T(x)} = \overline{x} + \overline{\overline{x}} = \overline{x} + x = T(x)$ e $\overline{N(x)} = \overline{x\overline{x}} = \overline{\overline{x}}\ \overline{x} = x\overline{x} = N(x)$. Portanto, pela observação 2.23(6), temos que $N(x)$, $T(x) \in F$.

2.2.1 Álgebra de Quatérnios como Espaço Quadrático

Iremos definir uma forma quadrática na álgebra de quatérnios $A = (\frac{a,b}{F})$ e mostrar que muitas informações sobre A podem ser obtidas a partir desta forma quadrática, e vice-versa.

Definição 2.26. Considere a aplicação $B : A \times A \to F$ definida por $B(x, y) = \frac{1}{2}(x\overline{y}+y\overline{x}) = \frac{1}{2}T(x\overline{y}) \in F$. É fácil ver que B é uma forma bilinear simétrica. Observe que a forma quadrática associada à B é dada por $q_B(x) = B(x, x) = \frac{1}{2}T(x\overline{x}) = N(x)$. Logo, N é uma forma quadrática em A, chamada *forma norma de* A. Assim, (A, N) é um espaço quadrático.

Observação 2.27. Seja (A, B) o espaço bilinear associado a forma norma de $A = (\frac{a,b}{F})$. Considere os quatérnios puros $x, y \in A_0$. Assim $B(x, y) = \frac{1}{2}(x\overline{y} + y\overline{x}) = \frac{1}{2}(-xy - yx) = -\frac{1}{2}(xy + yx)$. Consequentemente, $x, y \in A_0$ são ortogonais no espaço bilinear (A_0, B) se, e somente se, x e y anticomutam em A_0. Em particular, $\{i, j, k\}$ forma uma base ortogonal para o subespaço $A_0 \subset A$, pois $ij = -ji$, $ik = -ki$ e $kj = -jk$.

Se x é um quatérnio puro, então $\overline{x} = -x$ e assim $T(x) = 0$. Logo $1 \perp x$, para todo $x \in A_0$, pois $B(x, 1) = \frac{1}{2}T(x)$.

Proposição 2.28. *Seja* $A = (\frac{a,b}{F})$. *O espaço bilinear* (A, B) *tem base ortogonal* $\{1, i, j, k\}$, *a forma norma* N *é regular e isométrica a* $\langle 1, -a, -b, ab\rangle$.

Demonstração: Como observado em 2.27 temos que $\{i, j, k\}$ é uma base ortogonal para (A_0, B) e 1 é ortogonal a $\{i, j, k\}$. Portanto, $\{1, i, j, k\}$ é uma base ortogonal para (A, B).

Observe, que rad $A = \{x \in A \mid B(x, A) = 0\}$. Seja $x = \alpha+\beta i+\gamma j+\delta k \in \operatorname{rad} A$, então $B(\alpha + \beta i + \gamma j + \delta k, y) = 0$, para todo $y \in A$. Tomando $y = 1$, substituindo e usando a linearidade de B, obtemos $\alpha B(1, 1) + \beta B(i, 1) + \gamma B(j, 1) + \delta B(k, 1) = 0$, então α é necessariamente zero. Analogamente para $y = i$, j, k, obtemos $\beta = \gamma = \delta = 0$. Assim, rad $A = \{0\}$. Consequentemente, N é uma forma quadrática regular. Agora, como $N(i) = i\overline{i} = -i^2 = -a$, $N(j) = j\overline{j} = -j^2 = -b$, $N(k) = k\overline{k} = -k^2 = ab$, segue que se $x = \alpha + \beta i + \gamma j + \delta k \in A$, então $N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2$. Logo, $\langle 1, -a, -b, ab\rangle$ é uma diagonalização de N. Portanto os espaços quadráticos (A, N) e $(A, \langle 1, -a, -b, ab\rangle)$ são isométricos. □

Proposição 2.29. *Sejam* $A = (\frac{a,b}{F})$ *e* $N : A \to F$ *a forma norma de* A. *Então,*

(1) *Para todos* $x, y \in A$, $N(xy) = N(x)N(y)$;

(2) $x \in A$ *é inversível se, e somente se,* $N(x) \neq 0$ *(isto é, se* x *é anisotrópico);*

Demonstração: (1) Sejam $x, y \in A$, então $N(xy) = xy\overline{xy} = xy\overline{y}\ \overline{x} = xN(y)\overline{x}$. Como $N(y) \in F = Z(A)$, temos que $N(xy) = x\overline{x}N(y) = N(x)N(y)$.

(2) Seja $x \in A$. Se existe $x^{-1} \in A$, então por **(1)** $N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1$, assim $N(x) \neq 0$. Reciprocamente se $N(x) \neq 0$, da equação $x\overline{x} = N(x).1$, segue que $x.\frac{\overline{x}}{N(x)} = 1$. Portanto $x^{-1} = \frac{\overline{x}}{N(x)} \in A$. □

O próximo resultado mostra que as álgebras de quatérnios são completamente determinadas pelas suas formas normas.

Proposição 2.30. *Para as álgebras de quatérnios* $A = (\frac{a,b}{F})$ *e* $A' = (\frac{a',b'}{F})$*, as seguintes afirmações são equivalentes:*

(1) *A é isomorfa à* A' *como* F*- álgebra;*

(2) $(A, N) \cong (A', N')$*;*

(3) $(A_0, N_0) \cong (A'_0, N'_0)$*, onde* $N_0 = \langle -a, -b, ab\rangle$ *e* $N'_0 = \langle -a', -b', a'b'\rangle$*.*

Demonstração: **(1)** $\Rightarrow$ **(2)** Se $\varphi : A \to A'$ é um isomorfismo de álgebras, pelo Corolário 2.21, temos que $\varphi(A_0) = {A_0}'$. Considere $x = \alpha + x_0$, onde $\alpha \in F$ e $x_0 \in A_0$, então $\overline{x} = \alpha - x_0$. Segue que $\varphi(x) = \varphi(\alpha + x_0) = \varphi(\alpha) + \varphi(x_0)$ e $\overline{\varphi(x)} = \overline{\varphi(\alpha) + \varphi(x_0)} = \varphi(\alpha) - \varphi(x_0) = \varphi(\alpha) + \varphi(-x_0) = \varphi(\alpha - x_0) = \varphi(\overline{x})$. 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 entre os espaços quadráticos (A, N) e (A', N').

(2) $\Rightarrow$ **(3)** Pela Proposição 2.28, temos que $N \cong \langle 1, -a, -b, ab\rangle$ e $N' \cong \langle 1, -a', -b', a'b'\rangle$. Utilizando o Teorema do Cancelamento de Witt 1.35, segue o resultado.

(3) $\Rightarrow$ **(1)** Seja $\sigma : A_0 \to {A_0}'$ uma isometria. Então, $-a = N(i) = N'(\sigma(i)) = \sigma(i)\overline{\sigma(i)} = -\sigma(i)^2$. Logo $\sigma(i)^2 = a$. Analogamente, verificamos que $\sigma(j)^2 = b$. Pelo fato de i ser ortogonal a j, temos $B_{N'}(\sigma(i), \sigma(j)) = B_N(i, j) = 0$. Assim, $\frac{1}{2}(\sigma(i)\overline{\sigma(j)} + \sigma(j)\overline{\sigma(i)}) = 0$, ou seja, $\sigma(i)\sigma(j) = -\sigma(j)\sigma(i)$. Pela observação 2.27, temos que $\sigma(i)\sigma(j) = -\sigma(j)\sigma(i) \in {A'}_0$. Então $\{1,\ \sigma(i),\ \sigma(j),\ \sigma(i)\sigma(j)\}$ é uma base para A' sobre F. Considerando $\varphi : A \to A'$ tal que $\varphi(1) = 1,\ \varphi(i) = i',\ \varphi(j) = j'$ e $\varphi(k) = k'$, podemos verificar facilmente que φ é um isomorfismo de F- álgebras. □

Corolário 2.31. $A = (\frac{a,a}{F}) \simeq (\frac{a,-1}{F}) = A'$.

Demonstração: Note que as formas normas $\langle 1, -a, -a, a^2\rangle$ *e* $\langle 1, -a, 1, -a\rangle$ são isométricas. □

Teorema 2.32. *Para* $A = (\frac{a,b}{F})$ *as seguintes afirmações são equivalentes:*

(1) $A \simeq (\frac{1,-1}{F})$*;*

(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) $(A_0, \langle -a, -b, ab\rangle)$ *é um espaço quadrático isotrópico;*

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

(7) $a \in N(E)$*, onde* $E = F(\sqrt{b})$*.*

Demonstração: (1) $\Rightarrow$ (2) Pela Proposição 2.18, $A \simeq M_2(F)$. Como $M_2(F)$ tem divisores de zero, segue que A também tem. Portanto A não é uma álgebra com divisão, pois os divisores de zero não são inversíveis.

(2) $\Rightarrow$ (3) Por hipótese, existe $x \in A$ não nulo tal que x não é inversível. Logo, pela Proposição 2.29(2), $N(x) = 0$. Portanto, (A, N) é um espaço quadrático isotrópico.

(3) $\Rightarrow$ (4) Como N é isotrópica, pelo Corolário 1.28 temos que $N \cong \mathbb{H} \perp q$, onde $\mathbb{H}$ é um plano hiperbólico e q uma forma binária regular, isto é, $\langle 1, -a, -b, ab\rangle \cong \mathbb{H} \perp \langle c, d\rangle$. Calculando o determinante obtemos $1.\dot{F}^2 = -cd.\dot{F}^2$. Assim, $d(\langle c, d\rangle) = -\dot{F}^2$. Pelo Teorema 1.26, temos $\langle c, d\rangle \cong \mathbb{H}$. Logo $N \cong \mathbb{H} \perp \langle c, d\rangle \cong 2\mathbb{H}$. Portanto (A, N) é um espaço quadrático hiperbólico.

(4) $\Rightarrow$ (5) Como (A, N) tem dimensão 4 e é hiperbólico, devemos ter $N \cong \langle 1, -1, 1, -1\rangle$. Mas $N \cong \langle 1\rangle \perp \langle -a, -b, ab\rangle$. Pelo Teorema do Cancelamento de Witt 1.35, $\langle -a, -b, ab\rangle \cong \langle -1\rangle \perp \mathbb{H}$. Como $\mathbb{H}$ é isotrópico, segue que $\langle -a, -b, ab\rangle$ é isotrópica.

(5) ⇒ (6) Por hipótese e pelo Corolário 1.28(1), temos que $\mathbb{H} \subseteq \langle -a, -b, ab\rangle$. Ou seja, $\langle -a, -b, ab\rangle \cong \mathbb{H} \perp \langle d\rangle$. Calculando os determinantes, temos que $d = -1$. Logo $\langle -a, -b, ab\rangle \cong \langle 1, -1, -1\rangle$. Somando ortogonalmente $\langle a, b, 1\rangle$ em ambos os lados, obtemos $\langle 1, a, -a, b, -b, ab\rangle \cong \langle a, b, 1, 1, -1, -1\rangle$. Já que $\langle a, -a\rangle \cong \mathbb{H} \cong \langle b, -b\rangle$, podemos cancelar $2\mathbb{H}$ de ambos os lados. Obtendo $\langle 1, ab\rangle \cong \langle a, b\rangle$. Portanto, $\langle a, b\rangle$ representa 1.

(6) ⇒ (7) Se $\sqrt{b} \in F$ é imediato. Podemos assumir que $\sqrt{b} \notin F$. Seja $x, y \in F$ e $x + y\sqrt{b} \in E$. Temos $N(x + y\sqrt{b}) = x^2 - by^2$. Por hipótese $1 \in D(N)$, assim existem x_0, $y_0 \in M$ tais que $a{x_0}^2 + b{y_0}^2 = 1$, de modo que x_0 não pode ser zero, caso contrário $\sqrt{b} \in F$. Ou seja,

$$a = \frac{1}{{x_0}^2}(1 - b{y_0}^2) = (\frac{1}{x_0})^2 - b(\frac{y_0}{x_0})^2 = N(\frac{1}{x_0} + \frac{y_0}{x_0}\sqrt{b}).$$

Portanto, $a \in N(E)$.

(7) ⇒ (2) Como anteriormente vamos analisar os casos em que $\sqrt{b} \in F$ e $\sqrt{b} \notin F$. Se $d = \sqrt{b} \in F$, então $d^2 = b = j^2$, assim $(d + j)(d - j) = 0$. Como $\{1, j\}$ são linearmente independentes sobre F, temos que $(d + j) \neq 0$ e $(d - j) \neq 0$. Portanto A tem divisores de zero.

Se $\sqrt{b} \notin F$, por hipótese existe $x, y \in F$ tais que $N(x + dy) = x^2 - by^2 = a$. Observe que x e y não são nulos simultaneamente. Logo o quatérnio $z = x+i+yj \in A$ é não nulo e tem norma $z\overline{z} = x^2 - a - by^2 = 0$. Portanto z é um divisor de zero e A não é uma álgebra com divisão.

