

Patrícia Beck Begnossi

# Formas Quadráticas e Extensões de Ordens

1910001168



# Formas Quadráticas e Extensões de Ordens

Patrícia Beck Begnossi

Orientador: Prof. Dr. Clotilzio Moreira dos Santos

Dissertação apresentada ao Departamento de  
Matemática - IBILCE - UNESP, como parte dos  
requisitos para obtenção do título de Mestre em  
Ciências Matemáticas – área de concentração:  
Matemática.

São José do Rio Preto – SP

Fevereiro - 2003



*t.1.168/03*

511.4  
B417P

10101039

Begnossi, Patrícia Beck.

Formas quadráticas e extensões de ordens / Patrícia Beck Begnossi. –  
São José do Rio Preto : [s.n.], 2003  
64 f. ; 30 cm.

Orientador: Clotilzio Moreira dos Santos

Dissertação (mestrado) – Universidade Estadual Paulista. Instituto de  
Biociências, Letras e Ciências Exatas

I. Formas quadráticas. I. Santos, Clotilzio Moreira dos. II.  
Universidade Estadual Paulista. Instituto de Biociências, Letras e  
Ciências Exatas. III. Título.

CDU – 511.55



“Pois que se uniu a mim,  
eu o livrarei; E o protegerei,  
pois conhece o meu nome.  
Quando me invocar, eu o atenderei,  
na tribulação estarei  
com ele; E o cobrirei de glórias.”

*Salmos, 90, 14-15*



## Agradecimentos

Aos meus pais,  
Carlos e Aparecida,  
e ao meu esposo, Ronaldo,  
dedico.

## Agradecimentos

Ao término deste trabalho deixo aqui meus sinceros agradecimentos:

A Deus, que, incomparável e inconfundível na sua infinita bondade, compreendeu meus anseios e me deu a força necessária para atingir meu objetivo.

Ao Prof. Dr. Clotilzio Moreira dos Santos, pela amizade, paciência, dedicação e pela preciosa orientação tanto para a conclusão deste, quanto para vida.

Aos meus pais, por revestirem minha vida de amor, carinho e dedicação, pela ajuda e incentivo em tudo aquilo que desejei realizar.

Ao meu esposo Ronaldo, pela compreensão na ausência, pela confiança, pelo carinho e estímulo dedicados em tudo que já vivemos.

Aos meus irmãos: Chrys, André e Dani, pelo incentivo e carinho durante este trabalho e pelo sempre presente apoio emocional e espiritual.

A todos os colegas do Curso de Mestrado, pelo companheirismo, especialmente ao meu grande amigo Rodrigo, pelos momentos de descontração e angústia que compartilhamos.

À Rita, com quem pude dividir sonhos, anseios, problemas e alegrias. Pelo incentivo, orações... enfim, pela verdadeira amizade.

A todos professores do IBILCE, pela formação.

À FAPESP, pelo apoio financeiro.



# Conteúdo

|          |                                                                             |           |
|----------|-----------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Formas Quadráticas e Espaços Quadráticos</b>                             | <b>2</b>  |
| 1.1      | Formas Quadráticas . . . . .                                                | 2         |
| 1.2      | Diagonalização de Formas Quadráticas . . . . .                              | 5         |
| 1.3      | Isotropia, Plano Hiperbólico e Decomposição de Formas Quadráticas . . . . . | 8         |
| 1.4      | Produto de Kronecker de Espaços Quadráticos. . . . .                        | 14        |
| <b>2</b> | <b>Anel de Witt</b>                                                         | <b>16</b> |
| 2.1      | Construção do Anel de Witt . . . . .                                        | 16        |
| 2.2      | Anéis de Witt de Alguns Corpos . . . . .                                    | 19        |
| <b>3</b> | <b>Formas Quadráticas Sobre Extensões Algébricas</b>                        | <b>22</b> |
| 3.1      | Transfer de Scharlau . . . . .                                              | 22        |
| 3.2      | Extensões Quadráticas . . . . .                                             | 28        |
| <b>4</b> | <b>Corpos Formalmente Reais e Reais Fechados</b>                            | <b>31</b> |
| 4.1      | Corpos Ordenados . . . . .                                                  | 31        |



|          |                                            |           |
|----------|--------------------------------------------|-----------|
| 4.2      | Corpos Reais Fechados . . . . .            | 35        |
| 4.3      | O Espectro Primo do Anel de Witt . . . . . | 41        |
| <b>5</b> | <b>Extensões de Assinaturas</b>            | <b>46</b> |
| 5.1      | Extensões de Assinaturas . . . . .         | 46        |
| <b>6</b> | <b>O Espaço das Ordens de um Corpo</b>     | <b>57</b> |
| 6.1      | O Espaço das Ordens de um Corpo . . . . .  | 57        |

# Capítulo 1

## Formas Quadráticas e Espaços Quadráticos

### 1.1 Formas Quadráticas

Em todo o contexto  $V$  denotará um espaço vetorial de dimensão finita sobre um corpo  $F$  de característica diferente de dois.

Uma *forma quadrática* ( $n$ -dimensional) sobre  $F$  é uma função  $q : V \rightarrow F$ , (onde  $\dim_F V = n$ ) tal que

(i)  $q(\alpha u) = \alpha^2 q(u)$ ,  $\forall \alpha \in F$  e  $\forall u \in V$  e a função

(ii)  $b_q : V \times V \rightarrow F$ , definida por  $b_q(u, v) = \frac{1}{2}(q(u+v) - q(u) - q(v))$  é uma forma bilinear simétrica.

O par  $(V, q)$  é dito *espaço quadrático* ( $n$ -dimensional) sobre  $F$  e  $b_q$  é dita a *forma bilinear associada a  $q$* .





Se  $b$  é uma forma bilinear definida sobre  $F$ , podemos verificar que  $q_b : V \rightarrow F$  dada por  $q_b(u) = b(u, u)$ , é uma forma quadrática tal que  $b_{q_b} = b$ . Dada uma forma quadrática  $q$ , por verificação imediata temos que  $q_{b_q} = q$ . Portanto o fato da característica de  $F$  ser diferente de dois, temos uma correspondência um-a-um entre as formas quadráticas e as formas bilineares definidas sobre  $F$ .

Dois espaços quadráticos  $(V, q)$  e  $(V_1, q_1)$  sobre um corpo  $F$  são *isométricos* e denotamos  $(V, q) \simeq (V_1, q_1)$  ou simplesmente  $q \simeq q_1$ , se existir um isomorfismo de espaços vetoriais  $\sigma : V \rightarrow V_1$  tal que  $q = q_1 \circ \sigma$ . Esta relação é de equivalência e podemos checar facilmente que  $q = q_1 \circ \sigma$  (ou  $q \simeq q_1$ ) se, e somente se,  $b_q(u, v) = b_{q_1}(\sigma(u), \sigma(v))$ .

Se  $q$  é uma forma quadrática definida de  $V$  em  $F$  e  $B = \{e_i\}_{i=1}^n$  é uma base de  $V$ , seja  $M_q = (b_q(e_i, e_j))$ , onde  $b$  é a forma bilinear associada a  $q$ . A existência de um isomorfismo  $\sigma : V \xrightarrow{\sim} V_1$  tal que  $q = q_1 \circ \sigma$ , equivale a existir  $C \in GL_n(F)$  ( $C$  é a matriz de  $\sigma$  em bases de  $V$  e  $V_1$  fixadas) tal que  $M_q = C^t M_{q_1} C$ . Portanto existe uma correspondência um-a-um entre as classes de isometrias das formas quadráticas sobre  $F$  e a classe de semelhança de matrizes de  $M_n(F)$ . Em outras palavras, dois espaços quadráticos  $(V, q)$  e  $(V_1, q_1)$  são isométricos se, e somente se, suas matrizes  $M_q$  e  $M_{q_1}$  (com relação a bases fixadas) são congruentes. A classe de semelhança de  $M_q$  é dita *matriz* da forma quadrática  $q$  ou de sua classe de isometria. Notemos ainda que o determinante de  $M_q$  e de  $M_{q_1}$  diferem pelo fator quadrático  $\det(C)^2$ . Portanto definimos o *determinante da forma quadrática*  $q$  como sendo o elemento  $d(q) = \det(M_q) \in \frac{F}{F^2}$ . Isto já mostra que o grupo  $\frac{F}{F^2}$  desempenhará um papel importante na teoria de formas quadráticas.

Da teoria de álgebra linear temos:

**Proposição 1.1.1** *Seja  $(V, q)$  um espaço quadrático sobre um corpo  $F$ . Então as proposições abaixo são equivalentes:*

1.  $M = (b_q(e_i, e_j))$  é não singular.
2. A aplicação  $\delta : V \rightarrow V^*$ ,  $\delta(x) = b_q(\cdot, x)$  é um isomorfismo.

3. Para  $x \in V$ ,  $b_q(x, y) = 0$ ;  $\forall y \in V$  implica que  $x = 0$ .

Dizemos que um espaço quadrático  $(V, q)$ , ou a forma quadrática  $q$  é *não singular* ou *regular*, ou ainda *não degenerado(a)* se o espaço quadrático  $(V, q)$  satisfaz uma das (portanto todas) condições equivalentes da proposição anterior. A menos da forma quadrática nula ( $q : \{0\} \rightarrow F$ ), em todo o texto serão consideradas apenas estes tipos de formas quadráticas. Portanto o termo espaço quadrático ou forma quadrática significará, respectivamente, espaço quadrático não singular ou forma quadrática não singular.

### Exemplo (1)

Sejam  $V$  um espaço vetorial de dimensão 2 sobre  $F$  e  $q, q_1 : V \rightarrow F$  definidas por  $q(x, y) = x^2 - y^2$  e  $q_1(x, y) = xy$ . Então  $\sigma(x, y) = (x + y, x - y)$  nos dá a isometria  $q \simeq q_1$ .

$$\text{Temos que } M_q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad M_{q_1} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \text{ e } C_{Can} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Assim  $M_q = C_{Can} M_{q_1} C_{Can}$ .

Sejam  $u, v \in V$ , onde  $(V, q)$  é um espaço quadrático. Se  $b_q(u, v) = 0$  dizemos que os vetores  $u, v \in V$  são *ortogonais*. Além disso, se  $U$  e  $W$  são subconjuntos de  $V$  e  $b(U, W) = 0$ , ou seja,  $b(u, w) = 0$  para todos  $u \in U, w \in W$ , também dizemos que  $U$  e  $W$  são *ortogonais*. A ortogonalidade será denotada por  $\perp$ . Assim  $u \perp v$  e  $U \perp W$ .

A cada subconjunto  $X$  de  $V$ , o subespaço  $X^\perp := \{v \in V \mid b_q(v, x) = 0, \forall x \in X\}$  é dito *complemento ortogonal* de  $X$ . Quando  $X = V$ , diz-se que  $V^\perp$  é o *radical* de  $V$ , e também denotaremos  $V^\perp$  por  $rad V$ . Notemos que a Proposição anterior nos diz que o espaço quadrático  $(V, q)$  é não singular se, e somente se,  $rad V = \{0\}$ .

**Exemplo (2)** A forma quadrática de dimensão três dada por  $q(u) = X^t M_q X$ , onde  $u$  tem coordenadas  $X = (x, y, z)$  numa base fixada e



$$M_q = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 2 \\ 0 & 2 & 0 \end{pmatrix} \text{ é não singular pois tem determinante não nulo.}$$

Se  $(V, q)$  é um espaço quadrático e  $U$  é um subespaço de  $V$ , então a restrição da forma quadrática  $q$  ao subespaço  $U$ ,  $q|_U$  é uma forma quadrática sobre  $U$ . Pode ocorrer de  $(V, q)$  ser um espaço quadrático regular e  $(U, q|_U)$  não ser regular. Por exemplo, tome  $U = \{\alpha e_1 + \beta e_2, \alpha, \beta \in F\}$ , no exemplo anterior. Encontramos  $U^\perp = \{\lambda(e_1 + e_2), \lambda \in F\} \neq \{0\}$ . Logo  $q_U$  não é regular. No entanto temos

**Proposição 1.1.2** *Sejam  $(V, q)$  um espaço quadrático regular e  $U$  um subespaço de  $V$ . Então:*

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

**Demonstração:** Também é um exercício de álgebra linear e será evitada. ■

## 1.2 Diagonalização de Formas Quadráticas

**Definição 1.2.1** Sejam  $(V_1, q_1)$  e  $(V_2, q_2)$  espaços quadráticos sobre um corpo  $F$  e  $V = V_1 \oplus V_2$ . Definimos  $q : V \rightarrow F$  por  $q(v_1 + v_2) = q_1(v_1) + q_2(v_2)$ . Então  $(V, q)$  é um espaço quadrático com forma bilinear associada  $b_q : V \times V \rightarrow F$  dada por  $b_q((u_1, u_2), (v_1, v_2)) = b_{q_1}(u_1, v_1) + b_{q_2}(u_2, v_2)$ . Denota-se este novo espaço quadrático por  $(V_1, q_1) \perp (V_2, q_2)$  ou simplesmente por  $q_1 \perp q_2$ .

Uma vez fixada uma base para o espaço vetorial  $V$  toda forma quadrática sobre  $V$  pode ser posta na forma  $q(x_1, \dots, x_n) = \sum_{i=1}^n a_{ii}x_i x_i$ . Termos mistos  $x_i x_j$  podem ocorrer na somatória, e normalmente ocorrem. Nossa intenção agora é *diagonalizar* uma forma quadrática, ou seja,

obter uma forma quadrática  $q_1$  isométrica a  $q$  de modo que  $q_1(x_1, \dots, x_n) = \sum_{i=1}^n a_{ii} x_i^2$ . Daí em diante só trabalharemos com este tipo de formas, por ser mais prático.