(2) ⇒ (1) Pelo Teorema de Wedderburn (veja [10], Cap.8, Cor 1.6), A é isomorfa a uma álgebra de matrizes $M_m(D)$, onde D é uma álgebra com divisão sobre F. Ou seja, dim $(A) = m^2$.dim D. Se $m = 1$, então dim $D = 4$ e $A \simeq M_1(D) \simeq D$, o que é um absurdo já que A não é uma álgebra com divisão. Logo $m = 2$, então $\dim(D) = 1$. Portanto $D \simeq F$ e $A \simeq M_2(F)$. □

Definição 2.33. Dizemos que uma álgebra de quatérnios $A = (\frac{a,b}{F})$ se *fatora*, se ela satisfaz uma (e portanto todas) condição do Teorema 2.32.

Corolário 2.34. (1) *Se $a \in \dot{F}$, então as álgebras de quatérnios $(\frac{1,a}{F}), (\frac{a,-a}{F})$ se fatoram;*

(2) *Se $a \neq 0, 1$, então $(\frac{a,1-a}{F})$ também se fatora.*

Demonstração: Observe que as formas binárias $\langle 1, a\rangle, \langle a, -a\rangle, \langle a, 1-a\rangle$ representam 1. Logo as álgebras de quatérnios $(\frac{a,1}{F})$, $(\frac{a,1-a}{F})$ satisfazem o Teorema 2.32. Portanto elas se fatoram. □

Corolário 2.35. ***(Classificação de Formas Binárias)*** *As formas regulares $q = \langle a, b\rangle$, $q' = \langle a', b'\rangle$ são isométricas se, e somente se, $d(q) = d(q')$ e $(\frac{a,b}{F}) \simeq (\frac{a',b'}{F})$.*

Demonstração: Se $q \cong q'$, então $M_q = C^t M_{q'} C$ e $d(q) = \det(M_q).\dot{F}^2 = \det(M'_q)\det(C^2)\dot{F}^2 = d(q')$. Agora temos que

$$\langle -1\rangle(\langle 1, -a, -b, ab\rangle) \cong \langle -1, a, b, -ab\rangle \cong \langle -1, a', b', -a'b'\rangle \cong \langle -1\rangle(\langle 1, -a', -b', a'b'\rangle),$$

pois $\langle a, b\rangle \cong \langle a', b'\rangle$ e $ab.\dot{F}^2 = a'b'.\dot{F}^2$. Então $(\frac{a,b}{F})$ e $(\frac{a',b'}{F})$ possuem formas normas isométricas. Portanto, $(\frac{a,b}{F})$ e $(\frac{a',b'}{F})$ são isomorfas.

Reciprocamente, se as álgebras de quatérnios são isomorfas, temos $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle$ e de $d(q) = d(q')$ temos $ab.\dot{F}^2 = a'b'.\dot{F}^2$. Assim, pelo Teorema do Cancelamento de Witt temos $\langle -a, -b\rangle \cong \langle -a', -b'\rangle$. Portanto, $q \cong q'$. □

Corolário 2.36. ***(Linearidade)*** *Para $a, b, c \in \dot{F}$, temos*

$$(\frac{a,b}{F}) \otimes (\frac{a,c}{F}) \simeq (\frac{a,bc}{F}) \otimes (\frac{c,-a^2c}{F}) \simeq (\frac{a,bc}{F}) \otimes M_2(F).$$

Demonstração: Considere $\{1, i, j, k\}$ e $\{1, i', j', k'\}$ bases de $A = (\frac{a,b}{F})$ e $A' = (\frac{a,c}{F})$, respectivamente. Queremos analizar o produto tensorial das álgebras A e A'. Primeiramente vamos construir uma subálgebra de A.

Consideremos $X = F(1\otimes 1)+F(i\otimes 1)+F(j\otimes j')+F(k\otimes j') = F.1+FI+FJ+FK$, onde $I = i \otimes 1$, $J = j \otimes j'$ e $K = IJ$. Logo X é uma subálgebra de $A \otimes A'$ de

dimensão 4. Temos ainda que

$$\begin{aligned} I^2 &= (i\otimes 1)(i\otimes 1) = i^2\otimes 1 = a\otimes 1 = a; \\ J^2 &= (j\otimes j')(j\otimes j') = j^2\otimes j'^2 = b\otimes c = bc; \\ -IJ &= -(i\otimes 1)(j\otimes j') = -ij\otimes j' = ji\otimes j' = JI. \end{aligned}$$

É fácil ver que a subálgebra X é isomorfa a álgebra de quatérnios $(\frac{a,bc}{F})$.

Agora vamos construir uma nova subálgebra Y. Seja $Y = F(1\otimes 1)+F(1\otimes j')+F(i\otimes k')+F(i\otimes -ci') = F.1+F\widetilde{I}+F\widetilde{J}+F\widetilde{K}$, onde $\widetilde{I} = 1\otimes j'$, $\widetilde{J} = i\otimes k'$, $\widetilde{K} = i\otimes -ci'$ e

$$\begin{aligned} \widetilde{I^2} &= 1\otimes j'^2 = c; \\ \widetilde{J^2} &= i^2\otimes k'^2 = -a^2c; \\ \widetilde{I}\widetilde{J} &= i\otimes j'k' = i\otimes(-ci') \ e \\ \widetilde{J}\widetilde{I} &= i\otimes k'j' = -\widetilde{K} = -\widetilde{I}\widetilde{J}. \end{aligned}$$

Dessa forma, é fácil ver que Y é isomorfo a álgebra de quatérnios $(\frac{c,-a^2c}{F})$. Pela Proposição 2.18(1) e pelo Corolário 2.34, temos que $Y \simeq (\frac{c,-a^2c}{F}) \simeq (\frac{c,-c}{F}) \simeq M_2(F)$.

Para termos o resultado só nos resta mostrar que $A\otimes A'$ é isomorfa ao produto tensorial das subálgebras X e Y. Primeiro observemos que os elementos de $\{1, I, J, K\}$ comutam com os elementos de $\{1, \widetilde{I}, \widetilde{J}, \widetilde{K}\}$. Por exemplo,

$$\begin{aligned} I\widetilde{J} &= (i\otimes 1)(i\otimes k') = (i^2\otimes k') = (i\otimes k')(i\otimes 1) = \widetilde{J}I; \\ K\widetilde{J} &= (k\otimes j')(i\otimes k') = ki\otimes j'k' = (-ik)\otimes(-k'j') = (i)\otimes k'(k\otimes j') = \widetilde{J}K. \end{aligned}$$

Analogamente se verifica para os outros elementos.

O produto das bases de X e de Y nos fornece a seguinte base para $X\otimes Y$, $B = \{1\otimes 1 = e_1,\ 1\otimes\widetilde{I} = e_2,\ 1\otimes\widetilde{J} = e_3,\ 1\otimes\widetilde{K} = e_4,\ I\otimes 1 = e_5,\ I\otimes\widetilde{I} = e_6,\ I\otimes\widetilde{J} = e_7,\ I\otimes\widetilde{K} = e_8,\ J\otimes 1 = e_9,\ J\otimes\widetilde{I} = e_{10},\ J\otimes\widetilde{J} = e_{11},\ J\otimes\widetilde{K} = e_{12},\ K\otimes 1 = e_{13}, K\otimes\widetilde{I} = e_{14},\ K\otimes\widetilde{J} = e_{15},\ K\otimes\widetilde{K} = e_{16}\}$ é uma base para $X\otimes Y$.

Definimos $\varphi : X \otimes Y \to A \otimes A'$ tal que $\varphi(x \otimes y) = xy$, com $x \otimes y \in B$ e estendemos por linearidade. Como os elementos da base de X e de Y comutam, temos que dados $x \otimes y$, $x_1 \otimes y_1 \in B$, então $\varphi((x \otimes y).(x_1 \otimes y_1)) = \varphi((xx_1) \otimes (yy_1)) = xx_1yy_1 = xyx_1y_1 = \varphi(x \otimes y).\varphi(x_1 \otimes y_1)$. Dessa forma temos que $\varphi(ZW) = \varphi(Z)\varphi(W)$, para todos $Z, W \in X \otimes Y$. Como φ é linear e $\dim(X \otimes Y) = 16 = \dim(A \otimes A')$, se demonstrarmos que φ é sobrejetora teremos um isomorfismo de F-álgebras. Para mostrar que φ é sobrejetora, basta verificar que o conjunto de geradores $C = \{1 \otimes 1, 1 \otimes i', 1 \otimes j', 1 \otimes k', i \otimes 1, i \otimes i', i \otimes j', i \otimes k', j \otimes 1, j \otimes i', j \otimes j', j \otimes k', k \otimes 1, k \otimes i', k \otimes j', k \otimes k'\}$ de $A \otimes A'$ está na imagem de φ. Fazendo os cálculos, temos:

$$
\begin{aligned}
\varphi(e_1) &= 1 \otimes 1; \\
\varphi(e_2) &= 1 \otimes j'; \\
\varphi(e_3) &= i \otimes k'; \\
\varphi(e_4) &= -c(i \otimes i') \Rightarrow \varphi(-e_4/c) = i \otimes i'; \\
\varphi(e_5) &= i \otimes 1; \\
\varphi(e_6) &= i \otimes j'; \\
\varphi(e_7) &= a(1 \otimes k') \Rightarrow \varphi(e_7/a) = 1 \otimes k'; \\
\varphi(e_8) &= a \otimes -ci' \Rightarrow \varphi(-e_8/ac) = 1 \otimes i'; \\
\varphi(e_9) &= j \otimes j'; \\
\varphi(e_{10}) &= j \otimes -c \Rightarrow \varphi(-e_{10}/c) = j \otimes 1; \\
\varphi(e_{11}) &= -k \otimes -i'c \Rightarrow \varphi(e_{11}/c) = k \otimes i'; \\
\varphi(e_{12}) &= -k \otimes ck' \Rightarrow \varphi(-e_{12}/c) = k \otimes k'; \\
\varphi(e_{13}) &= k \otimes j' \\
\varphi(e_{14}) &= k \otimes c \Rightarrow \varphi(e_{14}/c) = k \otimes 1; \\
\varphi(e_{15}) &= -ja \otimes -ci' \Rightarrow \varphi(e_{15}/ac) = j \otimes i'; \\
\varphi(e_{16}) &= -ja \otimes ck' \Rightarrow \varphi(-e_{16}/ac) = j \otimes k'.
\end{aligned}
$$

Segue que cada elemento da base C é da forma $\varphi(\alpha_i e_i)$, para algum $\alpha_i \in F$ e e_i conveniente. Portanto φ é sobrejetora. $\square$

2.3 O Invariante de Hasse

Seja (V, q) um espaço quadrático. Se $\langle a_1, ..., a_n\rangle$ é uma diagonalização de q, definimos o *invariante de Hasse*, como sendo a classe de $s(q) = \prod_{1\leqslant i<j\leqslant n}[(\frac{a_i,a_j}{F})]$ no grupo de Brauer $Br(F)$. Onde $s(q) = 1$ se $n = 1$.

Denotaremos apenas por $[a_i, a_j]$ a classe $[(\frac{a_i,a_j}{F})] \in Br(F)$.

Proposição 2.37. *Dada uma forma quadrática q sobre F. O invariante $s(q)$ independe da diagonalização escolhida para q.*

Demonstração: Pelo Teorema 1.43, quaisquer duas diagonalizações de uma mesma forma quadrática são equivalentes por cadeia. Dessa forma é suficiente comparar as diagonalizações $q_1 = \langle a, b, a_3, ..., a_n\rangle$ e $q_2 = \langle c, d, a_3, ..., a_n\rangle$ com $\langle a, b\rangle \cong \langle c, d\rangle$. Pelo Corolário 2.35, esta última isometria nos diz que $ab = cd\dot{F}^2$ e $(\frac{a,b}{F}) \simeq (\frac{c,d}{F})$. Logo $[a, b] = [c, d]$. Usando estes fatos e a linearidade (Corolário 2.36), temos

$$\begin{aligned}
s(\langle a, b, a_3, ..., a_n\rangle) &= [a, b][a, a_3...a_n][b, a_3...a_n].\prod_{3\leq i\leq j}^{n}[a_i, a_j] \\
&= [a, b][ab, a_3...a_n]\prod_{3\leq i\leq j}^{n}[a_i, a_j] \\
&= [c, d][cd, a_3...a_n]\prod_{3\leq i\leq j}^{n}[a_i, a_j] \\
&= [c, d][c, a_3...a_n][d, a_3...a_n]\prod_{3\leq i\leq j}^{n}[a_i, a_j] \\
&= [c, da_3...a_n][d, a_3...a_n]\prod_{3\leq i\leq j}^{n}[a_i, a_j] \\
&= s(\langle c, d, a_3, ..., a_n\rangle).
\end{aligned}$$

Portanto $s(q_1) = s(q_2)$. $\square$

O próximo teorema nos fornece uma classificação de formas quadráticas de dimensão menor ou igual a 3.

Teorema 2.38. *Sejam q e q_1 formas quadráticas sobre F tais que* $\dim q \leq 3$, $\dim q_1 \leq 3$. *Então, $q \cong q_1$ se, e somente se, $s(q) = s(q_1)$, $d(q) = d(q_1)$ e* $\dim q = \dim q_1$.

Demonstração: Se $q \cong q_1$, pelo que já vimos $s(q) = s(q_1)$, $d(q) = d(q_1)$ e $\dim q = \dim q_1$. Reciprocamente, se $\dim q = \dim q_1 = 2$, o resultado segue do Corolário 2.35. Vamos supor que $\dim q = \dim q_1 = 3$, logo $q \cong \langle a, b, c\rangle$ e $q_1 \cong \langle a_1, b_1, c_1\rangle$. Se $d = \det(q) = \det(q_1)$, temos que

$$\begin{aligned} s(\langle -d\rangle q) &= s(\langle -ad, -bd, -cd\rangle) \\ &= [-ad, (-bd)(-cd)][-bd, -cd] \\ &= [-ad, bc][-bd, -cd] \\ &= [a, b][a, c][-d, b][-d, c][b, c][b, -d][-d, c][-d, -d] \\ &= [a, b][a, c][b, c][-d, c]^2[-d, c^2][-d, -d] = s(q)[d, -d]. \end{aligned}$$

Analogamente, $s(\langle -d\rangle q_1) = s(q_1)[-d, d]$ e como $s(q) = s(q_1)$, temos que $s(\langle -d\rangle q) = s(\langle -d\rangle q_1)$. Como $d = abc$, temos $\langle -d\rangle q \cong \langle -abc\rangle\langle a, b, c\rangle \cong \langle -bc, -ac, -ab\rangle = \langle x, y, -xy\rangle$, onde $x = -bc$, $y = -ac$. Assim

$$\begin{aligned} s(\langle -d\rangle q) &= s(\langle x, y, -xy\rangle) = [x, y][x, -xy][y, -xy] \\ &= [x, y][xy, -xy] = [x, y]. \end{aligned}$$

Analogamente, $\langle -d\rangle q_1 \cong \langle x_1, y_1, -x_1y_1\rangle$ e $s(\langle -d\rangle q_1) = [x_1, y_1]$.

Como $s(\langle -d\rangle q) = s(\langle -d\rangle q_1)$, segue que $[x, y] = [x_1, y_1]$. Assim suas formas normas são isométricas, ou seja, $\langle 1, -x, -y, xy\rangle \cong \langle 1, -x_1, -y_1, x_1y_1\rangle$. Pelo Teorema do Cancelamento de Witt, $\langle -x, -y, xy\rangle \cong \langle -x_1, -y_1, x_1y_1\rangle$, o que implica que $\langle -d\rangle q \cong \langle -d\rangle q_1$. Multiplicando ambos os lados por $\langle -d\rangle$, temos que $q \cong q_1$. $\square$

Proposição 2.39. *Uma forma ternária q é isotrópica se, e somente se,* $s(q) = [-1, -d(q)]$.

Demonstração: Suponha q isotrópica, então $q \cong \langle 1, -1, a\rangle$, para algum $a \in \dot{F}$. Claramente $s(q) = [1, -1].[1, a][-1, a] = [-1, a] = [-1, -d(q)]$.

Reciprocamente, q e $\langle 1, -1, -d(q)\rangle$ tem a mesma dimensão, mesmo determinante e o mesmo invariante de Hasse. Pelo Teorema 2.38, temos que $q \cong \langle 1, -1, -d(q)\rangle$. Portanto q é isotrópica. □

O teorema de classificação que segue se aplica a uma larga classe de corpos, por exemplo, corpos p-ádicos e corpos de números álgebricos não reais.

Teorema 2.40. *Suponhamos que toda forma quadrática de dimensão 5 sobre F é isotrópica. Então dimensão, determinante e invariante de Hasse classificam formas quadráticas sobre F, ou seja $q \cong q_1$ se, e somente se,* $\dim q = \dim q_1$, $d(q) = d(q_1)$ *e* $s(q) = s(q_1)$.

Demonstração: A ida é imediata. Reciprocamente, se $\dim q \leq 3$, segue do Teorema 2.38. Assim, suponhamos $\dim q = \dim q_1 = n \geq 4$, $d(q) = d(q_1)$ e $s(q) = s(q_1)$. Façamos por indução sobre n. Para $n = 4$ temos que $q' = q \perp \langle -1\rangle \cong q_1 \perp \langle -1\rangle = q_1'$ e por hipótese q', q_1' são isotrópicas, logo q, q_1 representam o 1, já que $\langle -1\rangle$ não representa 1. Ou seja, pelo Teorema do Cancelamento de Witt e pelo Teorema 2.38 temos o resultado. Agora para n, pelo Corolário 1.28 q e q_1 são universais. Em particular, q e q_1 representam 1. Assim $q \cong \langle 1\rangle \perp q'$ e $q_1 \cong \langle 1\rangle \perp q'_1$. Dessa forma, $d(q') = d(q) = d(q_1) = d(q'_1)$ e $\dim q' = \dim q'_1$. Sejam $q' \cong \langle a_1, ..., a_{n-1}\rangle$ e $q'_1 \cong \langle b_1, ..., b_{n-1}\rangle$. 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 $[1, a_1...a_n]s(q') = [1, b_1...b_n]s(q'_1)$, mas $[1, x] = 1$ em $Br(F)$, para todo $x \in \dot{F}$. Assim, $s(q') = s(q'_1)$.

Como $\dim q' = \dim q'_1 = n - 1$ podemos usar indução e concluir que $q' \cong q'_1$. Portanto $q \cong \langle 1\rangle \perp q' \cong \langle 1\rangle q'_1 \cong q_1$. □

Capítulo 3

Matrizes de Hankel, Formas Traço e Traço Escalar

Neste capítulo daremos uma caracterização das matrizes de Hankel e mostraremos como elas surgem naturalmente como uma representação matricial de formas traços e traços escalares de extensões separáveis de corpos.

3.1 Matrizes de Hankel

Definição 3.1. Sejam F um corpo e s_0, s_1, ..., s_{2n-2} uma sequência de elementos de F. Uma matriz S de ordem $n \times n$ da forma abaixo é chamada de *matriz de Hankel*

$$S = \begin{pmatrix} s_0 & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{pmatrix}.$$

A matriz de Hankel S é uma matriz simétrica listrada, isto é, as entradas são constantes ao longo de cada linha paralela a diagonal secundária. Note que a entrada (i, j) de uma matriz de Hankel depende apenas da soma dos dígitos i, j.

Proposição 3.2. *Seja H uma matriz $n \times n$ com entradas em F. Suponha que H é não singular, ou, de modo mais geral, que H possui as primeiras $n-1$ linhas linearmente independentes. Então H é uma matriz de Hankel se, e somente se,*

existem elementos $c_1, ..., c_n \in F$ *tais que a matriz*

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & & & 1 \\ -c_n & -c_{n-1} & & \dots & & -c_1 \end{pmatrix}$$

satisfaz $CH = HC^t$.

Demonstração: Seja H com entradas h_{ij}. Por hipótese temos que $CH = HC^t$, para alguma matriz C. Fazendo as multiplicações de ambos os lados da igualdade, obtemos

$$\begin{pmatrix} h_{21} & \dots & h_{2n} \\ h_{31} & & h_{3n} \\ \vdots & & \vdots \\ -(c_n h_{11} + c_{n-1} h_{21} + ... + c_1 h_{n1}) & \dots & -(c_n h_{1n} + c_{n-1} h_{2n} + ... + c_1 h_{nn}) \end{pmatrix} =$$

$$= \begin{pmatrix} h_{12} & h_{13} & \dots & -(c_n h_{11} + ... + c_1 h_{1n}) \\ h_{22} & h_{23} & & -(c_n h_{21} + ... + c_1 h_{2n}) \\ \vdots & & & \vdots \\ h_{n2} & h_{n3} & & -(c_n h_{1n} + ... + c_1 h_{nn}) \end{pmatrix}.$$

Analisando termo a termo, conseguimos concluir que H é uma matriz de Hankel.

Reciprocamente, vamos assumir que H é uma matriz de Hankel com as primeiras $n-1$ linhas linearmente independentes. Tomemos $H = \begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ \vdots & \vdots & \dots & \vdots \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{pmatrix}$.

Vamos encontrar uma matriz $C = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & & 1 \\ -c_n & -c_{n-1} & & \dots & & -c_1 \end{pmatrix}$ tal que $CH = HC^t$. Desenvolvendo estes produtos obtemos uma igualdade de matrizes onde os $n-1$ elementos das $n-1$ primeiras linhas são obviamente iguais. Igualando as entradas correspondentes na última linha (ou última coluna) obtemos o seguinte sistema

$$\begin{cases} -s_0 c_n - s_1 c_{n-1} - ... - s_{n-1} c_1 = s_n \\ \vdots \\ -s_{n-1} c_n - s_n c_{n-1} - ... - s_{2n-2} c_1 = s_{2n-1}. \end{cases}$$

A representação matricial deste sistema é

$$\begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ \vdots & \vdots & & \vdots \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{pmatrix} \cdot \begin{pmatrix} -c_n \\ -c_{n-1} \\ \vdots \\ -c_1 \end{pmatrix} = \begin{pmatrix} s_n \\ s_{n+1} \\ \vdots \\ s_{2n-1} \end{pmatrix}.$$

Como temos que as $n-1$ linhas de H são linearmente independentes, a matriz dos coeficientes do sistema é não singular. Portanto, o sistema tem solução. $\square$

Exemplo 3.3. A proposição anterior é em geral falsa se as $n-1$ primeiras linhas não forem linearmente independentes. Como por exemplo, a matriz de Hankel 2×2 $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ não satisfaz a equação $CH = HC^t$, para qualquer C. De fato, a igualdade

$$\begin{pmatrix} 0 & 1 \\ -c_2 & -c_1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -c_2 \\ 1 & -c_1 \end{pmatrix}$$

não ocorre para qualquer $c_1, c_2 \in F$, pois $\begin{pmatrix} 0 & 1 \\ 0 & -c_1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & -c_1 \end{pmatrix}$.

Definição 3.4. Uma matriz de Hankel é chamada de *matriz de Hankel periódica* se $s_i = s_{n+i}$, para cada i.

Observação 3.5. A matriz

$$S = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

é usada para caracterizar as matrizes de Hankel que são periódicas.

Proposição 3.6. *Uma matriz H é uma matriz de Hankel periódica se, somente se, $SH = HS^t$.*

Demonstração: Ao supormos que H é uma matriz de Hankel periódica é fácil calcular e observar que $HS^t = SH$. Agora seja H uma matriz de Hankel que satisfaz $HS^t = SH$ e mostremos que ela é periódica, isto é $s_{n+i} = s_i$, para todo i. Por um

lado temos

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} . \begin{pmatrix} s_k & s_{k+1} & \dots & s_{k+n-1} \\ s_{k+1} & s_{k+2} & \dots & s_{k+n} \\ s_{k+2} & s_{k+3} & \dots & s_{k+n+1} \\ \vdots & & & \vdots \\ s_{k+n-1} & s_{k+n} & \dots & s_{k+2n-2} \end{pmatrix} = \begin{pmatrix} s_{k+1} & s_{k+2} & \dots & s_{k+n} \\ s_{k+2} & s_{k+3} & \dots & s_{k+n+1} \\ s_{k+3} & & & s_{k+n+2} \\ \vdots & & & \vdots \\ s_k & s_{k+1} & \dots & s_{k+n-1} \end{pmatrix} .$$

E por outro lado

$$\begin{pmatrix} s_k & s_{k+1} & \dots & s_{k+n-1} \\ s_{k+1} & s_{k+2} & \dots & s_{k+n} \\ s_{k+2} & s_{k+3} & \dots & s_{k+n+1} \\ \vdots & & & \vdots \\ s_{k+n-1} & s_{k+n} & \dots & s_{k+2n-2} \end{pmatrix} . \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} s_{k+1} & s_{k+2} & \dots & s_k \\ s_{k+2} & s_{k+3} & \dots & s_{k+1} \\ s_{k+3} & & & s_{k+n+2} \\ \vdots & & & \vdots \\ s_{k+n} & s_{k+1} & \dots & s_{k+n-1} \end{pmatrix} .$$

Observe que $s_{k+n} = s_k$, para todo k. Portanto, H é Hankel periódica. $\square$

Vamos agora estudar um tipo particular de matrizes de Hankel que está relacionado a polinômios separáveis. Sejam $p(x)$ um polinômio mônico separável de grau n sobre F e $\alpha_1, ..., \alpha_n$ suas raízes em algum corpo de decomposição. Logo $p(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n + c_1x^{n-1} + ... + c_{n-1}x + c_n$. Recordemos que os coeficientes c_i são as funções simétricas elementares nas raízes de $p(x)$, ou seja, $c_1 = \sum_{i=1}^{n} \alpha_i$, $c_2 = \sum_{i<j} \alpha_i\alpha_j$, $c_3 = \sum_{i<j<k} \alpha_i\alpha_j\alpha_k$, ..., $c_n = \alpha_1...\alpha_n$.