**Definição 1.2.2** Sejam  $q : V \rightarrow F$  uma forma quadrática sobre  $F$  e  $d \in \dot{F}$ . Dizemos que  $q$  representa  $d$  se existir  $v \in V$  tal que  $q(v) = d$ . Denota-se por  $D_F(q)$  ou por  $D(q)$ , ou ainda por  $Dq$  o conjunto dos elementos de  $\dot{F}$  representado por  $q$ . Se  $D(q) = \dot{F}$  dizemos que  $q$  é (uma forma quadrática) *universal*.

**Observação 1.2.3** É claro que se  $q$  e  $q_1$  são formas quadráticas isométricas e  $q$  representa  $d$  então  $q_1$  também representa  $d$ . Assim, o conjunto  $D(q)$  dos elementos de  $\dot{F}$  representados pela forma quadrática  $q$  depende apenas da classe de isometria de  $q$ . Além disso, se  $\alpha, d \in \dot{F}$ , temos que  $d \in D(q)$  se, e somente se,  $\alpha^2 d \in D(q)$  (pois:  $q(u) = d$  se, e somente se,  $q(\alpha u) = \alpha^2 d$ ). Com isso vemos que  $D(q)$  é uma reunião de classes de  $\dot{F}$  módulo  $\dot{F}^2$ , e podemos considerar  $D(q) \subset \frac{\dot{F}}{\dot{F}^2}$ .

**Notação 1.2.4** Se  $V = F.e_1$ , a forma quadrática sobre  $V$  definida por  $q(x.e_1) = dx^2$  será denotado por  $\langle d \rangle$ . Para  $d \in \dot{F}$  é evidente que  $q$  é não-degenerada.

**Proposição 1.2.5 Critério de Representação.**

Sejam  $q$  uma forma quadrática definida sobre  $F$  e  $d \in \dot{F}$ . Então  $d \in D(q)$  se, e somente se, existe uma forma quadrática  $q_1$  definida sobre  $F$  tal que  $q \simeq \langle d \rangle \perp q_1$ .

**Demonstração:**

Se  $q \simeq \langle d \rangle \perp q_1$  então  $d \in D(\langle d \rangle \perp q_1) = D(q)$ .

Reciprocamente se  $d \in D(q)$  então existe  $v \in V$  tal que  $q(v) = d$ . O subespaço quadrático  $(F.w, q_{F.w}) = (F.w, \langle d \rangle)$  é regular. Provemos que  $(F.w, \langle d \rangle) \perp ((F.w)^\perp, q_{(F.w)^\perp}) = (V, q)$ .

De fato, seja  $F.w := U$ . Como  $(U, \langle d \rangle)$  é regular, temos que  $\theta_1 : U \rightarrow U^*$  dada por:  $\theta_1(u) = b_U(, u)$  é um isomorfismo. Como para todo  $v \in V$ ,  $\theta(v) \in V^*$ , vem que  $\theta(v)_U \in U^*$ .



Como  $\theta_1$  é um isomorfismo existe  $u \in U$  tal que  $\theta(v)_U = \theta_1(u)$ . Assim  $\theta(v)_U(u_1) = \theta_1(u)(u_1)$ ,  $\forall u_1 \in U$ . Ou seja  $b_q(v, u_1) = b_q(u, u_1)$ ,  $\forall u_1 \in U$ . Daí  $b_q(v - u, u_1) = 0$ ,  $\forall u_1 \in U$ . Isto significa que  $v - u \in U^\perp$ . Como  $v = u + (v - u)$  segue-se que  $V = U \oplus U^\perp$ , e como  $b(u, v) = 0$ ,  $\forall u \in U$ ,  $v \in U^\perp$  a proposição está demonstrada. ■

A primeira consequência deste critério é a existência de uma base ortogonal para qualquer espaço quadrático. De fato por indução sobre  $\dim q$  temos:

**Teorema 1.2.6** *Seja  $(V, q)$  um espaço quadrático sobre  $F$ . Então  $(V, q)$  é uma soma ortogonal de subespaços quadráticos unidimensionais, ou seja, existem escalares  $d_1, d_2, \dots, d_n \in \dot{F}$ , tais que  $q \simeq \langle d_1 \rangle \perp \langle d_2 \rangle \dots \perp \langle d_n \rangle$ . Em outras palavras,  $V$  tem uma base constituída de vetores dois a dois ortogonais entre si (base ortogonal), com relação a  $b_q$ .*

**Notação 1.2.7** A isometria  $q \simeq \langle d_1 \rangle \perp \dots \perp \langle d_n \rangle$  será denotada por  $q = \langle d_1, d_2, \dots, d_n \rangle$ , e dizemos que  $q$  está na forma diagonal. Considerando esta base ortogonal temos que se  $u = \sum_{i=1}^n x_i e_i \in V$ , então  $q(u) = b_q(u, u) = \sum_{i,j=1}^n b_q(e_i, e_j) x_i x_j = \sum_{i=1}^n b_q(e_i, e_i) x_i^2 = d_1 x_1^2 + d_2 x_2^2 + \dots + d_n x_n^2$ . Ou seja, na expressão de  $q(u)$  ocorre a separação de variáveis. Este fato só é verdadeiro se a característica do corpo  $F$  for distinta de dois. Ainda temos a notação reduzida  $n \langle d \rangle$  quando  $d_i = d$  para todo  $i = 1, 2, \dots, n$ .

Temos ainda que se  $q = \langle a_1, a_2, \dots, a_n \rangle$  é uma forma quadrática sobre  $F$  então o determinante de  $q$  é  $d(q) = (a_1 \dots a_n) \dot{F}^2$  e no caso em que  $q = q_1 \perp q_2$  então  $d(q) = d(q_1) \cdot d(q_2)$ .

**Observação 1.2.8** Algumas isometrias entre formas quadráticas são evidentes. Por exemplo se

(i)  $\sigma$  é um elemento do grupo das permutações de  $n$  elementos, então as formas quadráticas  $\langle a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)} \rangle$  e  $\langle a_1, a_2, \dots, a_n \rangle$  são isométricas.

(ii) Para qualquer  $\beta \in \dot{F}$ , as formas quadráticas  $\langle a_1 \beta_1^2, a_2 \beta_2^2, \dots, a_n \beta_n^2 \rangle$  e  $\langle a_1, a_2, \dots, a_n \rangle$  também são isométricas. De fato, basta considerar o isomorfismo de  $V$  definido por  $\tau(x_1, x_2, \dots, x_n)$

$(\beta_1 x_1, \beta_2 x_2, \dots, \beta_n x_n)$ . Assim os elementos  $a_i$  da forma quadrática  $\langle a_1, a_2, \dots, a_n \rangle$  podem ser tomados livre de quadrados, ou seja, elementos do grupo  $\frac{F^\times}{F^{\times 2}}$ .

### 1.3 Isotropia, Plano Hiperbólico e Decomposição de Formas Quadráticas

**Definição 1.3.1** Seja  $(V, q)$  um espaço quadrático. Dizemos que  $q$  é *isotrópica* (ou  $(V, q)$  é *isotrópico*), se existe um vetor não nulo  $v \in V$  tal que  $q(v) = 0$ . O vetor  $v$  é dito *vetor isotrópico*. Caso contrário dizemos que  $q$  é *anisotrópica* (ou que  $(V, q)$  é *anisotrópico*) e  $v$  é um vetor *anisotrópico*.

Um subespaço quadrático  $(U, q_1)$  de  $(V, q)$  ( $q_1 = q|_U$ ) é dito totalmente isotrópico se  $q_1(x, y) = 0$  para todos  $x, y \in U$ .

Dizemos que uma forma quadrática  $q$  (ou espaço quadrático  $(V, q)$ ) contém a forma quadrática  $q_1$  como subforma se existe uma forma quadrática  $q_2$  tal que  $q \simeq q_1 \perp q_2$ .

Consideremos as formas quadráticas  $q$  e  $q_1$  do exemplo (1). Já vimos que elas são isométricas. Por abuso de linguagem vamos denotar por  $\mathbb{H}$  tanto sua classe de isometria quanto um de seus representantes. Sendo assim os teoremas que vem a seguir caracterizam as formas quadráticas isotrópicas e a classe  $\mathbb{H}$ . Começemos por

**Teorema 1.3.2** *Seja  $(V, q)$  um espaço quadrático bidimensional. As seguintes afirmações são equivalentes:*

1.  $(V, q)$  é não singular e isotrópico,
2.  $(V, q)$  é não singular, com  $d(q) = -1 \cdot \dot{F}^2$ ,
3.  $(V, q)$  é isométrico à  $(V, \langle 1, -1 \rangle)$ ,



4.  $q \simeq q_1$ , onde  $q_1(x, y) = xy$ .

### Demonstração:

O exemplo (1), mostra que (3) e (4) são equivalentes.

(1)  $\Rightarrow$  (2) Seja  $\{e_1, e_2\}$  uma base ortogonal de  $V$  em relação a qual  $q \simeq \langle d_1, d_2 \rangle$ . Por hipótese temos que  $d(q) = \begin{vmatrix} d_1 & 0 \\ 0 & d_2 \end{vmatrix} = d_1 d_2 \neq 0$ . Como  $q$  é isotrópica, segue-se que  $\langle d_1, d_2 \rangle$  é isotrópica. Seja  $v = xe_1 + ye_2 \neq 0$  tal que  $d_1 x^2 + d_2 y^2 = 0$ . Como  $x \neq 0$ , temos que  $d_1 = -d_2(\frac{y}{x})^2$ . Consequentemente  $d(q) = (-1) \cdot \dot{F}^2$ .

(2)  $\Rightarrow$  (3) Diagonalizando  $q$  temos que  $q \simeq \langle a, b \rangle$ . Por hipótese  $ab = -1$  ou  $b = -a$  em  $\frac{\dot{F}}{\dot{F}^2}$ . Logo  $q \simeq \langle a, -a \rangle$ . Seja  $q_1(x, y) = axy$  e  $\sigma(x, y) = (x - y, x + y)$ . Então  $q_1 \circ \sigma = \langle a, -a \rangle$ , ou seja,  $q \simeq q_1$ . Desde que  $q_1$  é universal,  $q$  também o é. Assim  $-1 \in D(q)$  e pelo Critério de Representação segue que  $q \simeq \langle -1, c \rangle$ , para algum  $c \in \dot{F}$ . Calculando o determinante obtemos a isometria  $q \simeq \langle 1, -1 \rangle$ .

(3)  $\Rightarrow$  (1) Desde que  $\langle 1, -1 \rangle$  é isotrópica e não singular, o mesmo vale para  $q$ , devido a hipótese. ■

**Observação 1.3.3** (a) O item (4) do Teorema justifica o nome plano hiperbólico, porque o gráfico das equações  $xy = d$ , (com  $d \neq 0$ ) são chamados de hipérboles. Uma soma ortogonal de  $m$  planos hiperbólicos é chamada espaço hiperbólico e será denotado por  $m\text{IH}$ . Dois representantes desta classe são  $x_1^2 - x_2^2 + \dots + x_{2m-1}^2 - x_{2m}^2$  e  $x_1 x_2 + \dots + x_{2m-1} x_{2m}$ , pelos itens (3) e (4) do Teorema anterior.

(b) Como  $q_1(x, 1) = x$ , para todo  $x \in F$  segue-se que o plano hiperbólico é universal. Logo qualquer forma quadrática que contém o plano hiperbólico também é universal.

**Teorema 1.3.4** Seja  $(V, q)$  um espaço quadrático regular. Então:



1. *Todo subespaço totalmente isotrópico,  $(U, q_1)$  de  $(V, q)$ , de dimensão positiva  $r$ , está contida num subespaço hiperbólico  $r\mathbb{H} \subseteq (V, q)$ .*

2.  *$q$  é isotrópico se, e somente se,  $q$  contém um plano hiperbólico.*

3.  *$q$  é isotrópico  $\Rightarrow q$  é universal.*

### Demonstração:

(1)  $\Rightarrow$  (2) é claro, basta fazer  $r = 1$  em (1).

(2)  $\Rightarrow$  (3) é óbvio, pois por (2)  $q \supset \mathbb{H}$  cujo uma das formas quadráticas representantes é  $q(x, y) = xy$  que é universal.

Agora demonstraremos (1), por indução em  $r$ .

Tome uma base  $\{e_1, e_2, \dots, e_r\}$  de  $U$ , e seja  $S$  o subespaço gerado por  $\{e_2, \dots, e_r\}$ . Então  $U^\perp \subset S^\perp$  e desde que  $(V, q)$  é regular, pela Proposição 1.1.2(1) obtemos:

$$\dim S^\perp = \dim V - \dim S > \dim V - \dim U = \dim U^\perp.$$

Isto significa que existe  $v_1$  ortogonal a  $e_2, e_3, \dots, e_r$  mas não ortogonal a  $e_1$ . Desde que  $e_1$  é isotrópico,  $\{e_1, v_1\}$  é linearmente independente. Consequentemente a forma quadrática  $q_1 :$

$Fe_1 \oplus Fv_1 \rightarrow F$  tem determinante

$$d(q) = \begin{vmatrix} 0 & b_{q_1}(e_1, v_1) \\ b_{q_1}(e_1, v_1) & b_{q_1}(v_1, v_1) \end{vmatrix} \cdot \dot{F}^2 = -1 \cdot \dot{F}^2$$

Então  $(Fe_1 \oplus Fv_1, q_1) = \mathbb{H}$ , pelo Teorema 1.3.2. Assim temos decomposto  $(V, q)$  na soma  $(V, q) = \mathbb{H} \perp (V', q')$ , onde  $(V', q') = \mathbb{H}^\perp$  e  $\mathbb{H}^\perp$  contém  $e_2, \dots, e_r$  por construção. Desde que  $(V', q')$  é regular (pois  $0 \neq d(q) = d(q_1) \cdot d(q')$ ), a demonstração se completa por indução em  $r$ .

■

**Observação 1.3.5** *Uma consequência importante do item (2) deste Teorema é que podemos repetir este raciocínio para a forma quadrática  $q_1$ , desde que ela seja isotrópica. Como  $q$  tem*



dimensão finita, depois de alguns passos vamos chegar a  $q \simeq q_a \perp m\mathbb{H}$ , onde  $q_a$  é uma subforma de  $q$  anisotrópica e  $m \geq 0$ . Mais que isto, o Teorema de Decomposição de Witt que veremos adiante nos afirma que esta decomposição é única, a menos de isometria.

**Teorema 1.3.6 Teorema de Representação.** *Seja  $q$  uma forma quadrática, e  $d \in \dot{F}$ . Então  $d \in D(q)$  se, e somente se,  $q \perp \langle -d \rangle$  é isotrópica.*

#### Demonstração:

Seja  $X = (x_1, \dots, x_n)$  tal que  $q(x_1, \dots, x_n) = d$ . Então  $(q \perp \langle -d \rangle)(X, 1) = d - d = 0$ . Como  $(X, 1) \neq 0$ ,  $q \perp \langle -d \rangle$  é isotrópica. Reciprocamente, se  $X' = (x_1, \dots, x_n, x_{n+1})$  é um vetor isotrópico para  $q \perp \langle -d \rangle$ , então  $(q \perp \langle -d \rangle)(X') = 0$ . Se  $x_{n+1} \neq 0$ , isto implica que  $d = q(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}) \in D(q)$ . Se  $x_{n+1} = 0$ , então  $q(x_1, \dots, x_n) = 0$  e  $q$  é isotrópica, pois  $(x_1, x_2, \dots, x_n) \neq 0$ . Logo  $q \supset \mathbb{H}$ , e como  $\mathbb{H}$  é universal segue que  $q$  é universal, ou seja,  $d \in D(q) = \dot{F}$ . ■

**Corolário 1.3.7** *Para um inteiro positivo  $r$ , as afirmações seguintes são equivalentes:*

1. *Toda forma quadrática regular de dimensão  $r$  é universal.*
2. *Toda forma quadrática de dimensão  $r + 1$  é isotrópica.*

#### Demonstração

(1)  $\Rightarrow$  (2) Seja  $q \simeq \langle a_1, a_2, \dots, a_r, a_{r+1} \rangle$ . Como  $q' = \langle a_1, a_2, \dots, a_r \rangle$  é universal segue-se que  $q'$  representa  $-a_{r+1}$ . Pelo Teorema da Representação  $q \simeq q' \perp \langle a_{r+1} \rangle$  é isotrópica.

(2)  $\Rightarrow$  (1) Seja  $q \simeq \langle a_1, a_2, \dots, a_r \rangle$ . Para qualquer  $d \in \dot{F}$ ,  $q' \perp \langle -d \rangle$  é isotrópica. Pelo Teorema da Representação  $d \in D(q')$ . Logo  $q'$  é universal. ■

Para demonstrarmos o Teorema de Cancelamento de Witt precisaremos da noção de reflexão segundo um hiperplano. Um hiperplano é determinado por um vetor anisotrópico  $v$  de  $V$ . É exatamente o complemento ortogonal de  $v$ ,  $(Fv)^\perp$ .

**Lema 1.3.8** Sejam  $(V, q)$  um espaço quadrático,  $v$  um vetor anisotrópico de  $V$ . Definimos  $\tau_v : V \rightarrow V$  por  $\tau_v(u) = u - \frac{2b_q(u, v)}{q(v)} \cdot v$ . Então  $\tau_v$  satisfaz:

1.  $\tau_v$  é um endomorfismo de  $V$ .
2.  $\tau_v$  restrita a  $(Fv)^\perp$  é a aplicação identidade e  $\tau_v(v) = -v$ . Em particular, temos que  $\tau_v$  é uma involução (ou seja:  $\tau_v^2 = Id$ ).
3.  $\tau_v$  é uma isometria.
4.  $\det(\tau_v) = -1$ .

#### Demonstração:

É imediata e se resume a verificações. ■

**Lema 1.3.9** Sejam  $(V, q)$  um espaço quadrático e  $u, v \in V$  tais que  $q(u) = q(v) \neq 0$ . Então existe uma isometria  $\tau : V \rightarrow V$  tal que  $\tau(u) = v$ .

#### Demonstração:

Geometricamente, se considerarmos a reflexão em torno de  $F(u - v)^\perp$  o vetor  $u$  será levado em  $v$ . Isto é possível se  $u - v$  é um vetor anisotrópico. Por outro lado tem-se  $q(u + v) + q(u - v) = b(u + v, u + v) + b(u - v, u - v) = b(u, u) + 2b(u, v) + b(v, v) + b(u, u) - 2b(u, v) + b(v, v) + (u, u) + 2b(v, v) = 2q(u) + 2q(u) = 4q(u) \neq 0$ . Assim  $q(u + v) \neq 0$  ou  $q(u - v) \neq 0$ . Se  $q(u - v) \neq 0$ , o Lema está concluído, pois tomamos  $\tau = \tau_{u-v}$ . Agora, se  $q(u - v) = 0$  então  $q(u + v) \neq 0$  e neste caso  $\tau_{u+v}(u) = u - \frac{2b(u, u+v)}{q(u+v)} \cdot (u+v)$ . Mas  $q(u + v) = q(u) + q(v) + 2b(u, v) = 2q(u) + 2b(u, v) + (u, u + v)$ . Logo  $\tau_{u+v}(u) = u - \frac{2b(u, u+v)}{q(u+v)} \cdot (u+v) \cdot u - (u+v) = -v$ . Portanto  $-\tau_{u+v}(u) = v$ . Logo  $\tau = \tau_{u+v}$  é a isometria procurada. ■

**Teorema 1.3.10** [Cancelamento de Witt.] Sejam  $q, q_1, q_2$  formas quadráticas arbitrárias. Se  $q \perp q_1 \simeq q \perp q_2$  então  $q_1 \simeq q_2$ .

### Demonstração:

Sejam  $q_3 = \langle a_1 \rangle^\perp q_1$ , e  $q_4 = \langle a_1 \rangle^\perp q_2$ . Seja  $\sigma : V \rightarrow V$  tal que  $q_3 = q_4 \circ \sigma$ . De  $0 \neq a_1 \in D(q_3) \cap D(q_4)$ , existem  $u, v \in V$  tal que  $q_3(u_1) = a_1 = q_4(v)$ , ou  $a_1 = q_3(u_1) = q_4(\sigma(u_1)) = q_4(u)$ , onde  $u = \sigma(u_1)$ . Assim  $q_4(u) = q_4(v)$ . Pelo Lema anterior existe uma isometria  $\tau$  de  $V$  tal que  $\tau(u) = v$  e  $q_4 \circ \sigma = q_4$ . Temos  $q_3 = q_4 \circ (\tau \circ \sigma)$  e  $q_3(u_1) = a_1 = q_4((\tau \circ \sigma)(u_1)) = q_4(v_1)$ , (onde  $(\tau \circ \sigma)(u_1) = v$ ). Logo  $(\tau \circ \sigma)|_{(Fu_1)^\perp} : (Fu_1)^\perp \rightarrow (Fv)^\perp$  é um isomorfismo tal que

$$q_4|_{(Fv)^\perp} \circ (\tau \circ \sigma)|_{(Fu_1)^\perp} = q_3|_{(Fu_1)^\perp},$$

ou seja,

$$q_2 \circ (\tau \circ \sigma) = q_1.$$

Assim  $q_1 \simeq q_2$ . O resto segue por indução. ■

**Teorema 1.3.11** [Decomposição de Witt.] *Todo espaço quadrático  $(V, q)$  se decompõe em uma soma ortogonal  $(V, q) \simeq (V_h, q_h) \perp (V_a, q_a)$ , de modo único (a menos de isometria) onde  $(V_h, q_h)$  espaço hiperbólico,  $(V_a, q_a)$  espaço anisotrópico.*

### Demonstração:

Pela Observação 1.3.5 já vimos que  $(V, q)$  se escreve na forma  $(V, q) \simeq r\mathbb{H} \perp (V_a, q_a)$  ( $r \geq 0$ ), onde  $r\mathbb{H}$  é o espaço hiperbólico (se  $r > 0$ ) e  $(V_a, q_a)$  é anisotrópico.

Para a unicidade, suponhamos que existe outra decomposição de  $(V, q) \simeq n\mathbb{H} \perp (V'_a, q'_a)$ . Sem perda de generalidade podemos supor  $r \geq n$ . Pelo Teorema do Cancelamento temos  $(r - n)\mathbb{H} \perp q_a \simeq q'_a$ . Desde que  $q'_a$  é anisotrópica, concluímos que  $r - n = 0$ . Logo  $r = n$  e  $q_a \simeq q'_a$ . ■



# 1.4 Produto de Kronecker de Espaços Quadráticos.

Já foi definido soma ortogonal de formas quadráticas. Agora definiremos produto de formas quadráticas, que juntamente com o Teorema de Cancelamento de Witt serão úteis na construção do anel de Witt das formas quadráticas sobre um corpo  $F$ .

**Definição 1.4.1** Sejam  $(V_1, q_1)$ ,  $(V_2, q_2)$  espaços quadráticos sobre  $F$  de dimensões  $m$  e  $n$ , e  $V = V_1 \otimes V_2$ . Definimos  $b : V \times V \rightarrow F$  a única forma bilinear simétrica satisfazendo  $b(v_1 \otimes v_2, u_1 \otimes u_2) = b_1(v_1, u_1).b_2(v_2, u_2)$  para todos  $u_1, v_1 \in V_1$  e  $u_2, v_2 \in V_2$ , onde  $b_i$  é a forma bilinear associada a  $q_i$ ,  $i = 1, 2$ . Agora definimos  $q : V \rightarrow F$  por  $q(v_1 \otimes v_2) = b(v_1 \otimes v_2, v_1 \otimes v_2)$ . Portanto  $q(v_1 \otimes v_2) = b_1(v_1, v_1).b_2(v_2, v_2) = q_1(v_1).q_2(v_2)$ . Segue-se que  $(V, q)$  é um espaço quadrático de dimensão  $m.n$ , e a forma bilinear associada à  $q$  é a forma bilinear definida acima. Denotemos  $q$  por  $q_1 \otimes q_2$  (ou  $q := q_1.q_2$ ).

Sejam  $\{e_1, \dots, e_m\}$  base de  $V_1$ ,  $\{f_1, \dots, f_n\}$  base de  $V_2$ ,  $a_{ij} = b(e_i, e_j)$  e  $b_{ke} = b(f_k, f_e)$ . Então  $M = (a_{ij})$  e  $N = (b_{ke})$  são as matrizes de  $q_1$  e  $q_2$  nestas bases. Na base  $\{e_1 \otimes f_1, e_1 \otimes f_2, \dots, e_1 \otimes f_n, \dots, e_m \otimes f_1, \dots, e_m \otimes f_n\}$  de  $V$  a matriz de  $q$  é

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

que é chamado de *produto de Kronecher* das matrizes  $M$  e  $N$ . Em particular  $\langle a \rangle \otimes \langle b \rangle = \langle ab \rangle \quad \forall a, b \in F$ .



**Proposição 1.4.2 (Propriedades):**

1.  $q_1 \otimes q_2 \simeq q_2 \otimes q_1$  (lei comutativa).
2.  $(q_1 \otimes q_2) \otimes q_3 \simeq q_1 \otimes (q_2 \otimes q_3)$  (lei associativa).
3.  $q \otimes (q_1 \perp q_2) \simeq (q \otimes q_1) \perp (q \otimes q_2)$  (lei distributiva).

**Demonstração:**

(1)  $V = V_1 \otimes V_2 \xrightarrow{\sigma} V_2 \otimes V_1$  dada por  $\sigma(x \otimes y) = y \otimes x$  leva base em base e  $q = q' \circ \sigma$ .

(2)  $(V_1 \otimes V_2) \otimes V_3 \xrightarrow{\sigma} V_1 \otimes (V_2 \otimes V_3)$   $(x \otimes y) \otimes z \rightarrow x \otimes (y \otimes z)$   $\sigma$  leva base em base e  $(q_1 \otimes (q_2 \otimes q_3)) \circ \sigma = (q_1 \otimes q_2) \otimes q_3$ .

(3)  $V \otimes (V_1 \perp V_2) \xrightarrow{\sigma} (V \otimes V_1) \perp (V \otimes V_2)$  definida por  $\sigma(x \otimes (y_1 + y_2)) = (x \otimes y_1) + (x \otimes y_2)$  satisfaz  $(q' \circ \sigma)[x \otimes (y_1 \perp y_2)] = q'((x \otimes y_1) + (x \otimes y_2)) = (q \otimes q_1)(x_1 \otimes y_1) = (q \otimes q_2)(x \otimes y_2) = q(x)(q_1 \perp q_2)(y_1 + y_2) = q \otimes (q_1 \perp q_2)(x \otimes (y_1 + y_2))$ . Logo  $q \otimes (q_1 \perp q_2) \simeq (q \otimes q_1) \perp (q \otimes q_2)$ . ■

**Observação 1.4.3** 1. Pela lei distributiva tem-se:

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

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

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



## Capítulo 2

### Anel de Witt

#### 2.1 Construção do Anel de Witt

Seja  $M(F)$  o conjunto de todas as classes de isometria das formas quadráticas não singulares sobre  $F$ . Sabemos que a operação  $\perp$  é associativa, comutativa e admite elemento neutro, e a operação  $\otimes$  é associativa e distributiva em relação  $\perp$ . Assim  $\perp$  e  $\otimes$  definem uma estrutura de semi-anel em  $M(F)$ . Pelo Teorema do Cancelamento de Witt para  $\perp$ , segue-se que  $M(F)$  é um semi grupo com cancelamento, embora nenhum elemento não nulo em  $M(F)$  não tenha inverso aditivo. A construção do anel de Witt Grothendieck resolve este problema. Ele é construído do mesmo modo em que se constrói o anel  $\mathbb{Z}$  dos inteiros a partir do semi-anel com cancelamento  $\mathbb{N}$ .