Agora, definamos $s_k = \sum_{i=1}^{n} \alpha_i^k$ sendo a *soma de potência das raízes*, com k inteiro não negativo. Estas somas são elementos de F e podem ser calculadas também por meio dos coeficientes de $p(x)$ utilizando as identidades de Newton como definidas abaixo.

$$s_k + c_1s_{k-1} + c_2s_{k-2} + ... + c_{k-1}s_1 + c_kk = 0, \text{ para } k < n \text{ e}$$

$$s_k + c_1s_{k-1} + c_2s_{k-2} + ... + c_ns_{k-n+1} + c_ns_{k-n} = 0, \text{ para } k \geq n.$$

Para cada inteiro não negativo k vamos definir uma matriz de Hankel $n \times n$ da seguinte forma

$$P_k = \begin{pmatrix} s_k & s_{k+1} & s_{k+2} & \dots & s_{k+n-1} \\ s_{k+1} & s_{k+2} & s_{k+3} & & s_{k+n} \\ s_{k+2} & s_{k+3} & & & s_{k+n+1} \\ \vdots & \vdots & & & \vdots \\ s_{k+n-1} & s_{k+n} & & & s_{k+2n-2} \end{pmatrix}.$$

Considere a matriz de Vandermonde de ordem $n \times n$ dos elementos $\alpha_1, ..., \alpha_n$

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}$$

e a matriz companheira do polinômio $p(x)$

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & & 0 \\ 0 & 0 & 0 & 1 & & 0 \\ \vdots & & & & & 1 \\ -c_n & -c_{n-1} & \dots & & & -c_1 \end{pmatrix}.$$

E por fim, definimos a matriz D com entradas $\alpha_1, ..., \alpha_n$ na diagonal e zero no restante.

Proposição 3.7. *Seja $p(x) = x^n + c_1x^{n-1} + ... + c_{n-1}x + c_n \in F[x]$ e $\alpha_1, ..., \alpha_n$ suas raízes em um corpo de decomposição. As matrizes definidas anteriormente satisfazem as seguintes relações.*

(1) $VD = CV$;

(2) $CP_0 = P_1$;

(3) $VV^t = P_0$;

(4) $VDV^t = P_1$;

(5) $CP_k = P_{k+1}$, *para cada inteiro não negativo* k;

(6) $CP_k = P_kC^t$, *para cada inteiro não negativo* k.

Demonstração: Para demonstrarmos **(1)** consideremos o fato de $p(\alpha_i) = 0$, para todo α_i com $i = 1, .., n$. Assim, $\alpha_i^n = -(c_n + c_{n-1}\alpha_i + ... + c_1\alpha_i^{n-1})$. Calculando VD e CV obtemos:

$$VD = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^n & \alpha_2^n & \dots & \alpha_n^n \end{pmatrix} \quad e$$

$$CV = \begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \alpha_1^2 & \dots & \alpha_n^2 \\ \vdots & & \vdots \\ -(c_n + c_{n-1}\alpha_1 + ... + c_1\alpha_1^{n-1}) & \dots & -(c_n + c_{n-1}\alpha_n + ... + c_1\alpha_n^{n-1}) \end{pmatrix}.$$

Pelo observado inicialmente, temos a igualdade $VD = CV$.

(2) Ao fazermos a multiplicação da matriz companheira C pela matriz P_0 obtemos

$$\begin{pmatrix} s_1 & s_2 & \dots & s_n \\ s_2 & s_3 & \dots & s_{n+1} \\ \vdots & \vdots & & \vdots \\ -(c_n s_0 + ... + c_1 s_{n-1}) & -(c_n s_1 + ... + c_1 s_n) & \dots & -(c_n s_{n-1} + ... + c_1 s_{2n-2}) \end{pmatrix}.$$

Pelas identidades de Newton temos que $s_k + c_1 s_{k-1} + ... + c_n s_{k-n} = 0$, para todo $k \geq n$. Assim, $s_k = -(c_1 s_{k-1} + ... + c_n s_{k-n})$, para todo $k \geq n$. Substituindo a igualdade na matriz resultante da multiplicação CP_0 obtemos

$$CP_0 = \begin{pmatrix} s_1 & s_2 & \dots & s_n \\ s_2 & s_3 & \dots & s_{n+1} \\ \vdots & \vdots & & \vdots \\ s_n & s_{n+1} & \dots & s_{2n-1} \end{pmatrix} = P_1.$$

(3) Fazendo o cálculo de VV^t diretamente obtemos

$$\begin{pmatrix} n & \alpha_1 + \alpha_2 + ... + \alpha_n & \dots & \alpha_1^{n-1} + \alpha_2^{n-1} + ... + \alpha_n^{n-1} \\ \alpha_1 + \alpha_2 + ... + \alpha_n & \alpha_1^2 + \alpha_2^2 + ... + \alpha_n^2 & \dots & \alpha_1^n + \alpha_2^n + ... + \alpha_n^n \\ \vdots & & & \vdots \\ \alpha_1^{n-1} + \alpha_2^{n-1} + ... + \alpha_n^{n-1} & \alpha_1^n + \alpha_2^n + ... + \alpha_n^n & \dots & \alpha_1^{2n-2} + \alpha_2^{2n-2} + ... + \alpha_n^{2n-2} \end{pmatrix}.$$

Podemos observar que cada elemento da matriz resultante é uma soma de potência das raízes do polinômio $p(x)$. Identificando corretamente o índice de cada uma

dessas somas, obtemos

$$VV^t = \begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ \vdots & & & \vdots \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{pmatrix} = P_0.$$

(4) Fazendo diretamente a multiplicação VDV^t obtemos

$$\begin{pmatrix} \alpha_1 + \alpha_2 + ... + \alpha_n & \alpha_1^2 + \alpha_2^2 + ... + \alpha_n^2 & \dots & \alpha_1^n + \alpha_2^n + ... + \alpha_n^n \\ \alpha_1^2 + \alpha_2^2 + ... + \alpha_n^2 & \alpha_1^3 + \alpha_2^3 + ... + \alpha_n^3 & & \alpha_1^{n+1} + \alpha_2^{n+1} + ... + \alpha_n^{n+1} \\ \vdots & & & \vdots \\ \alpha_1^n + \alpha_2^n + ... + \alpha_n^n & \alpha_1^{n+1} + \alpha_2^{n+1} + ... + \alpha_n^{n+1} & \dots & \alpha_1^{2n-1} + \alpha_2^{2n-1} + ... + \alpha_n^{2n-1} \end{pmatrix}.$$

Podemos observar novamente que cada elemento da matriz resultante é uma soma de potência das raízes do polinômio $p(x)$. Identificando corretamente o índice de cada uma dessas somas, obtemos

$$VDV^t = \begin{pmatrix} s_1 & s_2 & \dots & s_n \\ s_2 & s_3 & \dots & s_{n+1} \\ \vdots & & & \vdots \\ s_n & s_{n+1} & \dots & s_{2n-1} \end{pmatrix} = P_1.$$

(5) Calculando CP_k obtemos

$$\begin{pmatrix} s_{k+1} & \dots & s_{k+n} \\ s_{k+2} & & s_{k+n+1} \\ \vdots & & \vdots \\ -(c_n s_k + ... + c_1 s_{k+n-1}) & \dots & -(c_n s_{k+n-1} + ... + c_1 s_{k+2n-2}) \end{pmatrix}.$$

Usando as identidades de Newton obtemos a igualdade $CP_k = P_{k+1}$.

(6) Observe que

$$P_k C^t = (CP_k)^t = (P_{k+1})^t = P_{k+1} = CP_k. \ \square$$

Proposição 3.8. *Seja F um corpo infinito de característica diferente de 2. Qualquer forma quadrática regular sobre F admite uma representação por uma matriz de Hankel.*

Demonstração: Sabemos que uma forma quadrática regular admite uma representação por meio de uma matriz diagonal pelo Teorema 1.20. Como F é infinito,

podemos assumir que os elementos da diagonal são distintos (se necessário, basta multiplicá-los por quadrados). Sejam $\alpha_1, ..., \alpha_n$ estas entradas da matriz diagonal D que representa esta forma quadrática. Vamos considerar a matriz de Vandermonde V dos elementos $\alpha_1, ..., \alpha_n$ e a matriz de Hankel P_1 com entradas sendo as somas de potências de $\alpha_1, ..., \alpha_n$. Observe que V é não singular, pois os α_i's são distintos. Logo, pela Proposição 3.7(4), temos que $VDV^t = P_1$. Portanto D é congruente a uma matriz de Hankel. □

3.2 Forma Traço e Forma Traço Escalar

Nesta seção iremos mostrar que é simples obter uma representação matricial por matriz de Hankel para formas traço e traço escalares de extensão separáveis de corpos. Estaremos assumindo que o leitor esteja familiarizado com a Teoria de Galois, daremos apenas algumas referências dos resultados mais importantes.

Definição 3.9. Seja K uma extensão separável de F de dimensão n e $\overline{F}$ um fecho algébrico de F contendo K. Sejam $\sigma_1, ..., \sigma_n$ todos os F-monomorfismos $K \to \overline{F}$. Se $u \in K$, o *traço de* u é definido por

$$\mathrm{Tr}_{K/F}(u) = \sigma_1(u) + ... + \sigma_n(u).$$

Quando não houver perigo de confusão usaremos a notação Tr ao invés de $\mathrm{Tr_{K/F}}$.

Observação 3.10. (1) A definição de traço não depende da escolha feita para $\overline{F}$ (ver [4], Teo. 7.3, pg 290).

(2) Para qualquer $u \in K$ temos que $\mathrm{Tr}_{K/F}(u) \in F$ (ver [4] Teo. 7.3, pg 290).

Definição 3.11. Seja K uma extensão separável de F de dimensão finita. A *forma traço* de K é a forma quadrática $q : K \to F$ definida por $q(x) = \mathrm{Tr}(x^2)$.
Dado um elemento $z \in K$ definimos a *forma traço escalar* $q_z : K \to F$ por $q_z(x) = \mathrm{Tr}(zx^2)$.

Como K é uma extensão separável finita, temos que ela é simples, (ver [4], Prop. 6.15, pg 287). Logo $K = F(\alpha)$, para algum $\alpha \in K$. Sabemos também que $F(\alpha) \simeq \frac{F[x]}{(p(x))}$, onde $p(x) = \prod(X - \sigma(\alpha))$ é o polinômio minimal de α sobre F. Como $p(x)$ é separável sobre F, tomemos $\alpha_1 = \alpha$, α_2, ..., α_n as raízes distintas de $p(x)$. Seja $\beta = \{\alpha^{i-1} | 1 \leq i \leq n\}$ uma base para K sobre F. Sejam $\sigma_1, ..., \sigma_n$ os F-monomorfismos $K \to \bar{F}$ e suponhamos que $\alpha_j = \sigma_j(\alpha)$. Logo para todo $1 \leq i \leq j$ temos que $\alpha_r^i = \sigma_r(\alpha)^i = \sigma_r(\alpha^i)$. Assim,

$$B_q(\alpha^i, \alpha^j) = \mathrm{Tr}(\alpha^i \alpha^j) = \sum_{r=1}^{n} \sigma_r(\alpha^i \alpha^j) = \sum_{r=1}^{n} \sigma_r(\alpha^i)\sigma_r(\alpha^j) = \sum_{r=1}^{n} \alpha_r^i \alpha_r^j.$$

Logo

$$\begin{aligned}
((B_q(\alpha^{i-1}, \alpha^{j-1})) &= (\mathrm{Tr}(\alpha^{i-1}\alpha^{j-1})) \\
&= \begin{pmatrix} \mathrm{Tr}(1.1) & \mathrm{Tr}(1.\alpha) & \cdots & \mathrm{Tr}(1.\alpha^{n-1}) \\ \mathrm{Tr}(\alpha.1) & \mathrm{Tr}(\alpha.\alpha) & \cdots & \mathrm{Tr}(\alpha.\alpha^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}(\alpha^{n-1}.1) & \mathrm{Tr}(\alpha^{n-1}.\alpha) & \cdots & \mathrm{Tr}(\alpha^{n-1}.\alpha^{n-1}) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{r=1}^n 1.1 & \sum_{r=1}^n 1.\alpha_r & \cdots & \sum_{r=1}^n 1.\alpha_r^{n-1} \\ \sum_{r=1}^n \alpha_r.1 & \sum_{r=1}^n \alpha_r.\alpha_r & \cdots & \sum_{r=1}^n \alpha_r.\alpha_r^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{r=1}^n \alpha_r^{n-1}.1 & \sum_{r=1}^n \alpha_r^{n-1}.\alpha_r & \cdots & \sum_{r=1}^n \alpha_r^{n-1}.\alpha_r^{n-1} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{r=1}^n 1 & \sum_{r=1}^n \alpha_r & \cdots & \sum_{r=1}^n \alpha_r^{n-1} \\ \sum_{r=1}^n \alpha_r & \sum_{r=1}^n \alpha_r^2 & \cdots & \sum_{r=1}^n \alpha_r^n \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{r=1}^n \alpha_r^{n-1} & \sum_{r=1}^n \alpha_r^n & \cdots & \sum_{r=1}^n \alpha_r^{2n-2} \end{pmatrix} \\
&= \begin{pmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & \vdots & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{pmatrix} \\
&= P_0.
\end{aligned}$$

Ou seja, a matriz da forma traço de K sobre F com relação a base $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é a matriz de Hankel P_0 com as entradas sendo as somas de potência s_i como já definidas.