Seja  $(M, \perp)$  um semi-grupo aditivo, comutativo com cancelamento. Definimos a relação  $\sim$  sobre  $M \times M$  por:

$$(x, y) \sim (x', y') \Leftrightarrow x \perp y' = x' \perp y \in M.$$

A relação  $\sim$  definida sobre  $M \times M$  é uma relação de equivalência. Vamos denotar o conjunto das classes de equivalência por  $Groth(M)$ , ou seja,  $Groth(M) := \{\overline{(a, b)}, (a, b) \in M \times M\}$ ,



onde  $\overline{(a,b)} = \{(x,y) \mid (x,y) \sim (a,b)\}$ .

Agora definimos em  $Groth(M)$  a operação de adição por:

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a \perp c, b \perp d)}.$$

É fácil a verificação de que esta operação está bem definida sobre  $Groth(M)$  e que valem as propriedades associativa, comutativa e existência do elemento neutro para a adição. Este elemento é  $\overline{(a,a)}$ ,  $a \in M$ . O oposto de  $\overline{(a,b)}$  é  $\overline{(b,a)}$  pois:  $\overline{(a,b)} \perp \overline{(b,a)} = \overline{(a \perp b, b \perp a)} = \overline{(c,c)}$ . Denotemos  $\overline{(b,a)}$  por  $-\overline{(a,b)}$ . Em particular temos que  $-\overline{(b,0)} = \overline{(0,b)}$ .

A aplicação  $\varphi : M \longrightarrow Groth(M)$  definida por  $\varphi(a) = \overline{(a,0)}$ , injeta  $M$  em  $Groth(M)$ , ou seja,  $\varphi$  é um homomorfismo injetor. Identificando  $M$  com sua imagem  $\{\overline{(a,0)}, a \in M\}$  em  $Groth(M)$ , podemos dizer que  $M \subset Groth(M)$ . Assim para  $\overline{(a,b)} \in Groth(M)$  temos que  $\overline{(a,b)} = \overline{(a,0)} \perp \overline{(0,b)} = \overline{(a,0)} - \overline{(b,0)} \equiv a - b$ . Com isso, no caso em que  $M = M(F)$ , podemos subtrair uma forma quadrática de outra, via a identificação  $q \equiv \varphi(q)$ . Esta última identificação será denotada pela igualdade  $q = \varphi(q)$ .

Sabemos que  $(M, \perp)$  é um semi-grupo comutativo com cancelamento. Se  $M$  tem outra operação "•" associativa e distributiva em relação a  $\perp$ , definimos  $\bullet : Groth(M) \times Groth(M) \rightarrow Groth(M)$  por  $\overline{(x,y)} \bullet \overline{(x',y')} = \overline{(x.x' \perp y.y', x.y' \perp x'.y)}$ .

É fácil demonstrar que esta operação está bem definida sobre  $Groth(M)$  e que  $(Groth(M), +, \bullet)$  é um anel. Este anel é dito anel de Witt Grothendieck. Assim, o anel de Witt Grothendieck de  $\mathbb{N}$  é  $\mathbb{Z}$  : o anel de inteiros. Também para  $M = M(F)$ , o produto tensorial nos dá uma multiplicação com as propriedades desejadas. Então temos:

**Definição 2.1.1**  $\hat{W}(F) := Groth(M(F))$  é chamado de *Anel de Witt Grothendieck das formas quadráticas* sobre o corpo  $F$ .

Todos os elementos de  $\hat{W}(F)$  são do tipo  $\overline{(q_1, q_2)} = \overline{(q_1, 0)} + \overline{(0, q_2)} = q_1 - q_2$ , onde  $q_1$  e



$q_2$  são formas quadráticas não singulares. Para quaisquer formas quadráticas  $q_1$  e  $q_2$  sobre  $F$ , tem-se  $q_1 = q_2 \in \hat{W}(F)$  se, e somente se,  $\overline{(q_1, 0)} = \overline{(q_2, 0)} \iff q_1 \sim q_2$ .

Para  $m, n \in \mathbb{N}$  os elementos,  $\overline{(m\mathbb{H}, n\mathbb{H})} \in \hat{W}(F)$  são iguais a  $((m-n)\mathbb{H}, 0)$  se,  $m \geq n$  ou igual  $(0, (n-m)\mathbb{H})$  caso  $n > m$ . Segundo a notação dada temos que  $\overline{(m\mathbb{H}, n\mathbb{H})} = s\mathbb{H}$ ,  $s \in \mathbb{Z}$ , qualquer que seja  $m, n \in \mathbb{Z}$ .

Juntando isto, ao fato de que  $q \otimes \mathbb{H} \simeq (\dim q)\mathbb{H}$ , podemos provar que o conjunto  $\mathbb{Z}\mathbb{H} = \{m\mathbb{H}, m \in \mathbb{Z}\}$  é um ideal de  $\hat{W}(F)$ .

**Definição 2.1.2** O anel quociente  $\frac{\hat{W}(F)}{\mathbb{Z}\mathbb{H}}$  denotado por  $W(F)$  é chamado de *anel de Witt* de  $F$ .

Note que em  $W(F)$ ,  $\mathbb{H} = \langle a, -a \rangle = 0$ . Logo  $-\langle a \rangle = \langle -a \rangle$  e por extensão  $-\langle a_1, \dots, a_n \rangle = \langle -a_1, \dots, -a_n \rangle$ , em  $W(F)$ . Isto mostra que podemos representar qualquer elemento de  $W(F)$  por formas quadráticas. Mais exatamente, pelo Teorema de Decomposição de Witt cada elemento do anel de Witt corresponde exatamente a uma única forma quadrática anisotrópica, a menos de isometria. Formalizemos na seguinte proposição,

### Proposição 2.1.3

1. Os elementos de  $W(F)$  estão em correspondência um a um com as classes de isometria de todas formas quadráticas anisotrópicas.
2. Duas formas quadráticas não singulares  $q$  e  $q'$ , representam o mesmo elemento de  $W(F)$  se, e somente se,  $q_a \simeq q'_a$  (isto é, suas partes anisotrópicas são isométricas).
3. Se  $\dim q = \dim q'$  então,  $q$  e  $q'$  representam o mesmo elemento de  $W(F)$  se, e somente se,  $q \simeq q'$ .



### Demonstração:

Seguem das definições e dos Teoremas de Decomposição e Cancelamento de Witt. ■

## 2.2 Anéis de Witt de Alguns Corpos

Alguns passos importantes para determinar o anel de Witt de um corpo  $F$  são:

(i) Como todos os elementos de  $W(F)$  são representados por formas quadráticas diagonalizadas basta considerar este tipo de forma.

(ii) Determinar o grupo de classes de quadrados  $\frac{F}{F^2}$ , pois as entradas  $a_i$  da forma quadrática diagonal são elementos deste grupo. (Ver Observação 1.2.8(ii)).

(iii) Determinar a classe  $-1 \in \frac{F}{F^2}$ , para conhecer  $\mathbb{H} = \langle 1, -1 \rangle$ : o gerador do ideal  $\mathbb{Z}\mathbb{H}$ .

Começemos com

**Exemplo 2.2.1**  $F$  é um corpo quadraticamente fechado.

Um corpo  $F$  é dito um corpo quadraticamente fechado se qualquer um de seus elementos é um quadrado. Assim  $\frac{F}{F^2} = \{1\}$ , e portanto toda forma quadrática  $q$  sobre  $F$  admite a seguinte diagonalização  $q = \langle 1, 1, \dots, 1 \rangle$ . Como  $1 = -1$  em  $\frac{F}{F^2}$ , segue-se que  $\mathbb{H} = \langle 1, 1 \rangle$ . Logo se  $q$  tem dimensão  $2n$  então  $q = n\mathbb{H}$ , e se  $\dim q = 2n + 1$  então  $q = \langle 1 \rangle + n\mathbb{H}$ . Pela Proposição 2.1.3 obtemos  $W(F) = \{\langle 0 \rangle, \langle 1 \rangle\}$ , ou seja,  $W(F)$  é isomorfo a  $\frac{\mathbb{Z}}{2\mathbb{Z}}$ .

**Exemplo 2.2.2**  $F = \mathbb{R}$ .

Temos duas classes de quadrados em  $\mathbb{R}$  uma constituída pelos elementos positivos (representada por 1) e outra constituída pelos elementos negativos (representada por -1). Logo toda forma quadrática sobre  $\mathbb{R}$  se escreve de modo único na forma  $q = n \langle 1 \rangle + m \langle -1 \rangle$ . Como



$H = \langle 1, -1 \rangle$ , temos que  $q = s \langle 1 \rangle \in W(\mathbb{R})$ , onde  $s = n - m \in \mathbb{Z}$ . Agora é fácil provar que a aplicação  $\varphi : W(\mathbb{R}) \rightarrow \mathbb{Z}$  definida por  $\varphi(s \langle 1 \rangle) = s$  é um isomorfismo de anéis. Assim  $W(\mathbb{R}) \simeq \mathbb{Z}$ .

**Exemplo 2.2.3**  $F$  : corpo finito.

**Lema 2.2.4** Seja  $F$  um corpo finito. Então

1.  $\frac{\dot{F}}{\dot{F}^2} = \{1, s\}$ .
2. Toda forma quadrática binária sobre  $F$  é universal.

**Demonstração:**

(1) Segue do fato que o grupo multiplicativo  $\dot{F}$  é cíclico, pois  $F$  é finito.

(2) Vamos demonstrar que  $\langle 1, 1 \rangle$  representa  $s$ . Como  $|\dot{F}^2| = \frac{|\dot{F}|}{2} = \frac{q-1}{2}$  pois  $\dot{F}$  é cíclico, então  $|F^2| = \frac{q-1}{2} + 1$ . Portanto  $|s - F^2| = \frac{q-1}{2} + 1$ . Como  $|F^2| + |s - F^2| = 2 \cdot \frac{q-1}{2} + 2 = q + 1 > q = |F|$ , segue-se que  $F^2 \cap (s - F^2)$  não é vazio. Logo existem  $x$  e  $y \in F$  tais que  $x^2 = s - y^2$ . Daí  $s = x^2 + y^2$ , isto é,  $s$  é soma de dois quadrados. Logo  $\langle 1, 1 \rangle$  é universal, pois  $1 \in D \langle 1, 1 \rangle$ . De  $\langle s, s \rangle = \langle s \rangle \cdot \langle 1, 1 \rangle$ , temos que  $D \langle s, s \rangle = s \cdot D \langle 1, 1 \rangle = s \cdot \dot{F} = \dot{F}$ . Como  $\langle 1, s \rangle$  é evidentemente universal o lema está demonstrado. ■

Agora precisamos saber qual é a classe de  $-1$ . Como  $q = p^n$  onde  $p = c(F) \neq 2$  segue-se que  $q \equiv 1 \pmod{4}$  ou  $q \equiv 3 \pmod{4}$ . Da teoria dos números tem-se  $q \equiv 1 \pmod{4}$  se, e somente se,  $-1 \in \dot{F}^2$  e  $q \equiv 3 \pmod{4}$  se, e somente se,  $-1 \notin \dot{F}^2$ . Com isto temos:

**Teorema 2.2.5** Sejam  $F = F_q$  um corpo finito com  $q$  elementos e  $\frac{\dot{F}}{\dot{F}^2} = \{1, s\}$ .

1.  $q \equiv 1 \pmod{4}$  então  $W(F) \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}[\{1, s\}]$ .

2. Se  $q \equiv 3 \pmod{4}$  então  $W(F) \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ .

### Demonstração:

(1) Se  $q \equiv 1 \pmod{4}$ , então  $1 = -1$  em  $\frac{F}{F^2}$ . Assim  $\mathcal{H} = \langle 1, 1 \rangle = \langle s, s \rangle$ , (Veja o Teorema 1.3.2(2)). Seja  $\langle a, b, c \rangle$  uma forma quadrática sobre  $F$ . Como  $\langle a, b \rangle$  é universal pelo Teorema de Representação segue-se que  $\langle a, b, c \rangle$  é isotrópica. Consequentemente as formas quadráticas anisotrópicas sobre  $F$  tem dimensões 1 ou 2. Da Proposição 2.1.3 vem que  $W(F) = \{0, \langle 1 \rangle, \langle s \rangle, \langle 1 \rangle + \langle s \rangle\}$ . Estruturalmente  $W(F)$  é isomorfo a  $\frac{\mathbb{Z}}{2\mathbb{Z}}[\{1, s\}]$ .

(2) Se  $q \equiv 3 \pmod{4}$  então  $1 \neq -1$  em  $\frac{F}{F^2}$ , e podemos considerar  $s = -1 \in \frac{F}{F^2}$ . Daí  $\mathcal{H} = \langle 1, s \rangle = \langle 1, -1 \rangle$ . Como  $\langle 1, 1 \rangle$  representa  $-1$  (Lema 2.2.4), pelo Critério de Representação segue-se que  $q = \langle 1, 1, 1 \rangle$  é isotrópica. Pelo Teorema de Representação  $\langle 1, 1, 1 \rangle = \mathcal{H} + \langle d \rangle$ , e calculando o determinante de  $q$  temos que:  $d = s = -1$ . Logo  $3 \langle 1 \rangle = \langle -1 \rangle$  em  $W(F)$ . Daí  $4 \langle 1 \rangle = \langle 1, -1 \rangle = 0$  em  $W(F)$ . Do mesmo modo  $3 \langle 1 \rangle = - \langle 1, 1, 1 \rangle = - \langle -1 \rangle = \langle 1 \rangle$  e  $4 \langle -1 \rangle = 0$  em  $W(F)$ . Portanto  $W(F) = \{0, \langle 1 \rangle, 2 \langle 1 \rangle, 3 \langle 1 \rangle\}$ , e  $W(F) \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ .





## Capítulo 3

# Formas Quadráticas Sobre Extensões Algébricas

### 3.1 Transfer de Scharlau

Sejam  $F, K$  corpos tais que  $F \subset K$ ,  $(V, q)$  um espaço quadrático com  $b = b_q$  a bilinear associada a  $q$ . Podemos construir  $(V_K, q_K)$  com  $b_K$  associada a  $q_K$  por  $V_K = K \otimes_F V$  e  $b_K : V_K \times V_K \rightarrow K$  a única extensão bilinear tal que  $b_K(k_1 \otimes v_1, k_2 \otimes v_2) = k_1 k_2 b(v_1, v_2)$ , onde  $k_1, k_2 \in K$  e  $v_1, v_2 \in V$ . Como  $V_K$  é um  $K$ -espaço vetorial com o produto  $k_3(k \otimes v) = (k_3 k) \otimes v$  (estende por linearidade), temos que  $b_k$  é uma forma bilinear associada a  $q_K : V_K \rightarrow K$  dada por extensão de  $q_K(k \otimes v) = k^2 q(v)$ ,  $\forall k \in K$  e  $v \in V$ .

Se  $B = \{v_1, \dots, v_n\}$  é uma  $F$ -base de  $V$  então  $B_1 = \{1 \otimes v_1, \dots, 1 \otimes v_n\}$  é uma  $K$ -base de  $V_K$ . De fato todo elemento de  $V_K$  é da forma  $X = \sum_{j=1}^m (k_j \otimes_F u_j) = \sum k_j (1 \otimes u_j)$  por definição da multiplicação. Como  $u_j = \sum \alpha_i u_i$ , com  $\alpha_i \in F \subset K$  temos que  $X = \sum_{j=1}^m k_j (1 \otimes \sum \alpha_i v_i) = \sum k_j \sum \alpha_i (1 \otimes v_i) = \sum \sum \alpha_i k_j (1 \otimes v_i)$ . Se  $\sum \alpha_i (1 \otimes v_i) = 0$ , com  $\alpha_i \in K$  e  $\{e_j\}$  uma  $F$ -base de  $K$ , então  $\alpha_i = \sum \beta_{ji} e_j$ ,  $\beta_{ji} \in F$ , e assim  $\sum (\alpha_i \otimes v_i) = \sum_i (\sum \beta_{ji} e_j) \otimes v_i = \sum_{i,j=1}^m \beta_{ji} (e_j \otimes v_i)$ . Como  $\{e_j \otimes v_i\}$  é uma  $F$ -base de  $K \otimes V$ , então  $\beta_{ji} = 0$ , para qualquer  $\beta_{ji}$  então  $\alpha_i = 0$ , para



todo  $i$ . Logo  $\{1 \otimes v_i\}$  é linearmente independente em  $K$ .

A matriz de  $q_K$  nesta base é da forma  $M_K = [q_K]_{B_i} = (b_K(1 \otimes v_i, 1 \otimes v_j))_{n \times n} = (1.1b(v_i, v_j)) = (b(v_i, v_j)) = M_q = [q]_B$ . Desta forma, segue-se que  $q_K$  é não-singular se, e somente se,  $q$  é não-singular. Também é claro que se  $M = [q]$ ,  $N = [q_1]$  então  $(M + N)_K = M_K + N_K$  ou  $(q + q_1)_K = q_K + q_{1K}$ , ou seja, a construção  $q \mapsto q_K$  induz um homomorfismo de semi-grupo  $M(F) \rightarrow M(K) \rightarrow \hat{W}(K)$ . Pela propriedade universal de  $\hat{W}$ , todo homomorfismo de semi-grupo  $f : M(F) \rightarrow G$ , com  $G$  grupo abeliano, se estende de modo único a um homomorfismo de grupos  $\hat{W}(F) \xrightarrow{\hat{r}^*} \hat{W}(K)$ , onde  $\hat{r}^*(V) = V_K$  e  $\hat{r}^*(q) = q$  ou ainda  $\hat{r}^*(V, q) = (V_K, q_K)$ .

Como a matriz de  $q_1 \otimes q_2$  é o produto de Kronecker  $M.N$  onde  $M = [q_1]$  e  $N = [q_2]$  e  $(M.N)_K = M_K.N_K$  tem-se que  $(q_1 \otimes q_2)_K = q_{1K} \otimes q_{2K}$  ou seja,  $\hat{r}^* : \hat{W}(F) \rightarrow \hat{W}(K)$  é um homomorfismo de anéis. Vejamos:

$$\begin{aligned} \hat{r}^*((q_1 - q_2) \cdot (q_3 - q_4)) &= \hat{r}^*((q_1 \otimes q_3 + q_2 \otimes q_4) - (q_2 \otimes q_3) + (q_1 \otimes q_4)) = r^*(q_1 \otimes q_3) + \\ &r^*(q_2 \otimes q_4) - (r^*(q_2 \otimes q_3) + r^*(q_1 \otimes q_4)) = \hat{r}^*q_1 \otimes \hat{r}^*q_3 + \hat{r}^*q_2 \otimes \hat{r}^*q_4 - (\hat{r}^*q_2 \otimes \hat{r}^*q_3 + \\ &\hat{r}^*q_1 \otimes \hat{r}^*q_4) = (\hat{r}^*(q_1)(\hat{r}^*q_3 - \hat{r}^*q_4) - \hat{r}^*(q_2)(\hat{r}^*q_3 - \hat{r}^*q_4)) = \hat{r}^*(q_1 - q_2) \cdot \hat{r}^*(q_3 - q_4). \end{aligned}$$

Além disso,  $\hat{r}^* : \hat{W}(F) \rightarrow \hat{W}(K)$  induz um homomorfismo de anéis  $r^* : W(F) \rightarrow W(K)$  pois  $\hat{r}^*(\mathbb{Z}H) \subset \mathbb{Z}H$  desde que  $\hat{r}^*(\langle 1, -1 \rangle_F) = \langle 1, -1 \rangle_K = H_K$ .

**Observação 3.1.1** Em geral,  $r^*$  não é monomorfismo. Se  $K$  é uma extensão de  $F$  de grau ímpar, o Teorema de Springer, que veremos adiante, nos dá que  $r^*$  é um monomorfismo e assim  $W(F)$  injeta em  $W(K)$ . No caso em que  $K$  é uma extensão quadrática de  $F$  então  $r^* : W(F) \rightarrow W(K)$  tem núcleo não trivial, a saber, é o ideal de  $W(F)$  gerado por  $\langle 1, -a \rangle$ , onde  $K = F(\sqrt{a})$ . Estes dois teoremas serão demonstrados adiante. Por exemplo,  $r^* : W(\mathbb{R}) \cong \mathbb{Z} \rightarrow W(\mathbb{C}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$  tem núcleo  $2\langle 1 \rangle \cdot W(\mathbb{R})$ .

Uma das ferramentas mais poderosas no estudo das aplicações functoriais  $\hat{r}^*$  e  $r^*$  é a construção de Scharlau da aplicação "transfer", a qual introduziremos agora.

Sejam  $F \subset K$  uma extensão finita,  $s : K \rightarrow F$  um funcional não nulo do  $F$ -espaço vetorial

$K$  e  $(V, b)$  um  $K$ -espaço bilinear. Definimos  $s \circ b : U \times U \rightarrow F$  por  $s \circ b(u, v) = s(b(u, v))$ , para quaisquer  $u, v \in U$ . Então  $(U, s \circ b)$  é um  $F$ -espaço bilinear, pois:  $\forall \alpha \in F, u, v, w \in U, s \circ b(\alpha u + v, w) = s(b(\alpha u + v, w)) = s(\alpha b(u, w) + b(v, w)) = \alpha s(b(u, w)) + s(b(v, w)) = \alpha(s \circ b)(u, w) + (s \circ b)(v, w)$ . Este espaço bilinear será denotado por  $(U, sb)$ .

**Proposição 3.1.2** *Se  $(U, b)$  é um  $K$ -espaço bilinear não-singular, então  $(U, sb)$  é um  $F$ -espaço bilinear não-singular. Em particular, se  $(U, q_b)$  é não-singular, então  $(U, q_{sob})$  é não-singular.*

### Demonstração:

Suponha o contrário. Assim, existe um vetor  $0 \neq u_0 \in U$  tal que  $(sb)(u_0, v) = 0$  para todo  $v \in U$ . Por outro lado, pela regularidade de  $(U, b)$  existe  $v_0 \in U$  tal que  $b(u_0, v_0) \neq 0$ . Para algum escalar  $c \in K$  temos:

$$b(u_0, \frac{c}{b(u_0, v_0)} v_0) = \frac{c}{b(u_0, v_0)} b(u_0, v_0) = c \in K$$

Aplicando o funcional  $s$  a ambos os membros desta equação

$$s(c) = (sb)(u_0, \frac{c}{b(u_0, v_0)} v_0) = 0 \quad \forall c \in K$$

Isto contradiz a hipótese que  $s : K \rightarrow F$  é um funcional não nulo. É evidente que se  $b$  é simétrica então  $sb$  o é. ■

**Notação 3.1.3 :** *Seja  $s : K \rightarrow F$  um funcional linear não-nulo como acima. Se  $(U, q)$  é um espaço quadrático escrevemos  $s_*(q)$  para denotar o espaço quadrático  $U$  sobre  $F$  com a forma bilinear  $sb_q$ . O espaço quadrático  $(U, s_*(q))$  ou simplesmente  $s_*(q)$  é chamado de transfer de  $q$  ou transfer de  $U$ . Assim  $\dim_F s_*(q) = [K : F] \dim_K q$ . Portanto  $\dim_F s_*(q) = [K : F] \dim_K U$ .*

*Esta construção se aplica, em particular, nos espaços quadráticos 1-dimensionais com a formas quadráticas  $q(x) = ax^2$  (ou  $b(x, y) = axy$ ). O transfer  $s_*(\langle 1 \rangle_K)$  tem espaço vetorial subjacente  $K$ , e forma bilinear associada sobre  $F$  dada por:  $(x, y) \mapsto s(xy) \in F$ , ou seja  $(s \circ b)(x, y) = s(\langle 1 \rangle(x, y)) = s(xy)$ .*



**Teorema 3.1.4** (Reciprocidade de Frobenius)

Sejam  $F \subset K$ ,  $r : F \rightarrow K$ ,  $s : K \rightarrow F$  como considerados anteriormente, e considere  $(V, q)$  um espaço quadrático sobre  $F$  e  $(U, q_1)$  um espaço quadrático sobre  $K$ . Então existe uma  $F$ -isometria

$$s_*(r^*(q) \otimes_K q_1) \simeq q \otimes_F s_*(q_1) \quad \text{ou então} \quad s_*((\hat{r}^*(V)) \otimes_K U) \simeq V \otimes_F s_*(U).$$

Em particular, para  $q_1 = \langle 1 \rangle_K$  então  $s_*(\hat{r}^*(q)) \simeq q \otimes_F s_*(\langle 1 \rangle_K)$ .

**Demonstração:**

Note que os espaços vetoriais subjacentes são  $(K \otimes_F V) \otimes_K U$  e  $V \otimes_F U$  como  $F$ -espaços vetoriais.

Seja  $f : s_*((K \otimes_F V) \otimes_K U) \rightarrow V \otimes_F s_*(U)$  a única extensão linear de  $f((k \otimes_F v) \otimes_K u) = v \otimes_F (ku)$ . Então  $f$  é um  $F$ -isomorfismo com inversa  $g : V \otimes_F s_*(U) \rightarrow s_*((K \otimes_F V) \otimes_K U)$  a extensão linear de  $g(v \otimes_F u) = (1 \otimes_F v) \otimes u$ , pois  $g(f((k \otimes_F v) \otimes_K u)) = g(v \otimes_F (ku)) = (1 \otimes_F v) \otimes_K (ku) = k((1 \otimes_F v) \otimes u) = (k \otimes_F v) \otimes_K u$  e  $f(g(v \otimes_F u)) = v \otimes u$ .

Tome  $k, k' \in K, v, v' \in V$  e  $u, u' \in U$ . Seja  $W = V \otimes_F s_*(U)$  e  $b_W$  a bilinear sobre  $W$ . Então  $b_W(f((k \otimes_F v) \otimes_K u), f((k' \otimes_F v') \otimes_K u')) = b_W(v \otimes_F (ku), v' \otimes_F (k'u'))$  que é por definição  $b_V(v, v') \cdot s b_U(ku, k'u') = b_V(v, v') \cdot s(kk' b_U(u, u'))$ .

Por outro lado, calculando em  $s_*((K \otimes_F V) \otimes_K U)$  temos:

$b_{s_*((K \otimes_F V) \otimes_K U)}(k \otimes_F v \otimes u, k' \otimes_F v' \otimes u') = s(b_{(K \otimes_F V) \otimes_K U}(k \otimes_F v \otimes u, k' \otimes_F v' \otimes u')) = s(b_{K \otimes_F V}(k \otimes_F v, k' \otimes_F v') \cdot b_U(u, u')) = s(kk' b_V(v, v') \cdot b_U(u, u')) = b_V(v, v') s(kk' b_U(u, u'))$ , desde que  $b_U(v, v) \in F$  e  $s$  é  $F$ -linear. Logo os dois cálculos mostram que  $f$  é uma  $F$ -isometria de  $s_*((r^*V) \otimes U)$  para  $V \otimes s_*(U)$ . Como  $b_q \simeq b_{q'}$  se, e somente se,  $q \simeq q'$ , o teorema está demonstrado. ■

**Corolário 3.1.5** Se  $(U, q)$  é um espaço hiperbólico sobre  $K$ , então  $(U, s_*(q))$  é um espaço hiperbólico sobre  $F$ .