Já a matriz da forma traço escalar q_z, com $z = \alpha^k$ para algum número natural k, nesta mesma base, é a matriz de Hankel P_k. De fato,

$$\begin{aligned}
((B_q(\alpha^{i-1}, \alpha^{j-1})) &= (\mathrm{Tr}(\alpha^k \alpha^{i-1} \alpha^{j-1})) \\
&= \begin{pmatrix} \mathrm{Tr}(\alpha^k.1.1) & \mathrm{Tr}(\alpha^k.1.\alpha) & \cdots & \mathrm{Tr}(\alpha^k.1.\alpha^{n-1}) \\ \mathrm{Tr}(\alpha^k.\alpha.1) & \mathrm{Tr}(\alpha^k.\alpha.\alpha) & \cdots & \mathrm{Tr}(\alpha^k.\alpha.\alpha^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}(\alpha^k.\alpha^{n-1}.1) & \mathrm{Tr}(\alpha^k.\alpha^{n-1}.\alpha) & \cdots & \mathrm{Tr}(\alpha^k.\alpha^{n-1}.\alpha^{n-1}) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{r=1}^n \alpha_r^k.1.1 & \sum_{r=1}^n \alpha_r^k.1.\alpha_r & \cdots & \sum_{r=1}^n \alpha_r^k.1.\alpha_r^{n-1} \\ \sum_{r=1}^n \alpha_r^k.\alpha_r.1 & \sum_{r=1}^n \alpha_r^k.\alpha_r.\alpha_r & \cdots & \sum_{r=1}^n \alpha_r^k.\alpha_r.\alpha_r^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{r=1}^n \alpha_r^k.\alpha_r^{n-1}.1 & .\sum_{r=1}^n \alpha_r^k.\alpha_r^{n-1}.\alpha_r & \cdots & \sum_{r=1}^n \alpha_r^k.\alpha_r^{n-1}.\alpha_r^{n-1} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{r=1}^n \alpha^k & \sum_{r=1}^n \alpha_r^{k+1} & \cdots & \sum_{r=1}^n \alpha_r^{k+n-1} \\ \sum_{r=1}^n \alpha_r^{k+1} & \sum_{r=1}^n \alpha_r^{k+2} & \cdots & \sum_{r=1}^n \alpha_r^{k+n} \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{r=1}^n \alpha_r^{k+n-1} & \sum_{r=1}^n \alpha_r^{k+n} & \cdots & \sum_{r=1}^n \alpha_r^{k+2n-2} \end{pmatrix} \\
&= \begin{pmatrix} s_k & s_{k+1} & \cdots & s_{k+n-1} \\ s_{k+1} & s_{k+2} & \cdots & s_{k+n+1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{k+n-1} & s_{k+n} & \cdots & s_{k+2n-2} \end{pmatrix} \\
&= P_k.
\end{aligned}$$

De modo mais geral, tomemos qualquer $z \in K$. Segundo a base $\{1\ , \alpha\ , \alpha^2, ...,\ \alpha^{n-1}\}$, podemos escrever $z = \sum_{k=0}^{n-1} b_k \alpha^k$, onde $b_k \in F$. Assim, a matriz traço escalar q_z é a matriz de Hankel $\sum_{k=0}^{n-1} b_k P_k$. De fato,

$$\begin{aligned}
(B_q(\alpha^{i-1}, \alpha^{j-1})) &= (\mathrm{Tr}(z\alpha^{i-1}\alpha^{j-1})) \\
&= (\mathrm{Tr}(\sum_{k=0}^{n-1} b_k \alpha^k \alpha^{i-1} \alpha^{j-1})) \\
&= \sum_{k=0}^{n-1} b_k (\mathrm{Tr}(\alpha^k \alpha^{i-1} \alpha^{j-1})) \\
&= \sum_{k=0}^{n-1} b_k P_k.
\end{aligned}$$

Ou seja, a forma traço escalar é representada naturalmente por uma matriz de Hankel, que é uma combinação linear de matrizes P_k sobre F.

Vejamos agora um exemplo bem conhecido e muito utilizado na Teoria de Galois.

Exemplo 3.12. Seja p um número primo e seja $K = \mathbb{Q}(w)$, onde w é uma raiz p-ésima primitiva da unidade. Então $p(x) = x^{p-1} + x^{p-2} + ... + x^2 + x + 1$ é o polinômio minimal de w e $\mathbb{Q}(w) = \frac{\mathbb{Q}[x]}{(p(x))}$. Sabemos ainda que $[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$ e que $\{1, w, ..., w^{p-2}\}$ é base de $\mathbb{Q}(w)$ sobre $\mathbb{Q}$. Como w, $w^2, ..., w^{p-1}$ são as raízes de $p(x)$, os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(w)$ são dados por $\sigma_1(w) = w$, $\sigma_2(w) = w^2$, ..., $\sigma_{p-1}(w) = w^{p-1}$.

Vamos obter a matriz A que representa a forma traço em relação a base $\{1, w, ..., w^{p-1}\}$. Assim $(a_{ij}) = B(w^{i-1}, w^{j-1}) = \mathrm{Tr}(w^{i-1}w^{j-1})$. Logo,

$$\begin{aligned}
&B(1,1) = \mathrm{Tr}(1) = p - 1\\
&B(1,w) = \mathrm{Tr}(w) = w + w^2 + ... + w^{p-1} = -1\\
&\vdots\\
&B(1,w^{p-1}) = \mathrm{Tr}(w^{p-1}) = -1\\
&\vdots\\
&B(w,w^{p-1}) = \mathrm{Tr}(w^p) = \mathrm{Tr}(1) = p - 1\\
&\vdots\\
&B(w^{p-1},w^{p-1}) = -1.
\end{aligned}$$

Observe que além de $a_{11} = p-1$, teremos que $a_{ij} = p-1$ quando $i+j = p+2$, ou seja, $p-1$ vai ocorrer também na segunda linha diagonal abaixo da diagonal secundária. Logo, a forma traço de $\mathbb{Q}(w)$ sobre $\mathbb{Q}$ é representada pela matriz $(p-1) \times (p-1)$

$$\begin{pmatrix}
p-1 & -1 & -1 & \dots & & -1\\
-1 & \ddots & -1 & \dots & & -1\\
-1 & & \ddots & & & p-1\\
\vdots & & & p-1 & & -1\\
 & & & & \ddots & -1\\
-1 & -1 & p-1 & \dots & & -1
\end{pmatrix}.$$

Por outro lado, usando as identidades de Newton, é fácil ver que a soma de potências s_k das raízes $w, w^2, ..., w^{p-1}$ são:

$$\begin{aligned}
s_k &= p-1, \ \ se \ \ k \equiv 0 \ (\mathrm{mod}\ p);\\
s_k &= -1, \ \ \text{para todos os outros } k.
\end{aligned}$$

Assim, podemos ver que a matriz simétrica A é a matriz de Hankel P_0.

Vamos agora obter a matriz da forma traço escalar $q_w : \mathbb{Q}(w) \to \mathbb{Q}$, $q_w(x) = \mathrm{Tr}(wx^2)$, na mesma base anterior. Temos que

$$\begin{aligned}
&B(1,1) = \mathrm{Tr}(w) = -1\\
&B(1,w) = \mathrm{Tr}(w^2) = -1\\
&\vdots\\
&B(1,w^{p-1}) = \mathrm{Tr}(w^p) = p-1\\
&\vdots\\
&B(w,w^{p-1}) = \mathrm{Tr}(w^p.w) = \mathrm{Tr}(w) = -1\\
&\vdots\\
&B(w^{p-1},w^{p-1}) = -1.
\end{aligned}$$

Neste caso as entradas $p-1$ ocorrem na posição $(1,p-1)$ e quando $i+j = p+1$.

Ou seja, a matriz simétrica que representa a forma traço escalar q_w é

$$\begin{pmatrix}
-1 & -1 & -1 & \dots & -1\\
-1 & \ddots & & -1 & p-1\\
\vdots & & \ddots & p-1 & -1\\
 & & & \ddots & -1\\
-1 & p-1 & \dots & -1 & -1
\end{pmatrix}.$$

Observando as somas de potências s_k, temos que esta forma traço escalar é representada por P_1.

Capítulo 4

Invariantes de Formas Quadráticas por meio dos Menores Principais

Neste capítulo vamos estudar os menores principais de matrizes e a partir destes vamos encontrar diagonalizações para formas quadráticas regulares que nos ajudarão a estudar algoritmos para o cálculo da assinatura e do invariante de Hasse.

4.1 Os Menores Principais de Matrizes de Formas Quadráticas

Se a matriz que representa a forma quadrática não possuir muitos menores principais nulos, é possível obter uma diagonalização da mesma em função dos menores. Para o caso em que a matriz é de Hankel, não importa o número de menores nulos. Tudo isto mostraremos nesta seção.

Definição 4.1. Seja $A = (a_{ij})$ uma matriz $n \times n$ com entradas em F. Para cada inteiro k, $1 \leq k \leq n$, o $k-$*ésimo menor principal de* A é o determinante da matriz

$$A_k = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ \\ \vdots & & & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kk} \end{pmatrix}.$$

Denotaremos por D_k o k-ésimo menor principal de A. Observe que $D_n = \det\ A$.

Proposição 4.2. *Seja q uma forma quadrática regular representada por uma matriz simétrica A, com menores principais $D_1, ..., D_n$. Se cada $D_k \neq 0$, então existe uma diagonalização $q = \langle D_1, D_1D_2, D_2D_3, ..., D_{n-1}D_n \rangle$.*

Demonstração: A prova é dada por indução sobre n. Para $n = 1$ o resultado é óbvio. Assuma que o resultado é válido para $n-1$. Sabemos que A_{n-1} representa uma subforma q_{n-1} de q de dimensão $n-1$. Assim $q \cong q_{n-1} \perp \mu$, onde μ é uma forma 1-dimensional. Aplicando a indução assumida para q_{n-1}, temos

$$q_{n-1} = \langle D_1, D_1D_2, ..., D_{n-2}D_{n-1} \rangle$$

e calculando o determinante de q temos

$$D_n = D(q) = D_1D_1D_2D_2...D_{n-2}D_{n-2}D_{n-1}d(\mu)\dot{F}^2 = D_{n-1}d(\mu)\dot{F}^2.$$

Ou seja, $d(\mu) = D_{n-1}D_n\dot{F}^2$. Logo, $\mu \cong \langle D_{n-1}D_n \rangle$. Portanto,

$$q = \langle D_1, D_1D_2, D_2D_3, ..., D_{n-2}D_{n-1} \rangle \perp \langle D_{n-1}D_n \rangle. \ \square$$

O teorema que segue é fundamental para analisarmos os casos em que aparecem menores nulos.

Teorema 4.3. *Seja q uma forma quadrática regular representada pela matriz simétrica A, com menores principais $D_1, ..., D_n$. Suponha que existem inteiros i, j, k entre 1 e n, com $i < j < k$ tais que $D_j = 0$, mas D_i e D_k são não nulos. Sejam q_i e q_k subformas de q representadas por A_i e A_k. Então $q_k = q_i \perp \mu$, onde μ é uma forma regular isotrópica.*

Demonstração: Vamos escrever A_k da seguinte forma:

$$A_k = \begin{pmatrix} A_i & P^t \\ P & Q \end{pmatrix},$$

onde Q é o bloco $(k-i) \times (k-i)$ e P é o bloco $(k-i) \times i$. Observe que a matriz A_k é congruente a matriz $\begin{pmatrix} A_i & 0 \\ 0 & S \end{pmatrix}$, onde $S = Q - PA_i^{-1}P^t$. De fato,

$$\begin{pmatrix} I & 0 \\ -A_i^{-1}P^t & I \end{pmatrix} \cdot \begin{pmatrix} A_i & P^t \\ P & Q \end{pmatrix} \cdot \begin{pmatrix} I & -A_i^{-1}P^t \\ 0 & I \end{pmatrix} = \begin{pmatrix} A_i & 0 \\ 0 & S \end{pmatrix}.$$

Note que a congruência é via uma matriz triangular, então todos os menores principais são preservados. Assim, como $D_j = 0$ temos que o j-ésimo menor principal de $\begin{pmatrix} A_i & 0 \\ 0 & S \end{pmatrix}$ é zero. De $D_j = D_i \det S_{j-i} = 0$ e $D_i \neq 0$, temos $\det S_{j-i} = 0$. Logo, o $(j-i)$-ésimo menor principal de S é nulo.

Seja μ uma forma quadrática representada pela matriz S. Como $D_k = D_i \det S$ e $D_i \neq 0$, temos $\det S \neq 0$. Ou seja, μ é regular. Pelo ítem (5) da Proposição 1.17, temos que $q_k = q_i \perp \mu$, onde μ é uma forma isotrópica, uma vez que μ admite uma subforma não regular representada pela matriz S_{j-i}. $\square$

Lema 4.4. *(**Um Zero**) Seja q uma forma quadrática regular representada pela matriz simétrica A, com os menores principais $D_1, ..., D_n$. Suponha $D_k = 0$, para um valor de k com $1 \leq k < n$ e $D_j \neq 0$ para os demais índices, então*

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, D_{k+1}D_{k+2}, ..., D_{n-1}D_n \rangle.$$

Isto é, os dois termos da diagonalização envolvendo D_k são substituídos pelo plano hiperbólico $\langle 1, -1 \rangle$. Além disso, $D_{k-1} = -D_{k+1}$ em $\frac{\dot{F}}{\dot{F}^2}$.

Demonstração: Observe que D_{k-1}, D_{k+1} são não nulos e $D_k = 0$. Seja q_{k+1} a subforma regular de q representada por A_{k+1}. Do mesmo modo, seja q_{k-1} a subforma representada por A_{k-1}. Pelo Teorema 4.3, temos que $q_{k+1} = q_{k-1} \perp \mu$, onde μ é uma forma regular isotrópica. Observe que a dimensão de μ é dois, pois $k+1-(k-1) = 2$. Assim, usando o Teorema 1.26, temos $\mu \cong \langle 1, -1 \rangle$ e $d(\mu) = -1\dot{F}^2$. Pela Proposição 4.2, $q = q_{k+1} \perp \langle D_{k+1}D_{k+2}, ..., D_{n-1}D_n \rangle$. Ou seja, temos o resultado, uma vez que $q_{k+1} = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, -1, 1 \rangle$. Obtemos que $D_{k-1} = -D_{k+1}$ em $\frac{\dot{F}}{\dot{F}^2}$ calculando os determinantes na equação $q_{k+1} = q_{k-1} \perp \mu$. $\square$

Lema 4.5. *(**Dois Zeros**) Seja q uma forma quadrática regular representada pela matriz simétrica A com os menores principais $D_1, ..., D_n$. Suponha $D_k = D_{k+1} = 0$, para um valor de k com $1 \leq k < n-1$ e $D_j \neq 0$ para os demais índices. Então*

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, a, D_{k+2}D_{k+3}, ..., D_{n-1}D_n \rangle,$$

onde $a = -D_{k-1}D_{k+2}\dot{F}^2$. *Isto é, os três termos envolvendo* $D_k, D_k + 1$ *são substituídos por* $\langle 1, -1, a\rangle$.

Demonstração: Observe que $D_{k-1} \neq 0$ e $D_{k+2} \neq 0$, enquanto $D_k = D_{k+1} = 0$. Pelo Teorema 4.3, temos $q_{k+2} = q_{k-1} \perp \mu$, onde q_{k+2}, q_{k-1} são as subformas regulares de q representadas pelas matrizes simétricas A_{k+2}, A_{k-1}, respectivamente. Temos que μ é a subforma regular isotrópica de dimensão 3, já que $k + 2 - (k - 1) = 3$. Pelo Teorema 1.28 toda forma isotrópica contém um plano hiperbólico. Ou seja, $\mu \cong \langle 1, -1, a\rangle$. Calculando os determinantes na equação $q_{k+2} = q_{k-1} \perp \mu$ obtemos que $D_{k+2}\dot{F}^2 = D_{k-1}.(-a)\dot{F}^2$, logo $a = -D_{k-1}D_{k+2}.\dot{F}^2$. A diagonalização é obtida como no lema anterior substituindo q_{k+2} por $\langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, a\rangle$. □

Lema 4.6. ***(Três Zeros)*** *Seja* q *uma forma quadrática regular representada pela matriz simétrica* A, *com os menores principais* $D_1, ..., D_n$. *Suponha* $D_k = D_{k+1} = D_{k+2} = 0$, *para um valor de* k *com* $1 \leq k < n - 2$ *e* $D_j \neq 0$ *para os demais índices. Então*

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, a, b, D_{k+3}D_{k+4}, ..., D_{n-1}D_n\rangle,$$

onde $ab = -D_{k-1}D_{k+3}\dot{F}^2$. *Isto é, os quatro termos envolvendo* $D_k, D_k + 1, D_{k+2}$ *são substituídos por* $\langle 1, -1, a, b\rangle$, *para* $a, b \in F$ *satizfazendo a relação acima.*

Demonstração: Aplicando o Teorema 4.3 para este caso, obtemos $q_{k+3} = q_{k-1} \perp \mu$, onde q_{k+3}, q_{k-1} são como anteriormente e μ é uma subforma regular isotrópica de dimensão 4. Pelo Teorema 1.28 devemos ter $\mu \cong \langle 1, -1, a, b\rangle$. Calculando os determinantes na equação $q_{k+3} = q_{k-1} \perp \mu$ obtemos que $ab = -D_{k-1}D_{k+3}\dot{F}^2$. □

Se a forma quadrática for representada por uma matriz de Hankel, pode-se obter uma diagonalização da mesma a partir dos menores principais independente do número de menores nulos. É isto que nos mostra a proposição abaixo.

Na próxima proposição daremos apenas uma idéia da demonstração, tendo em vista que são necessários argumentos de teoria de matrizes que fogem um pouco dos objetivos desta dissertação.

Proposição 4.7. *Seja q uma forma quadrática regular representada por uma matriz de Hankel, com os menores principais $D_1, ..., D_n$. Suponha $D_k = D_{k+1} = ... = D_{k+s-1} = 0$ para k, s com $1 \leq k < n - s$ e $D_j \neq 0$ para os demais índices. Ou seja, temos s menores principais iguais a zero. Então*

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}\rangle \perp \mu \perp \langle D_{k+s}D_{k+s+1}, ..., D_{n-1}D_n\rangle,$$

onde $\dim \mu = s + 1$ *com μ hiperbólica caso s seja ímpar e $\mu = \langle 1, -1, ...1, -1, a\rangle$ para s par, onde $a = (-1)^{s/2}D_{k-1}D_{k+s}$.*

Idéia da demonstração: (ver [2] p 340-341, para uma demonstração mais detalhada)

Vamos escrever A_{k+s} como na demonstração do Teorema 4.3, isto é,

$$A_{k+s} = \begin{pmatrix} A_{k-1} & P^t \\ P & Q \end{pmatrix},$$

onde Q é o bloco $(s+1) \times (s+1)$ e P o bloco $(s+1) \times (k-1)$. Tomando a mesma congruência que foi usada no Teorema 4.3, temos que A_{k+s} é congruente a matriz $\begin{pmatrix} A_{k-1} & 0 \\ 0 & S \end{pmatrix}$, onde $S = Q - PA_{k-1}^{-1}P^t$. Usando o fato da congruência ser via uma matriz triangular, temos que todos os menores principais são preservados. Assim, como $D_k = D_{k+1} = ... = D_{k+s-1} = 0$, temos que os $(k + i - 1)$-ésimos menores principais de $\begin{pmatrix} A_{k-1} & 0 \\ 0 & S \end{pmatrix}$ são nulos, $i = 1, ..., s$. De $D_{k-1+i} = D_{k-1} \det S_i = 0$ e $D_{k-1} \neq 0$, temos $\det S_i = 0$, $i = 1, ..., s$. Logo os primeiros s menores principais de S são nulos.

O argumento de Frobenius, como exposto em (ver [2],pg.340-341), usa as propriedades das matrizes de Hankel para tirar mais conclusões sobre as matrizes S_i e concluir que μ tem índice de Witt maximal. Portanto μ possui o maior número possível de planos hiperbólicos. □

4.2 Cálculo dos Invariantes

Nesta seção vamos calcular a assinatura e o invariante de Hasse de uma forma quadrática por meio dos menores principais da matriz que a representa. Lembremos que estes cálculos não se aplicam para qualquer forma quadrática, pois estamos impondo algumas condições sobre os menores principais.

Cálculo da Assinatura

Seja q uma forma quadrática regular sobre um corpo formalmente real F. Seja $\text{sign}_P\,(q)$ a assinatura de q em uma ordem P de F como definida em 1.54. Lembremos do Teorema 1.53 que $n = \dim\, V = \dim\, V^+ + \dim\, V^-$. Assim, $\text{sign}_P\,(q) = \dim\, V^+ - \dim\, V^- = \dim\, V^+ + \dim\, V^- - 2\dim\, V^- = n - 2\dim\, V^-$. Vamos calcular $\dim\, V^-$ em cada um dos casos. Tomemos D_k, $k = 1, 2, ..., n$ como sendo os menores principais da matriz simétrica $n \times n$ que representa q e $D_0 = 1$. Chamemos de r o número de trocas de sinais na sequência de D_k's não nulos.

1^0 caso: Se cada $D_k \neq 0$, para todo k, então $\dim\, V^-$ é o número de trocas de sinal na sequência $D_0, D_1, ..., D_n$. De fato, como temos que $D_k \neq 0$, para todo $k = 1, ..., n$, segue da Proposição 4.2 que $q = \langle D_1, D_1D_2, ..., D_{n-1}D_n\rangle$. Observemos que cada elemento da diagonalização é negativo se, e somente se, apenas um dos fatores de D_iD_{i+1} for negativo, isto é, quando houver uma troca de sinal de D_i e D_{i+1}.

2^0 caso: Se um D_k é nulo, então $\dim\, V^-$ é o número de trocas de sinal da sequência $D_0, D_1, ..., D_{k-1}, D_{k+1}, ..., D_n$. De fato, pelo Lema 4.4 temos

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, -1, 1, D_{k+1}D_{k+2}, ..., D_{n-1}D_n\rangle,$$

onde $D_{k-1} = -D_{k+1}.\dot{F^2}$. Observemos que trocas de sinais na sequência $D_0, D_1, ..., D_{k-1}, D_{k+1}, ..., D_n$ nos fornece elementos negativos na diagonalização a menos da troca de sinal de D_{k-1} e D_{k+1} que não fornece negativo na diagonalização. Mas esta

troca é compensada pelo elemento $\langle -1 \rangle$. Portanto, $\dim V^-$ é o número de trocas de sinais na sequência acima.

3^0 caso: Se tivermos dois menores principais sucessivos nulos, isto é, $D_k = D_{k+1} = 0$, então pelo Lema 4.5

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, a, D_{k+2}D_{k+3}, ..., D_{n-1}D_n \rangle,$$

onde $a = -D_{k-1}D_{k+2}.\dot{F}^2$. Seguindo o mesmo raciocínio, deletamos D_k, D_{k+1} da sequência dos menores e contamos o número de trocas de sinal. Observe que se $D_{k-1}D_{k+2} > 0$, então significa que não houve troca de sinal entre D_{k-1} e D_{k+2} e assim temos que adicionar 2 no números de trocas para obtermos a dimensão de V^-, pois $\langle -1, a \rangle \subset V^-$. Logo $\dim V^- = r + 2$. Já no caso em que $D_{k-1}D_{k+2} < 0$, temos a troca de sinal entre D_{k-1} e D_{k+2} e que $\langle a \rangle \subset V^+$. Mas esta troca de sinal é compensada por $\langle -1 \rangle$. Portanto $\dim V^- = r$ quando $D_{k-1}D_{k+2} < 0$.

4^0 caso: Se tivermos $D_k = D_{k+1} = D_{k+2} = 0$, então pelo Lema 4.6

$$q = \langle D_1, D_1D_2, ..., 1, -1, a, b, D_{k+3}D_{k+4}, ..., D_{n-1}D_n \rangle,$$

onde $ab = -D_{k-1}D_{k+3}.\dot{F}^2$. Deletamos D_k, D_{k+1}, D_{k+2} da sequência dos menores e contamos o número de trocas de sinal do restante da sequência. Seguindo o mesmo raciocínio do 3^0 caso, se $D_{k-1}D_{k+3} > 0$, então $\dim V^- = r + 2$. Se $D_{k-1}D_{k+3} < 0$, então não há uma regra para calcularmos a assinatura, pois não temos como analizar o sinal de a e b na diagonalização.

5^0 caso: Tomemos D_k, $k = 1, 2, ...n$ como sendo os menores principais de uma matriz Hankel. Pela Proposição 4.7, temos que

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1} \rangle \perp \mu \perp \langle D_{k+s}D_{k+s+1}, ..., D_{n-1}D_n \rangle,$$

onde $\dim \mu = s+1$ com μ hiperbólica caso s seja ímpar e $\mu = \langle 1, -1, ...1, -1, a \rangle$ para s par, com $a = (-1)^{s/2}D_{k-1}D_{k+s}$. Assim, a $\dim V^-$ pode ser obtida pelo número

de trocas de sinais da sequência de menores não nulos adicionado da quantidade indicada em cada um dos casos abaixo:

- $s/2$, se $s \equiv 0 \,(\mathrm{mod}\ 4)$.

  Observe que se $s \equiv 0 \,(\mathrm{mod}\ 4)$, então o número de D_k's nulos é par, múltiplo de 4 e ainda $s/2 \equiv 0 \,(\mathrm{mod}\, 2)$ é par. Ou seja, o termo a que aparece na forma μ é positivo no caso em que $D_{k-1}D_{k+s}$ é positivo, e negativo no caso contrário. Mas neste último caso está havendo uma troca de sinal entre D_{k-1} e D_{k+s} que está compensando o sinal negativo de a. Sendo assim o número de elementos a ser adicionado é igual ao número de espaços hiperbólicos na forma μ. Portanto, $\dim V^- = r + s/2$.

- $(s + 2\varepsilon)/2$, se $s \equiv 2 \,(\mathrm{mod}\, 4)$, onde $\varepsilon = \begin{cases} 1, & \text{se } D_{k-1}D_{k+s} \text{ for positivo;} \\ -1, & \text{se } D_{k-1}D_{k+s} \text{ for negativo.} \end{cases}$

  Neste caso o número de D_k's nulos é par e $s/2 \equiv 1 (\mathrm{mod}\, 2)$, ou seja, $s/2$ é ímpar. Assim o sinal de a dependerá do sinal de $D_{k-1}D_{k+s}$. Analisemos um dos caso e o outro segue de modo análogo. Se $D_{k-1}D_{k+s}$ for positivo, então $\dim V^-$ é o número de trocas de sinais adicionado do número de planos hiperbólicos na forma μ mais um pela forma negativa $\langle a \rangle$, ou seja, $\dim V^- = (s + 2)/2$.