### Demonstração:

Como  $s_*(q_1 \perp q_2) = s_*(q_1) \perp s_*(q_2)$  podemos assumir que  $q = \mathbb{H}_K$ . Como  $\mathbb{H}_K = \hat{r}^*(\mathbb{H}_F)$ , pela reciprocidade de Frobenius temos:  $s_*(q) = s_*(\mathbb{H}_K) = s_*(\hat{r}^*(\mathbb{H}_F)) \simeq \mathbb{H}_F \otimes_{s_*} (<1>_K)$ . Pela Observação 1.4.3(2) segue-se que  $s_*(q) \simeq [K : F] \cdot \mathbb{H}_F$ . Portanto  $s_*(q)$  é um espaço hiperbólico sobre  $F$ .

**Corolário 3.1.6** (1) A aplicação  $q \longrightarrow s_*(q)$  define um homomorfismo de grupos  $s_* : W(K) \longrightarrow W(F)$ , e

(2) a composição  $W(F) \xrightarrow{r^*} W(K) \xrightarrow{s_*} W(F)$  coincide com a multiplicação por  $s_*(<1>_K)$ .

(3) A imagem de  $s_* : W(K) \longrightarrow W(F)$  é um ideal em  $W(F)$ .

### Demonstração:

Todas as afirmações anteriores seguem da Reciprocidade de Frobenius e do Corolário 3.1.5. Por exemplo, a demonstração do item (3) segue:

Sejam  $q_1 \in W(F)$  e  $s_*(q_2) \in \text{Im } s_*$ . Então pela Reciprocidade de Frobenius  $q_1 \cdot s_*(q_2) = s_*(r^*(q_1) \cdot q_2) \in \text{Im}(s_*)$ . ■

### Observação 3.1.7

(1) Pela reciprocidade de Frobenius temos que  $s_* : W(K) \rightarrow W(F)$  é um isomorfismo de  $W(F)$ -módulos, se considerarmos  $W(K)$  como um  $W(F)$ -módulo via o homomorfismo de anéis  $r^* : W(F) \rightarrow W(K)$ .

(2) Embora  $s_*$  não é um homomorfismo de anéis ele é "functorial", ou seja, se  $F \subset K \subset L$  são extensões finitas e  $s : K \rightarrow F$  é  $F$ -linear,  $t : L \rightarrow K$  é  $K$ -linear e não nulos, então  $(s \circ t)_* = s_* \circ t_*$ .

(3) Se  $s, t : K \rightarrow F$  são não nulos, então  $s_*$  e  $t_* : W(K) \rightarrow W(F)$  são iguais a



menos de um automorfismo de grupos  $\langle b \rangle: W(K) \rightarrow W(K)$ , ou seja,  $t_* = s_* \cdot \langle b \rangle$ , onde  $(s_* \cdot \langle b \rangle)(q) = s_*(\langle b \rangle \cdot q)$ , (ver [L, p. 194]).

### Proposição 3.1.8 (Scharlau)

Seja  $K = F(x)$  uma extensão algébrica simples de grau ímpar. Então  $r^*: W(F) \rightarrow W(K)$  é um monomorfismo.

#### Demonstração:

Pelo Corolário 3.1.6(2) a composição  $W(F) \xrightarrow{r^*} W(K) \xrightarrow{s_*} W(F)$  coincide com a multiplicação por  $s_*(\langle 1 \rangle_K)$ . Se  $s_*(\langle 1 \rangle_K) = \langle 1 \rangle_F$  em  $W(F)$  então  $s_* r^* = 1_{W(F)}$ , e daí  $r^*$  é um monomorfismo. Então basta demonstrar que  $s_*(\langle 1 \rangle_K) = \langle 1 \rangle_F \in W(F)$ .

Sejam  $[K : F] = n = 2m + 1$  e  $B = \{1, x, x^2, \dots, x^{n-1}\}$  uma  $F$ -base para o espaço vetorial  $K$ . Tendo em vista a Observação 3.1.7(3) vamos considerar o funcional linear  $s : K \rightarrow F$  tal que  $s(1) = 1$  e  $s(x) = s(x^2) = \dots = s(x^{n-1}) = 0$ . A forma quadrática  $s_* \langle 1 \rangle_K$  tem espaço vetorial subjacente  $K$  e forma bilinear associada definida de  $K \times K$  em  $F$  por  $(y, z) \rightarrow s(\langle 1 \rangle(y, z)) = s(yz)$ ,  $y, z \in K$ . Como  $K = F \cdot 1 + Fx + \dots + Fx^{n-1}$ , por definição de  $s : K \rightarrow F$  temos que  $F \cdot 1 \perp K_0$  e  $s_*(\langle 1 \rangle_K)|_F = \langle 1 \rangle_F$ , onde  $K_0 = Fx + Fx^2 + \dots + Fx^{n-1}$ . Seja  $q = (s_*(\langle 1 \rangle_K))|_{K_0}$ . Podemos escrever  $s_*(\langle 1 \rangle_K) = \langle 1 \rangle_F \perp q$ . Vamos demonstrar que  $q \simeq mIH$ , ( $n = 2m + 1$ ).

Desde que  $b_{s_*(\langle 1 \rangle_K)}(x^i, x^j) = s(x^{i+j}) = 0$  para  $1 \leq i, j \leq m$  então  $K_0$  é totalmente isotrópico. Pelo Teorema 1.3.4 o subespaço  $Fx + \dots + Fx^m$  está contido no espaço hiperbólico, digamos  $T \subset K_0$  de dimensão  $2m$ . Como  $\dim K_0 = 2m$  segue que  $(K_0, q) \simeq mIH$ , e a demonstração está concluída. ■

### Teorema 3.1.9 (Springer)

Seja  $F \subset K$  uma extensão de grau ímpar. Se uma forma quadrática  $q_F$  é anisotrópica sobre  $F$ , então  $q_K$  é anisotrópica sobre  $K$ .

**Observação 3.1.10** *O Teorema de Springer foi originalmente enunciado como está. A demonstração original pode ser vista em [L] e [S] e foi feita antes da formulação da técnica do Transfer. Apesar de elegante vamos preferir outra demonstração usando a técnica do Transfer. Para isto temos que enunciá-lo de outro modo, usando o anel de Witt. Já sabemos que a classe de uma forma quadrática anisotrópica corresponde de modo único a um elemento do anel de Witt e vice-versa. Logo,*

**Teorema 3.1.11** *Seja  $F \subset K$  uma extensão finita de grau ímpar. Então  $r^* : W(F) \rightarrow W(K)$  é um monomorfismo.*

**Demonstração:**

Desde que  $F \subset L \subset K$ ,  $r^* = (r_1 \circ r_2)^* = r_1^* \circ r_2^*$  onde  $r_1 : L \rightarrow K$  e  $r_2 : F \rightarrow L$  e  $K$  pode ser obtido a partir de  $F$  por uma cadeia de extensões simples  $F = F_0 \subset F_1 \subset \dots \subset F_t = K$ , o Teorema segue da Proposição 3.1.8, aplicando indução sobre o grau  $[K : F]$ . ■

## 3.2 Extensões Quadráticas

Para fechar este capítulo vamos investigar o comportamento de  $r^*$  no caso de uma extensão quadrática.

**Lema 3.2.1** *Seja  $K = F(\sqrt{d})$  uma extensão quadrática de  $F$ , e  $q$  uma forma anisotrópica sobre  $F$ . Então  $q_K$  é isotrópica sobre  $K$  se, e somente se,  $q$  contém a subforma binária  $\langle a \rangle \langle 1, -d \rangle$  onde  $a \in \dot{F}$ .*

**Demonstração**

Temos que a recíproca é clara, desde que  $(\langle a \rangle \langle 1, -d \rangle)_K \simeq \langle a \rangle_K \amalg_K \simeq \amalg_K$ .

Para provarmos a parte "necessária", tome  $\langle a_1, \dots, a_n \rangle$  uma diagonalização de  $q$  e assumamos que  $q_K$  é isotrópica. Existe uma equação  $\sum_{i=1}^n a_i(x_i + y_i\sqrt{d})^2 = 0$  onde  $x_i, y_i \in F$  são não todos nulos. Considerando a parte racional e a parte irracional desta equação, obtemos  $\sum a_i x_i^2 + d \sum a_i y_i^2 = 0$  e  $\sum a_i x_i y_i = 0$ . Este último nos diz que os vetores  $x = (a_1, \dots, a_n)$ ,  $y = (y_1, \dots, y_n)$  são ortogonais no espaço quadrático  $(F^n, q)$ . A outra equação diz que  $q(x) = -dq(y)$  o qual implica que  $x$  e  $y$  devem ambos ser não-nulos, desde que  $q$  é anisotrópico. Consequentemente,  $q$  contém a forma binária  $\langle q(x), q(y) \rangle$ , pois  $x \perp y$ . Então  $\langle q(x), q(y) \rangle = \langle q(y) \rangle \langle 1, q(x)q(y)^{-1} \rangle = \langle q(y) \rangle \langle 1, -d \rangle$ . ■

**Teorema 3.2.2** *Seja  $K = F(\sqrt{d})$  uma extensão quadrática de  $F$ ,  $q$  uma forma anisotrópica sobre  $F$  e  $\delta = \langle 1, -d \rangle$ . Então  $q_K$  é hiperbólico sobre  $K$  se, e somente se, existe uma forma  $\theta$  sobre  $F$  tal que  $q \simeq \delta \otimes \theta$ . Em particular, o núcleo de  $r^* : W(F) \rightarrow W(K)$  coincide com o ideal principal  $W(F) \cdot \delta$ .*

#### Demonstração:

A parte "suficiente" é clara, desde que  $\delta_K \simeq \mathbb{H}_K$ . Para a parte "necessária" fazemos por indução sobre a  $\dim q$ . Para  $\dim q = 0$  é trivial. Se  $\dim q > 0$ , o Lema anterior fornece uma isometria  $q \simeq \langle a \rangle \delta \perp q'$ , onde  $a \in \dot{F}$ , e  $\dim q' = \dim q - 2$ . Pelo Teorema do Cancelamento de Witt (1.3.10)  $(q')_K$  é hiperbólico. Pela hipótese de indução existe uma forma  $\theta'$  tal que  $q' \simeq \delta \otimes \theta'$ . Temos agora que  $q \simeq \langle a \rangle \delta \perp (\delta \otimes \theta') \simeq \delta \otimes \theta$ , onde  $\theta = \langle a \rangle \perp \theta'$  ■

**Teorema 3.2.3** *Com as mesmas notações acima, seja  $t : K \rightarrow F$  uma aplicação  $F$ -linear definida por  $t(1) = 0$ ,  $t(\sqrt{d}) = 1$ . Seja  $t_* : W(K) \rightarrow W(F)$  o transfer definido por  $t$ . Então a seguinte sequência é exata:*

$$0 \rightarrow W(F) \cdot \delta \rightarrow W(F) \xrightarrow{r^*} W(K) \xrightarrow{t_*} W(F)$$

#### Demonstração:

Pelo Teorema 3.2.2 basta mostrar que  $\text{Im}(r^*) = \ker(t_*)$ . Primeiramente, mostremos que  $t_* r^* = 0$ . Para  $a \in \dot{F}$ , o  $F$ -espaço quadrático  $t_* r^* \langle a \rangle$  tem espaço vetorial subjacente  $K$  e



forma bilinear  $(x, y) \longrightarrow t_{\star} r^{\star} \langle a \rangle (x, y) = t_{\star}(\langle a \rangle_K (x, y)) = t(axy)$ . Desde que  $\dim_F K = 2$  e  $(\sqrt{d}, \sqrt{d}) \longrightarrow t(a, d) = 0$ , segue-se que  $t_{\star} r^{\star} \langle a \rangle$  é o plano hiperbólico (Teorema 3.2.2). Como  $t_{\star} r^{\star} q = t_{\star} r^{\star}(\langle a_1, \dots, a_n \rangle) = \sum_{i=1}^n t_{\star} r^{\star} \langle a_i \rangle = 0$ , para todo  $q \simeq \langle a_1, \dots, a_n \rangle \in W(F)$ . Reciprocamente, se  $q$  (ou  $B$ ) é uma forma quadrática anisotrópica sobre  $K$  tal que  $t_{\star}(q)$  é  $F$ -hiperbólico, então existe  $0 \neq v \in V$  tal que  $t(q(v)) = 0$  (ou  $t(b(v, v)) = 0$ ). A definição de  $t$  mostra que  $a = q(v) \in \dot{F}$ . Então nós temos uma  $K$ -fatoração  $q \simeq \langle a \rangle_K \perp q'$ . Desde que  $t_{\star}(\langle a \rangle_K) = t_{\star} r^{\star}(\langle a \rangle)$  é hiperbólico (ou seja, nulo em  $W(F)$ ) como mostrado acima, o Teorema do cancelamento de Witt implica que  $t_{\star}(q')$  é também hiperbólico. Agora uma indução sobre  $\dim_K q$  mostra que a classe de isometria de  $q$  pertence a  $Im(r^{\star})$  ■

Fechados

## 4.1 Corpos Ordenados

Um corpo ordenado é um par  $(K, \leq)$  onde  $K$  é um corpo e  $\leq$  é uma relação de ordem total em  $K$  satisfazendo as propriedades:

1. Se  $a \leq b$  e  $c \leq d$ , então  $a + c \leq b + d$ .
2. Se  $a \leq b$  e  $c > 0$ , então  $ac \leq bc$ .

Um corpo ordenado é dito positivo se  $1 > 0$ . Neste caso, podemos definir a norma  $|x|$  em  $K$  por:

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

onde  $x \geq 0$  significa que  $x$  é positivo. A norma  $|x|$  satisfaz as propriedades:

1.  $|x| \geq 0$  e  $|x| = 0$  se e somente se  $x = 0$ .
2.  $|x + y| \leq |x| + |y|$ .
3.  $|xy| = |x||y|$ .