- $(s - 1)/2$, se $s \equiv 1 \,(\mathrm{mod}\, 4)$.

  Observe que se $s \equiv 1 \,(\mathrm{mod}\, 4)$, então $s - 1 \equiv 0 \,(\mathrm{mod}\, 4)$. Voltando ao primeiro caso analisado.

- $(s + 1)/2$, se $s \equiv 3 \,(\mathrm{mod}\, 4)$.

  Aqui temos que $s \equiv 3 \,(\mathrm{mod}\, 4)$, então $s - 3 \equiv 0 \,(\mathrm{mod}\, 4)$. Que nos leva a $s + 1 \equiv 0 \,(\mathrm{mod}\, 4)$, voltando ao primeiro caso.

Cálculo do Invariante de Hasse

Seja q uma forma quadrática sobre F e vamos assumir que q possua uma representação por uma matriz $n \times n$ para a qual cada menor principal $D_k \neq 0$, $k = 1, 2, ..., n$. Vamos então calcular o invariante de Hasse a partir da diagonalização $q = \langle D_1, D_1D_2, ..., D_{n-1}D_n \rangle$. Usando que em $Br(F)$, $[a, a] = [a, -1]$, $[a, b].[a, c] = [a, bc]$ e $[a, b]$ tem ordem 2, a maioria dos fatores se cancelam, restando

$$\begin{aligned} s(q) &= [D_1, D_1][D_1, D_2][D_2, D_2][D_2, D_3]...[D_{n-1}, D_{n-1}][D_{n-1}, D_n] \\ &= [D_1, -1][D_1, D_2][D_2, -1][D_2, D_3]...[D_{n-1}, -1][D_{n-1}, D_n] \\ &= [D_1, -D_2][D_2, -D_3]...[D_{n-1}, -D_n] \in B_r(F). \end{aligned}$$

Se um ou dois menores são nulos, basta aplicar a fórmula do resultado anterior para a sequência de menores principais excluindo os nulos, e depois, multiplicar por $[-1, -D_{k-1}D_{k+1}]$ se $D_k = 0$ e por $[-1, -D_{k-1}D_{k+2}]$ se $D_k = D_{k+1} = 0$. De fato, façamos para o caso de dois menores nulos e de modo análogo pode ser feito para um menor nulo. Pela Proposição 4.5 temos que

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, -D_{k-1}D_{k+2}, D_{k+2}D_{k+3}, ..., D_{n-1}D_n \rangle,$$

onde $a = -D_{k-1}D_{k+2}\dot{F}^2$. Calculando o invariante de Hasse de q obtemos

$$\begin{aligned} s(q) &= [D_1, -D_2][D_2, -D_3]...[D_{k-3}D_{k-2}, D_{k-2}D_n][D_{k-2}D_{k-1}, D_{k-1}D_n] \\ &\quad [-1, -D_{k-1}D_n][-D_{k-1}D_{k+2}, D_{k+2}D_n][D_{k+2}D_{k+3}, D_{k+3}D_n]...[D_{n-1}, -D_n] \\ &= [D_1, -D_2][D_2, -D_3]...[D_{k-2}, -D_{k-1}][D_{k-1}, -D_{k+2}][-1, -D_{k+1}] \\ &\quad [-1, D_{k+2}][D_{k+2}, D_{k+2}][D_{k+2}, D_{k+3}]...[D_{n-1}, -D_n] \\ &= [D_1, -D_2][D_2, -D_3]...[D_{k-2}, -D_{k-1}][D_{k-1}, -D_{k+2}] \\ &\quad [-1, -D_{k+1}D_{k+2}][D_{k+2}, -D_{k+3}]...[D_{n-1}, -D_n]. \end{aligned}$$

Se três sucessivos menores forem nulos, isto é, $D_k = D_{k+1} = D_{k+2} = 0$, então o algoritmo anterior para o cálculo do invariante de Hasse pode ser usado somente se

$-D_{k-1}D_{k+3} = 1\dot{F}^2$. De fato, pela Proposição 4.6 temos que

$$q = \langle D_1, D_1D_2, ..., D_{k-2}D_{k-1}, 1, -1, a, b, D_{k+3}D_{k+4}, ..., D_{n-1}D_n\rangle,$$

onde $ab = -D_{k-1}D_{k+3}\dot{F}^2$. Calculando o Invariante de Hasse de q como anteriormente obtemos

$$\begin{aligned} s(q) &= [D_1, -D_2][D_2, -D_3]...[D_{k-1}, -D_{k+3}][-1, -D_{k-1}D_{k+3}] \\ &\quad [a, b][D_{k+3}, -D_{k+4}]...[D_{n-1}, D_n]. \end{aligned}$$

Note que $(\frac{a,b}{F})$ se fatora se, e somente se, $D_{k-1}D_{k+3} = 1\dot{F}^2$. Assim obtemos a afirmação.

Cálculo dos Invariantes da Forma Traço Escalar

Seja K uma extensão de corpos separável finita de grau n do corpo F, logo $K = F[\alpha]$ para $\alpha \in K$. Tomemos $z \in K$, e consideremos a forma traço escalar $q_z : K \to F$, $q_z(x) = \mathrm{Tr}(zx^2)$. Sabemos que $z = b_0 + b_1\alpha + ... + b_n\alpha^{n-1}$, para $b_i \in K$.

Podemos calcular o invariante de Hasse e a assinatura de q_z seguindo o procedimento abaixo.

(1) Usemos as identidades de Newton para calcular as somas de potências s_k e escrevamos a matriz P_k $n \times n$, $k = 1, ..., n$;

(2) Usando $z = \sum_0^{n-1} b_k\alpha^k$ onde $b_k \in F$, escrevamos a matriz de Hankel $\sum_{k=0}^{n-1} b_kP_k$ que representa a forma traço escalar q_z;

(3) Calculemos os menores principais D_k's para a matriz de Hankel em **(2)** para escrever a diagonalização de q_z conforme a Proposição 4.7;

(4) Calcule a assinatura e o invariante de Hasse de q_z pela diagonalização em **(3)**.

4.3 Exemplos

Nesta seção vamos trabalhar com alguns exemplos para colocarmos em prática os resultados vistos neste capítulo.

Exemplo 4.8. Seja $K = F(\alpha^{1/m})$, uma extensão radical simples do corpo F, onde $\alpha \in F$, m é um inteiro positivo e $x^m - \alpha$ é irredutível sobre F. Vamos assumir que a característica de F não divide m e calcular a assinatura e o invariante de Hasse da forma traço q de K sobre F.

(1) Usando as identidade de Newton obtemos que

$$\begin{aligned} s_0 &= m; \\ s_j &= 0 \text{ para } 1 \leq j \leq m-1 \\ s_m &= m\alpha. \end{aligned}$$

(2) A matriz de Hankel P_0 representa a forma traço q de K sobre F, ou seja,

$$M_q = \begin{pmatrix} m & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & m\alpha \\ 0 & 0 & \cdots & m\alpha & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & m\alpha & \cdots & 0 & 0 \end{pmatrix}.$$

(3) Os menores principais são

$$\begin{aligned} D_1 &= m; \\ D_j &= 0 \text{ para } 2 \leq j \leq m-1; \\ D_m &= (-1)^t \alpha^m m^{m-1} \text{ onde } t = \begin{cases} (m\text{-}1)/2, & \text{para } m \text{ ímpar ;} \\ (m\text{-}2)/2, & \text{para } m \text{ par.} \end{cases} \end{aligned}$$

Então $D_m = (-1)^t \alpha . \dot{F^2}$ para m ímpar e $D_m = (-1)^t m \dot{F^2}$ para m par. Vamos calcular as diagonalizações a partir dos menores calculados para q nos dois casos:

<u>1^0caso:</u> m **par**

Sendo m par temos um número par de D_k's nulos, já que o número de D_k's nulos é $m-2$. Pela Proposição 4.7 temos que $q = \langle D_1, 1, -1, ..., 1, -1, (-1)^{(m-2)/2} D_1 D_m \rangle$.

Temos que $(-1)^{(m-2)/2}D_1D_m = (-1)^{(m-2)/2}m(-1)^{(m-2)/2}\alpha\dot{F}^2 = m\alpha\dot{F}^2$. Logo

$$q = \langle m, 1, -1, ..., 1, -1, m\alpha\rangle, \text{ para } m \text{ par.}$$

$\underline{2^0\text{caso:}}$ m **ímpar**

Sendo m ímpar temos um número ímpar de D_k's nulos. Pela Proposição 4.7 temos que $q = \langle D_1, 1, -1, ..., 1, -1\rangle$. Assim

$$q = \langle m, 1, -1, ..., 1, -1\rangle.$$

(4) Se F é formalmente real, então a assinatura em qualquer ordem P de F é

$$\text{sign}_P(q) = 1, \text{ se } m \text{ é ímpar;}$$

$$\text{sign}_P(q) = 1 + \text{sign}_\text{P}(\langle\alpha\rangle), \text{ se } m \text{ é par.}$$

O invariante de Hasse de q é dado por

$$s(q) = [m, (-1)^{(m-1)/2}][-1, (-1)^{(m-1)(m-3)/8}] \in Br(F) \text{ para } m \text{ ímpar;}$$

$$s(q) = [m, -\alpha][\alpha, (-1)^{(m-2)/2}][-1, (-1)^{(m-2)(m-4)/8}] \in Br(F) \text{ para } m \text{ par,}$$

usamos aqui o fato que $[1, a] = 1$ em $Br(F)$, para todo $a \in F$. Usando congruências e as propriedades de álgebras de quatérnios, obtemos

$$\begin{aligned}
s(q) &= 1 \text{ se } m \equiv 1 \pmod 8;\\
s(q) &= [m, -1] \text{ se } m \equiv 3 \pmod 8;\\
s(q) &= [-1, -1] \text{ se } m \equiv 5 \pmod 8;\\
s(q) &= [-m, -1] \text{ se } m \equiv 7 \pmod 8;\\
s(q) &= [-m, -\alpha] \text{ se } m \equiv 0 \pmod 8;\\
s(q) &= [m, -\alpha] \text{ se } m \equiv 2 \pmod 8;\\
s(q) &= [-m, -\alpha][-1, -1] \text{ se } m \equiv 4 \pmod 8;\\
s(q) &= [m, -\alpha][-1, -1] \text{ se } m \equiv 6 \pmod 8
\end{aligned}$$

De fato, façamos para um dos casos e os outros seguem de modo análogo. Se $m \equiv 3 \pmod 8$, então m é ímpar, $\frac{m-1}{2} \equiv 1 \pmod 4$ é ímpar e $\frac{m-3}{4} \equiv 0 \pmod 4$ é par. Assim

$$s(q) = [m, -1][-1, 1] = [m, -1].$$

Exemplo 4.9. Seja a e b elementos de um corpo F e seja $n \in \mathbb{Z}$, $n > 1$. Considere o polinômio $p(x) = x^n + ax + b$. Vamos supor que este polinômio seja irredutível e separável sobre F, então $F[x]/(p(x))$ é uma extensão separável de F. Seja q a forma traço de $F[x]/(p(x))$ sobre F. Vamos calcular a assinatura e o invariante de Hasse de q.

(1) Temos que $s_0 = \sum_n^n \alpha_i^0 = n$. Usando as identidades de Newton, obtemos os demais s_k como segue

$s_1 + c_1 1 = 0 \Rightarrow s_1 = 0$;

$s_2 + c_1 s_1 + c_2.2 = 0 \Rightarrow s_2 = 0$;

$\vdots$

$s_{n-2} + c_1 s_{n-3} + c_2 s_{n-4} + ... + c_{n-2}(n-2) = 0 \Rightarrow s_{n-2} = 0$

$s_{n-1} + c_1 s_{n-2} + c_2 s_{n-3} + ... + c_{n-1}(n-1) = 0 \Rightarrow s_{n-1} = (1-n)a$

$s_n + c_1 s_{n-1} + c_2 s_{n-2} + ... + c_n s_0 = 0 \Rightarrow s_n = -bn$

$s_{n+1} + c_1 s_n + c_2 s_{n-1} + ... + c_n s_1 = 0 \Rightarrow s_{n+1} = 0$

$\vdots$

$s_{2n-3} + c_1 s_{2n-2} + c_2 s_{2n-1} + ... + c_n s_{n-3} = 0 \Rightarrow s_{2n-3} = 0$

$s_{2n-2} + c_1 s_{2n-1} + c_2 s_{2n} + ... + c_n s_{n-2} = 0 \Rightarrow s_{2n-2} = (n-1)a^2$.

Como a matriz de Hankel P_0 representa a forma traço, não precisamos das somas de potências com $k > 2n-2$.

(2) A forma traço q é representada pela matriz de Hankel P_0, ou seja,

$$\begin{pmatrix} n & 0 & \cdots & 0 & (1-n)a \\ 0 & 0 & \cdots & (1-n)a & -nb \\ 0 & 0 & \cdots & -nb & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ (1-n)a & -nb & \cdots & 0 & (n-1)a^2 \end{pmatrix}.$$

(3) Calculando os menores principais obtemos

$$\begin{aligned}
D_1 &= n;\\
D_j &= 0, \text{para } 2 \leq j \leq n-2;\\
D_{n-1} &= (-1)^s n(1-n)^{n-2}a^{n-2}, \text{ onde } s = \begin{cases} (n\text{-}2)/2, & \text{para } n \text{ par;} \\ (n\text{-}3)/2, & \text{para } n \text{ ímpar.} \end{cases}\\
D_n &= \begin{cases} (\text{-}1)^{n/2}[n^n b^{n-1} - (n-1)^{n-1}a^n], & \text{para } n \text{ par;} \\ (\text{-}1)^{n/2}[n^n b^{n-1} + (n-1)^{n-1}a^n], & \text{para } n \text{ ímpar.} \end{cases}
\end{aligned}$$

Vamos denotar $D_n = \delta$ para simplificar a escrita. Vamos assumir que a característica de F não divide n ou $n-1$. A partir dos menores calculados vamos encontrar uma diagonalização para q nos seguintes casos:

<u>1^0caso</u> n **par**

Sendo n par temos que o número de D_k nulos é ímpar, já que o número de D_k nulos é $n-3$. Pela Proposição 4.7 temos que $q = \langle D_1, 1, -1, ..., 1, -1, D_{n-1}D_n\rangle$. O cálculo de

$$\begin{aligned}
D_{n-1}D_n &= (-1)^{(n-2)/2}n(1-n)^{n-2}a^{n-2}\delta\dot{F}^2\\
&= (-1)^{(n-2)/2}n\delta\dot{F}^2
\end{aligned}$$

nos fornece $q = \langle n, 1, -1, ..., 1, -1, (-1)^{(n-2)/2}n\delta\rangle$;

<u>2^0caso</u> n **ímpar**

Sendo n ímpar temos que o número de D_k nulos é par. Pela Proposição 4.7 temos que $q = \langle D_1, 1, -1, ..., 1, -1, (-1)^{(n-3)/2}D_1D_{n-1}, D_{n-1}D_n\rangle$. Mas

$$\begin{aligned}
(-1)^{(n-3)/2}D_1D_{n-1} &= (-1)^{(n-3)/2}n(-1)^{(n-3)/2}n(1-n)^{n-2}a^{n-2}\dot{F}^2\\
&= (1-n)a\dot{F}^2, \text{ e}\\
D_{n-1}D_n &= n(-1)^{(n-3)/2}n(1-n)^{n-2}a^{n-2}\dot{F}^2\\
&= (-1)^{(n-3)/2}n(1-n)\delta\dot{F}^2,
\end{aligned}$$

logo $q = \langle n, 1, -1, ..., 1, -1, (1-n)a, (-1)^{(n-3)/2}n(1-n)\delta\rangle$.

(4) Se F é formalmente real então a assinatura em qualquer ordem P de F é dada por

$$\text{sign}_P(q) = 1 + (-1)^{(n-2)/2}\text{sign}_P\langle\delta\rangle, \text{ para } n \text{ par;}$$

$$\text{sign}_P(q) = 1 + \text{sign}_P\langle(1-n)a\rangle + (-1)^{(n-3)/2}\text{sign}_P\langle\delta\rangle, \text{ para } n \text{ ímpar.}$$

Usando as propriedades de álgebras de quatérnios, o invariante de Hasse de q é dado por

$$\begin{aligned}
s(q) &= [-n, -\delta] \text{ se } n \equiv 0 \pmod 8;\\
s(q) &= [n, \delta] \text{ se } n \equiv 2 \pmod 8;\\
s(q) &= [-n, -\delta][-1, -1] \text{ se } n \equiv 4 \pmod 8;\\
s(q) &= [n, \delta][-1, -1] \text{ se } n \equiv 6 \pmod 8;\\
s(q) &= [1-n, \delta] \text{ se } n \equiv 1 \pmod 8;\\
s(q) &= [n-1, -\delta] \text{ se } n \equiv 3 \pmod 8;\\
s(q) &= [1-n, \delta][-1, -1] \text{ se } n \equiv 5 \pmod 8;\\
s(q) &= [n-1, -\delta][-1, -1] \text{ se } n \equiv 7 \pmod 8.
\end{aligned}$$

Capítulo 5

Apêndice

5.1 Produto Tensorial

Sejam U e V espaços vetoriais sobre um corpo F e K o F-espaço vetorial que tem por base o conjunto $U \times V$. Assim um elemento de K é da forma

$$x = \sum_{i=1}^{r} \lambda(u_i, v_i), u_i \in U, v_i \in V \text{ e } \lambda_i \in F.$$

Considere K_1 o subespaço vetorial de K gerado pelos elementos das formas:

(1) $(u + u', v) - (u, v) - (u', v)$;

(2) $(u, v + v') - (u, v) - (u, v')$;

(3) $(\lambda u, v) - \lambda(u, v)$;

(4) $(u, \lambda v) - \lambda(u, v)$, onde $u, u' \in U$, $v, v' \in V$ e $\lambda \in F$.

Definição 5.1. O espaço quociente $\frac{K}{K_1}$ é chamado de *produto tensorial de U por V*, denotado $U \otimes V$. As classes $(u, v) + K_1$ serão denotadas por $u \otimes v$.

Note que um elemento de $U \otimes V$ é da forma

$$\overline{x} = \sum_{i=1}^{r} \lambda_i(u_i \otimes v_i), u_i \in U, v_i \in V \text{ e } \lambda_i \in F.$$

O conjunto $\{u \otimes v : u \in U, v \in V\}$ é uma derador de de $U \otimes V$ sobre V.

Lema 5.2. *Os geradores de $U \otimes V$ satisfazem:*

(1) $(u + u') \otimes v = u \otimes v + u' \otimes v$;

(2) $u \otimes (v + v') = u \otimes v + u \otimes v'$;

(3) $(\lambda u) \otimes v = \lambda(u \otimes v)$;

(4) $u \otimes (\lambda v) = \lambda(u \otimes v)$, *onde* $u, u' \in U$, $v, v' \in V$ *e* $\lambda \in F$.

Demonstração: (1) Queremos mostrar que $(u + u', v) + K_1 = [(u, v) + K_1] + [(u', v) + K_1]$. Por construção temos que $(u + u', v) - (u, v) - (u', v) \in K_1$. Logo, $[(u+u', v)-(u, v)-(u', v)]+K_1 = K_1 = 0 \in \frac{K}{K_1}$, ou seja, $[(u+u', v)+K_1]-[(u, v)+K_1]-[(u', v)+K_1] = 0$. Portanto, $[(u + u', v) + K_1] = [(u, v) + K_1] + [(u', v) + K_1]$, isto é, $(u + u') \otimes v = u \otimes v + u' \otimes v$.

A demonstração de **(2)**,**(3)** e **(4)** são análogas. □

Observação 5.3. (1) $u \otimes 0 = 0 \otimes v = 0 \otimes 0 = 0$, para todo $u \in U$ e $v \in V$.
(2) $-(u \otimes v) = (-u) \otimes v$, para todo $u \in U$ e $v \in V$.

Definição 5.4. Sejam U, V e W espaços vetoriais sobre F. Uma *aplicação linear mediana de $U \times V$ em W* é uma aplicação $F : U \times V \to W$ tal que

(1) $F(u_1 + u_2, v) = F(u_1, v) + F(u_2, v)$;

(2) $F(u, v_1 + v_2) = F(u, v_1) + F(u, u_2)$;

(3) $F(\lambda u, v) = \lambda F(u, v) = F(u, \lambda v)$, onde $u, u_1, u_2 \in U$, $v, v_1, v_2 \in V$ e $\lambda \in F$.

A aplicação $i : U \times V \to U \otimes V$ é linear mediana e é chamada aplicação linear mediana canônica.

Teorema 5.5. *Sejam U, V, W espaços vetorias sobre um corpo F. Se $g : U \times V \to W$ é uma aplicação linear mediana, então existe uma única tranformação linear $\bar{g} : U \otimes V \to W$ tal que $\bar{g} \circ i = g$, onde $i : U \times V \to U \otimes V$ é a aplicação linear mediana canônica. O espaço vetorial $U \otimes V$ é unicamente determinado a menos de isomorfismo por esta propriedade (chamada propriedade universal).*

Demonstração: Sejam K o espaço vetorial sobre F com base $U \times V$ e K_1 o subespaço vetorial descrito na definição de $U \otimes V$. A aplicação $(u, v) \to g(u, v)$ induz uma transformação linear $g_1 : K \to W$, basta estender por linearidade.

Afirmação $g_1(K_1) = 0$. Basta mostrar que g_1 leva os geradores de K_1 em 0.

$$\begin{aligned} g_1((u+u', v) - (u, v) - (u', v)) &= g_1(u+u', v) - g_1(u, v) - g_1(u', v) \\ &= g(u+u', v) - g(u, v) - g(u', v) \\ &= g(u, v) + g(u', v) - g(u, v) - g(u', v) = 0. \end{aligned}$$

Analogamente para os demais geradores. Segue que $K_1 \subset \text{Ker } g_1$, logo g_1 induz uma tranformação linear $\bar{g} : \frac{K}{K_1} \to W$ dada por $\bar{g}[(u, v) + K_1] = g_1(u, v) = g(u, v)$. Mas $\frac{K}{K_1} = U \otimes V$ e $(u, v) + K_1 = u \otimes v$. Logo $\bar{g} : U \otimes V \to W$ é uma tranformação linear tal que $\bar{g} \circ i(u, v) = \bar{g}(u \otimes v) = g(u, v)$ para todo $(u, v) \in U \times V$. Portanto $\bar{g} \circ i = g$.

Vamos agora mostrar que $\bar{g}$ é única. Suponha que exista $h : U \otimes V \to W$ uma tranformação linear tal que $h \circ i = g$. Assim $h(u \otimes v) = h \circ i(u, v) = g(u, v) = \bar{g} \circ i(u, v) = \bar{g}(u \otimes v)$. Como h e $\bar{g}$ coincidem nos geradores de $U \otimes V$, devemos ter que $h = \bar{g}$. Portanto $\bar{g}$ é única.

Para mostrarmos a última afirmação, suponhamos que existam dois espaços vetoriais $U \otimes_1 V$ e $U \otimes_2 V$. Logo existem duas aplicações bilineares canônicas $i_1 : U \times V \to U \otimes_1 V$ e $i_2 : U \times V \to U \otimes_2 V$. Aplicando o teorema para i_1 no lugar de g e $U \otimes_1 V$ no lugar de W obtemos que existe uma única transformação linear $\bar{i_1} : U \otimes_2 V \to U \otimes_1 V$ tal que $\bar{i_1} \circ i_2 = i_1$ (estendemos i_1 para $U \otimes_2 V$). Analogamente obtemos que existe uma única tranformação linear $\bar{i_2} : U \otimes_1 V \to U \otimes_2 V$ tal que

$\bar{i_2} \circ i_1 = i_2$. Compondo obtemos uma transformação linear $\bar{i_1} \circ \bar{i_2} : U \otimes_1 V \to U \otimes_1 V$. Note que $\bar{i_1} \circ \bar{i_2} \circ i_1 = \bar{i_1} \circ i_2 = i_1$. Porém se aplicarmos o teorema para $g = i_1$ e $W = U \otimes_1 V$ e agora estendermos para $U \otimes_1 V$ obteremos que existe uma única transformação linear $T : U \otimes_1 V \to U \otimes_1 V$ tal que $T \circ i_1 = i_1$. Mas obviamente $Id_1 : U \otimes_1 V \to U \otimes_1 V$ é esta única transformação linear. Logo $\bar{i_1} \circ \bar{i_2} = Id_1$. Analogamente mostra-se que $\bar{i_2} \circ i_1 = Id_2$. Portanto $U \otimes_2 V \simeq U \otimes_1 V$. $\square$

Bibliografia

[1] FROBENIUS, G.: **Ueber die Transformation einer quadratischen Formen**. J. Reine Angew Math, 114, 187-230, 1895.

[2] GANTMACHER, F. R.: **Matrix theory Vol 1**. New york, Chelsea Publilshing, 1959.

[3] GUNDELFINGER, S.: **Ueber die Transformation einer quadratischen Form in einer Summe von Quadraten**. J.Reine Angew, Math 91, 221-237, 1881.

[4] HUNGERFORD, T. W.: **Algebra**. New York: 1974. (Springer-Verlag).

[5] JACOBSON, N.: **Basic Algebra I**. New York: Freeman W. H. and Company,1996.

[6] JACOBI, C. G. J.: **Ueber eine elementare Transformation eines in Bezug auf jedes von zwei Variablen-Systemen linearen und homogen Ausdrucks**. J. Reine Angew, Math 53, 265-270, 1857.

[7] JONES, B. W.: **The arithmetic theory of quadratic forms**. Carus Math, Monographs 10, Wiley, 1950.

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

[9] LEWIS D.W. .: **Hankel Matrices and Quadratic Forms**. Ireland:1996. (Department of Mathmatics, University College Dublin).

[10] SCHARLAU, W.: **Quadratic and Hermitian forms**. New York: B.Heidelberg, 1985 J. (Springer-Verlag) .

[11] SYLVESTER, J.: **A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real ortogonal substitution to the of sum of positive and negative squares**. Philosophical Magazine 15, 138-142, 1852.

[12] THOMPSON, R. C.: **Principal submatrices V; Some results concerning principal submatrices of arbitrary matrices**. Res. Nat.Bureau of Standards Sect. B, 72B, 115-125, 1968.