Um corpo ordenado é dito completo se toda sequência crescente e limitada superiormente em  $K$  converge para um elemento de  $K$ . Um exemplo clássico de corpo ordenado completo é o corpo dos números reais  $\mathbb{R}$ . Outro exemplo importante é o corpo dos números  $p$ -ádicos  $\mathbb{Q}_p$ , onde  $p$  é um número primo. A completude é uma propriedade importante que garante a existência de limites para certas sequências, o que é fundamental para a análise matemática.



## Capítulo 4

# Corpos Formalmente Reais e Reais Fechados

### 4.1 Corpos Ordenados

Uma *ordem de  $F$*  ou (*sobre  $F$* ) é uma relação binária  $\preceq$  sobre  $F$  que é reflexiva, anti-simétrica e transitiva e é compatível com a estrutura do corpo  $F$ , isto é,  $a \preceq b$  implica que  $a + c \preceq b + c$ ; e se  $0 \preceq a$  e  $0 \preceq b$  então  $0 \preceq ab$ , quaisquer que sejam  $a, b$  e  $c$  em  $F$ . Além disso, exige-se que a ordem seja *total*, ou seja, quaisquer dois elementos de  $F$  são comparáveis; o que significa que,  $a \preceq b$  ou  $b \preceq a$ ,  $\forall a, b \in F$ .

Nestas condições se considerarmos  $P = \{x \in \dot{F} \mid 0 \preceq x\}$ , pode-se demonstrar que qualquer que seja  $x \in \dot{F}$ ,  $x$  ou  $-x$  pertence a  $P$  (não ambos). Além disso  $P$  é fechado para a adição e para a multiplicação. Reciprocamente se existe em  $F$  um subconjunto  $P$  com as propriedades mencionadas anteriormente, então a relação definida por  $a \preceq_P b$  se, e somente se,  $b - a \in P \cup \{0\}$  é uma relação de ordem total em  $F$ . A correspondência entre ordens totais de  $F$  e subconjuntos  $P$  de  $F$  com as propriedades acima é 1-1. Portanto sem ambiguidade podemos definir:



**Definição 4.1.1** Uma *ordem* de  $F$  é um subconjunto  $P \subset F$  (chamado elementos positivos da ordem) que possui as seguintes propriedades:

$$(P_1) \quad 0 \notin P$$

$$(P_2) \quad \text{Se } 0 \neq x \in F, \text{ então ou } x \in P \text{ ou } -x \in P.$$

$$(P_3) \quad P \text{ é fechado para a multiplicação e para a adição.}$$

Denotaremos por  $N$  o conjunto dos elementos negativos de  $F$ , relativos a ordem  $P$  definido por

$$N := -P = \{-y \mid y \in P\}.$$

Dessa forma, temos que  $F$  é a união disjunta de  $\{0\}$ ,  $P$ ,  $N$ . Usualmente, a notação  $x \prec y$ , significará  $y - x \in P$  (e  $x \preceq y$  significa que  $y - x \in P \cup \{0\}$ ).

Se  $F_0$  é um subcorpo de  $F$  podemos ordenar  $F_0$  definindo  $P_0 = F_0 \cap P$  como o conjunto dos elementos positivos em  $F_0$ . Esta ordem é dita ser *induzida* pela ordem  $P$  de  $F$ .

Para um dado corpo  $F$ , temos que as seguintes condições são equivalentes:

$$(i) \quad -1 \text{ não é soma de quadrados}$$

$$(ii) \quad \text{Para qualquer número natural } n > 0, \text{ a forma quadrática } n \langle 1 \rangle \text{ é anisotrópica sobre } F.$$

De fato, para algum  $n \in \mathbb{N}^*$ ,  $n \langle 1 \rangle$  é isotrópica se, e somente se, existem  $x_1, \dots, x_n \in F$ , não todos nulos tais que  $\sum_{i=1}^n x_i^2 = 0$ . Isto equivale a  $\sum_{i=1, i \neq j}^n x_i^2 = -x_j^2$ , onde  $x_j \neq 0$ . Equivalentemente  $\exists n \in \mathbb{N}^*$ , tal que  $\sum_{i=1, i \neq j}^n \left(\frac{x_i}{x_j}\right)^2 = -1$ .

Desta forma, temos que  $-1$  não é soma de quadrados, se, e somente se,  $n \langle 1 \rangle$  é anisotrópica sobre  $F$ ,  $\forall n \in \mathbb{N}^*$ . ■

**Definição 4.1.2** Um corpo  $F$  é dito *formalmente real*, se satisfaz as duas condições anteriores.

Claramente, temos que os corpos formalmente reais  $F$  têm característica zero, pois se  $\text{car}(F) = p > 0$ ,  $p$  primo em  $\mathbb{Z}$ , então a forma  $p < 1 >$  é anisotrópica, o que gera uma contradição, pois  $p \cdot 1 = 0$ .

**Notação 4.1.3** Para um corpo  $F$  arbitrário, denote por  $\sigma(F)$  o conjunto de elementos de  $F$  que podem ser expressos como uma soma de quadrados. Isto é:

$$\sigma(F) = \{x \in F \mid x = \sum_{i=1}^n x_i^2, x_i \in F, n \in \mathbb{N}^*\}$$

**Proposição 4.1.4** (i)  $\sigma(F)$  é fechado para a adição e  $\sigma(F) - \{0\}$  é um subgrupo multiplicativo de  $F$ .

(ii) Se  $F$  não é formalmente real (e  $\text{car}(F) \neq 2$ ), então  $\sigma(F) = F$ . (Se  $\text{car}(F) = 2$ ,  $\sigma(F) = F^2$ )

**Demonstração:** (i) Tome  $0 \neq x = x_1^2 + \dots + x_n^2$  em  $F$ . Então  $\frac{1}{x} = \frac{x}{x^2} = (\frac{x_1}{x})^2 + \dots + (\frac{x_n}{x})^2 \in \sigma(F)$ . O restante das afirmações em (i) são mais simples ainda.

(ii) Tome  $x \in F$ . Desde que o plano hiperbólico  $< 1, -1 >$  é universal, existe  $y, z \in F$  tal que  $x = y^2 - z^2$ . Como  $-1 \in \sigma(F)$ , pois  $n < 1 >$  é isotrópica para algum  $n$ , temos que  $x = y^2 + (-1)z^2 \in \sigma(F) + \sigma(F)\sigma(F) \subset \sigma(F)$ . Consequentemente,  $F \subset \sigma(F)$ . Como  $\sigma(F) \subset F$  é trivial, concluímos que  $\sigma(F) = F$ .

Se  $\text{car}(F) = 2$ ,  $x^2 + y^2 = (x + y)^2$  e daí por indução temos que  $\sum x_i^2 = (\sum x_i)^2$  ■

**Proposição 4.1.5** Sejam  $F$  um corpo e  $P$  uma ordem de  $F$ . Então

(1)  $\sigma(F) - \{0\} \subset P$

(2)  $F$  é formalmente real (em particular, possui característica zero)



(3) Se  $P' \subset F$  é uma outra ordem sobre  $F$ , temos: Se  $P \subset P'$ , então  $P = P'$ .

### Demonstração:

(1) Tome  $0 \neq x = x_1^2 + \dots + x_n^2$ . Podemos assumir que cada  $x_i \neq 0$ . Se  $x_i \in P$ , claramente  $x_i^2 \in P$ . Caso contrário,  $-x_i \in P$  e daí  $x_i^2 = (-x_i)(-x_i) \in P$ . Como  $P$  é fechado para adição segue-se que  $x \in P$ .

(2) Desde que  $1 = 1^2 \in P$  temos que  $-1 \notin P$ , (senão  $0 = 1 + (-1) \in P$ , uma contradição). Por (1) obtemos que  $-1 \notin \sigma(F)$ . Isto é,  $F$  é formalmente real.

(3) Se  $P \subset P'$  e  $P \neq P'$ , existe  $x \in F$  tal que  $x \in P'$  e  $x \notin P$ . Então  $-x \in P \subset P'$  (por hipótese). Daí  $x$  e  $-x \in P'$ , uma contradição. Portanto  $P' = P$ . ■

**Lema 4.1.6** Se  $F$  é formalmente real mas a extensão quadrática  $F(\sqrt{a})$  não é formalmente real, então  $-a \in \sigma(F)$ .

### Demonstração:

Em  $F(\sqrt{a})$ , existe uma equação  $-1 = \sum (b_i + c_i \sqrt{a})^2$ , onde  $b_i, c_i \in F$ . Desenvolvendo obtemos  $-1 = \sum (b_i^2 + a c_i^2) + (\sum 2 b_i c_i) \sqrt{a}$  em  $F(\sqrt{a})$ . Assim  $-1 = \sum b_i^2 + a(\sum c_i^2)$ . Dessa forma  $-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$ . Seja  $c := \sum c_i^2$ . Então  $-a = \frac{1}{c} + \frac{\sum b_i^2}{c} = \frac{c}{c^2} + \frac{\sum c b_i^2}{c^2}$ . Segue-se que  $-a = c(\frac{1}{c})^2 + c \sum (\frac{b_i}{c})^2$ . Como  $\sigma(F) - \{0\}$  é um grupo (Proposição 4.1.4), concluímos que  $-a \in \sigma(F)$ .

**Definição 4.1.7** Um corpo  $F$  é chamado *pitagoriano* se a soma de dois quadrados (ou se qualquer soma de um número finito de quadrados em  $F$ ) é sempre um quadrado.

Para verificar se um corpo  $F$  é pitagoreano é suficiente mostrar que  $1 + y^2$  é um quadrado para todo  $y \in F$ .

É claro que se  $F$  é pitagoreano então  $\sigma(F) = F^2$ .





## 4.2 Corpos Reais Fechados

**Definição 4.2.1** Um corpo  $F$  é chamado *real-fechado*, se  $F$  é formalmente real e nenhuma extensão algébrica própria de  $F$  é formalmente real.

**Proposição 4.2.2** Se  $F$  é real-fechado, então  $F$  é pitagoriano.

### Demonstração:

Suponha que  $x = 1 + y^2$  não seja um quadrado. Então  $F(\sqrt{x})$  é uma extensão própria de  $F$  e portanto não é formalmente real, pois  $F$  é real-fechado por hipótese. Pelo Lema 4.1.6,  $-x \in \sigma(F)$ , então existe  $z_1, \dots, z_n \in F$  tais que  $\sum z_i^2 = -x = -1 - y^2$ . Logo  $-1$  é soma de quadrados em  $F$ . Uma contradição, pois  $F$  é formalmente real. Portanto,  $F$  é pitagoriano. ■

O próximo Teorema tratará da estrutura dos corpos reais-fechados.

**Teorema 4.2.3** Seja  $F$  um corpo real-fechado. Então:

- (i) Para todo  $0 \neq x \in F$ , temos que  $x \in \dot{F}^2$  ou  $-x \in \dot{F}^2$ .
- (ii)  $F$  tem uma única ordem  $P$ , a saber  $P = \dot{F}^2$ .

### Demonstração:

(i) Suponha que  $x \notin \dot{F}^2$ . Como  $F$  é real-fechado, então  $F\sqrt{x}$  não é formalmente real. Pelo Lema 4.1.6,  $-x \in \sigma(F) - \{0\}$ . Mas  $F$  é pitagoreano (pela Proposição 4.2.2), e então  $\sigma(F) - \{0\} = \dot{F}^2$ . Consequentemente,  $-x \in \dot{F}^2$ .

(ii) Verifiquemos que  $\dot{F}^2$  é uma ordem de  $F$ .

O axioma  $(P_1)$  da Definição 4.1.1 é óbvia.  $(P_2)$  segue do item (i). Para demonstrarmos  $(P_3)$  note que  $\dot{F}^2$  é claramente fechado para a multiplicação e a condição  $P + P \subset P$  segue da



Proposição 4.2.2. Como  $\dot{F}^2$  está contido em qualquer ordem  $P'$ , a unicidade segue da Proposição 4.1.5(3). ■

Um exemplo clássico de corpo real-fechado é o corpo dos números reais  $\mathbb{R}$ .

**Proposição 4.2.4** *Seja  $F$  um corpo formalmente real e  $\overline{F}$  o fecho algébrico de  $F$ . Então, existe um corpo real fechado  $\Delta$  entre  $F$  e  $\overline{F}$ .*

**Demonstração:**

Considere a coleção  $\mathcal{S}$  de todos subcorpos formalmente reais de  $\overline{F}$ . Observe que  $F \in \mathcal{S}$ , e então  $\mathcal{S} \neq \emptyset$ .

Se  $\{F_\alpha\}$  é uma cadeia (relativa à inclusão) de tais subcorpos, então  $F_0 = \bigcup_{\alpha} F_\alpha$ , claramente pertence a mesma coleção  $\mathcal{S}$ . Pelo Lema de Zorn, existe um elemento maximal  $\Delta \in \mathcal{S}$ . Pela maximalidade de  $\Delta$  segue-se que  $\Delta$  é real-fechado. ■

**Corolário 4.2.5** *Um corpo  $F$  é formalmente real se, e somente se,  $F$  possui pelo menos uma ordem.*

**Demonstração:**

Suponha que  $F$  é um corpo formalmente real. Pela Proposição 4.2.4, existe uma extensão algébrica  $\Delta \supset F$  real-fechado. A única ordem de  $\Delta$  (pelo Teorema 4.2.3) induz uma ordem sobre  $F$ . A recíproca segue da Proposição 4.1.5(2). ■

**Definição 4.2.6** Um elemento  $b \in \dot{F}$  é chamado *totalmente positivo* se ele é positivo em todas as possíveis ordens de  $F$ .

**Corolário 4.2.7 (Artin-Schreier)** *Sejam  $F$  um corpo qualquer e  $b \in \dot{F}$ . Então  $b$  é totalmente positivo se, e somente se,  $b \in \sigma(F)$ .*



### Demonstração:

Primeiramente vejamos o caso de  $F$  não ser formalmente real. Se  $F$  não é formalmente real, então pela Proposição 4.1.4, todo  $b \in \dot{F}$  pertence a  $\sigma(F)$ , pois  $\sigma(F) = F$ . A conclusão segue por vacuidade, desde que  $F$  não admite ordens.

Para  $F$  formalmente real, suponha  $b \notin \sigma(F)$ . Pelo Lema 4.1.6,  $K = F(\alpha)$  é formalmente real, onde  $\alpha\sqrt{-b}$ . Escolha uma ordem sobre  $K$  (isto é possível pelo Corolário 4.2.5). Esta, induz uma ordem sobre  $F$ , na qual  $b$  é negativo, pois  $b = -(\alpha)^2$ . Consequentemente,  $b$  é totalmente positivo, então  $b \in \sigma(F)$ . A recíproca segue da Proposição 4.1.4(1). ■

**Observação 4.2.8** *Os corpos  $F$  reais fechados possuem algumas caracterizações e várias propriedades, como por exemplo:  $F$  é real fechado se, e somente se,  $\sqrt{-1} \notin F$  e  $F(\sqrt{-1})$  é algebricamente fechado; equivalentemente,  $F$  tem apenas duas classes de quadrados e todo polinômio sobre  $F$  de grau ímpar tem uma raiz em  $F$ . Outras propriedades destes corpos podem ser vistas em [L, Cap. viii]. Algumas propriedades deste corpo de interesse para nós serão desenvolvidas a seguir. Por exemplo, é de fundamental importância para o que segue o anel de Witt de um corpo real fechado  $F$ . Pelo Teorema 4.2.3 temos que  $\frac{\dot{F}}{F^2} = \{1, -1\}$  e como  $F$  é formalmente real o exemplo 2.2.2 de anéis de Witt nos dá que  $W(F) \simeq \mathbb{Z}$ .*

**Definição 4.2.9** Seja  $F$  um corpo e  $P$  uma ordem de  $F$ . Uma extensão  $\Delta \supset F$  é dita *fecho-real* de  $F$ , (relativo a  $P$ ) se  $\Delta$  satisfaz as seguintes condições:

- (i)  $\Delta$  é real-fechado.
- (ii)  $\Delta$  é uma extensão algébrica de  $F$  (não necessariamente finita).
- (iii) A ordem  $P$  de  $F$  é induzida pela uma única ordem de  $\Delta$ , ou seja,  $P = \dot{\Delta}^2 \cap F$ .

A seguir vamos demonstrar que todo corpo ordenado possui fecho real.





**Lema 4.2.10** *Seja  $F$  um corpo ordenado por  $P$  e  $\Omega$  o fecho algébrico de  $F$ . Seja  $E$  o subcorpo de  $\Omega$  obtido por adjunção à  $F$  de todas as raízes quadradas de todos os elementos de  $P$ . Então  $E$  é formalmente real.*

**Demonstração:**

Suponha que  $\sum a_i^2 = 0$ ,  $a_i \in E$ . Os  $a_i$ 's estão todos contidos numa extensão finita de  $F$  da forma:  $F(\sqrt{b_1}, \dots, \sqrt{b_r})$ , onde  $b_i \in P$ . Assim, é suficiente mostrar que qualquer extensão  $F(\sqrt{b_1}, \dots, \sqrt{b_r})$  é formalmente real e para verificarmos isto estabeleceremos as seguintes afirmações:

Se  $\sum c_i a_i^2 = 0$ , onde  $c_i \in P$  e  $a_i \in F(\sqrt{b_1}, \dots, \sqrt{b_r})$  então  $a_i = 0$ , para qualquer  $i$ . (\*)

Esta demonstração será feita por indução sobre  $f := [F(\sqrt{b_1}, \dots, \sqrt{b_r}) : F]$ . Se este grau é 1, temos  $a_i \in F$ ,  $c_i \in P$ , para qualquer  $i$ . Se  $a_i \neq 0$ , então  $a_i^2 \in P$ . Portanto  $c_i a_i^2 \in P$ . Como  $P$  é fechado para a soma e para a multiplicação temos que  $\sum c_i a_i^2 \in P$ , uma contradição. Assumamos  $f > 1$ . Também podemos assumir que  $F(\sqrt{b_1}, \dots, \sqrt{b_{r-1}}) \subsetneq F(\sqrt{b_1}, \dots, \sqrt{b_r})$ . Na afirmação (\*) escreva  $a_i = x_i + y_i \sqrt{b_r}$ ,  $x_i, y_i \in F(\sqrt{b_1}, \dots, \sqrt{b_{r-1}})$ . Então:  $0 = \sum c_i a_i^2 = \sum c_i (x_i + y_i \sqrt{b_r})^2 = (\sum c_i x_i^2 + \sum b_r c_i y_i^2) + 2 \sum c_i x_i y_i \sqrt{b_r}$ . Em particular, o termo entre parênteses é zero. Como  $c_i \in P$  e  $b_r \in P$ , por a hipótese de indução obtemos que  $x_i = y_i = 0$ . Assim  $a_i = 0$ , para todo  $i$ . ■

Sejam  $F_1$  e  $F_2$  corpos ordenados por  $P_1$  e  $P_2$ , respectivamente. Dizemos que  $f : F_1 \rightarrow F_2$  é um *homomorfismo ordenado* ou *compatível com as ordens  $P_1$  e  $P_2$*  se  $f(P_1) \subset P_2$ .

O Teorema seguinte afirma que as possíveis ordens de um corpo  $F$  estão em correspondência um-a-um com os fechos reais de  $F$  que são dois a dois não isomorfos.

**Teorema 4.2.11** (i) *Todo corpo ordenado  $F$  possui um fecho real relativo a ordem considerada.*

(ii) *Se  $F_1, F_2$  são corpos ordenados, e  $\Delta_1, \Delta_2$  são seus fechos reais relativos às respectivas*



ordens. Então qualquer isomorfismo ordenado  $f : F_1 \rightarrow F_2$  estende de modo único à um isomorfismo  $\tilde{f} : \Delta_1 \rightarrow \Delta_2$ , que é automaticamente um isomorfismo ordenado

### Demonstração:

Seja  $F$  um corpo ordenado por um conjunto de elementos positivos  $P$ . Seja  $E$  a extensão de  $F$  definida no Lema 4.2.10, a qual é formalmente real. Pela Proposição 4.2.4 existe um corpo  $\Delta$  real-fechado em  $\Omega$  contendo  $E$ . Afirmamos que  $\Delta$  é um fecho real de  $F$  relativo à  $P$ .

Para demonstrarmos a afirmação acima resta demonstrarmos que  $P = \dot{\Delta}^2 \cap F$ . Pelo Corolário 4.1.5(3) basta demonstrarmos que  $P \subset \dot{\Delta}^2 \cap F$ . Para qualquer  $b \in P$ ,  $\sqrt{b} \in E \subset \Delta$ . Assim  $b \in \dot{\Delta}^2 \cap F$ . Logo  $P \subset \dot{\Delta}^2 \cap F$ . A demonstração de (ii) que implica na unicidade do fecho real e será demonstrada no capítulo seguinte (Teorema 5.1.9). ■

Para encerrarmos esta seção discutiremos um exemplo que, em particular mostra a existência de corpos pitagoreanos formalmente reais com  $2^n$ -classes de quadrados, para  $n$  arbitrário.

Seja  $F$  com corpo de característica diferente de 2 e denote por  $F_1 := F((t))$  o "corpo de séries formais de Laurent" sobre  $F$ . O corpo  $F_1$  consiste de todas as séries formais de Laurent do tipo  $f = a_m t^m + a_{m+1} t^{m+1} + \dots$ , ( $m \in \mathbb{Z}$ ), com a adição e multiplicação usual de séries. Podemos escrever  $f$  na forma  $f = t^m(a_m + a_{m+1}t + \dots)$ . Assim se  $g = t^n(b_n + b_{n+1}t + \dots)$  então  $f = g$  se, e somente se,  $n = m$  e  $(a_m + a_{m+1}t + \dots) \equiv b_n + b_{n+1}t + \dots \pmod{t^s}$ ,  $\forall s \in \mathbb{N}$ . Se  $h = 1 + c_1 t + c_2 t^2 + \dots \in F_1$ , por indução sobre  $s$  encontramos  $h_1 \in F_1$  tal que  $h \equiv h_1^2 \pmod{t^s}$ . Em outros termos,  $h$  é um quadrado em  $F_1$ . Este fato será usado na próximo exemplo.

**Exemplo 4.2.12** Sejam  $F$  um corpo,  $\preceq$  uma ordem de  $F$  e  $F_1 = F((t))$ . Então

(1) Existem precisamente duas ordens de  $F_1$  que estende  $\preceq$ . Em uma delas  $t$  é positivo e na outra  $t$  é negativo. Em particular, se  $F$  é formalmente real,  $F_1$  também o é.

(2) Se  $F$  é pitagoreano então  $F_1$  também é pitagoreano.

(3) Se  $F$  é real fechado, então  $F_n = F((t_1) \dots (t_n))$  é um corpo pitagoreano com  $2^{n+1}$  classes de quadrados.

### Demonstração:

(1) Se  $f = a_m t^m + a_{m+1} t^{m+1} \dots$ , com  $a_m \neq 0$ , dizemos  $0 \prec_1 f$  se, e somente se,  $0 \prec a_m$ . Então  $\preceq_1$  é uma ordem sobre  $F_1$  e a demonstração deste fato será omitida. Vejamos que esta é a única ordem estendendo a ordem original  $\preceq$  de  $F$ , na qual  $t$  é positivo.

Expressemos  $f$  na forma  $f = a_m t^m (1 + e_1 t + \dots)$  (colocando  $a_m t^m$  em evidência). Como  $1 + e_1 t + e_2 t^2 + \dots$  é um quadrado em  $F_1$ , podemos escrever  $f$  na forma  $f = a_m t^m (g(t))^2$ . Agora seja  $\preceq_2$  outra ordem de  $F_1$  estendendo  $\preceq$ , na qual  $0 \prec_2 t$ . Se  $0 \prec_2 f = a_m t^m (g(t))^2$  então  $0 \prec_2 a_m$  (pois  $0 \prec_2 t^m$  e  $0 \prec_2 g(t)^2$ ). Logo  $0 \prec_1 f$ , ou seja  $P_2 \subset P_1$ . Pela Proposição 4.1.5(3) tem-se que  $\preceq_1$  e  $\preceq_2$  são iguais.

Observando que  $t$  e  $-t$  tem o mesmo papel em  $F_1$ , isto é,  $t \rightarrow -t$  induz um  $F$ -automorfismo  $\sigma$  de  $F_1$ , obtemos (por definição) que  $\sigma(P_{\preceq_1}) := P$  é um conjunto de elementos positivos de uma ordem  $\preceq_2$ . Assim  $F_1$  também tem uma única ordem estendendo  $\preceq$ , na qual  $t$  é negativo. Nesta nova ordem  $f = a_m t^m + \dots$  é positivo se, e somente se  $0 \prec (-1)^m a_m$ . Isto demonstra (1).

(2) Do item (1) temos que  $F_1$  é formalmente real. Mostremos que  $F_1$  é pitagoreano. Considere  $f^2 + g^2$ , onde  $f = a_m t^m + \dots$ , e  $g = b_n t^n + \dots$ ,  $a_m \neq 0$ ,  $b_n \neq 0$ . Se  $m < n$ , então  $f^2 + g^2 = (a_m t^m)^2 (1 + \dots)$  é um quadrado em  $F_1$  como vimos a pouco no item (1).

Se  $m = n$ , escreva  $a_m^2 + b_m^2 = c_m^2$ ,  $c_m \in F$ , pois  $F$  pitagoreano. Como, por hipótese,  $F$  é formalmente real, temos que  $c_m \neq 0$ . Temos agora  $f^2 + g^2 = 2(c_m t^m)^2 (1 + \dots)$ , novamente, um quadrado em  $F_1$ . Isto conclui (2).

(3) Segue de (2) e do Corolário 4.2.2.



## 4.3 O Espectro Primo do Anel de Witt

Nesta seção estudaremos o conjunto de todos ideais primos do anel comutativo  $W(F)$ , chamado "espectro primo". Determinaremos este conjunto e veremos que ele está intimamente relacionado com os conjunto das ordens de um corpo.

Se  $\mathcal{P}$  é um ideal primo em um anel comutativo  $A$ , e o domínio  $\frac{A}{\mathcal{P}}$  tem característica  $p$  (primo ou também zero), por conveniência, diremos que  $\mathcal{P}$  tem característica  $p$ .

Para o que vem a seguir precisaremos da

**Definição 4.3.1** Sejam  $q = \langle a_1, a_2, \dots, a_n \rangle$  uma forma quadrática sobre um corpo ordenado  $F$  e  $P$  a ordem de  $F$ . A assinatura de  $q$  (relativa a  $P$ ) é o número inteiro  $\text{sign}_P q = n_+ - n_-$ , onde  $n_+ = |\{a_1, a_2, \dots, a_n\} \cap P|$ , e  $n_- = |\{a_1, a_2, \dots, a_n\} \cap -P|$ . Ou seja: a assinatura da forma quadrática  $q$  é o número de elementos positivos menos o número de elementos negativos segundo a ordem  $P$ .

Denota-se também,  $\text{sign}_P q$  por  $\text{sign}_\alpha q$  onde  $\alpha$  é a ordem de  $F$  tal que  $P_\alpha = P$ . Tendo em vista o Teorema 4.2.3, que diz que os elementos  $a_i$ 's se reduzem a 1 ou  $-1$  no fecho real de  $F$  temos que  $\text{sign}_\alpha q = r^*(q) \in W(F_\alpha) \simeq \mathbb{Z}$ , onde  $F_\alpha$  é o fecho real de  $F$  relativamente a ordem  $\alpha$ .

**Lema 4.3.2** Seja  $\mathcal{P}$  um ideal primo em  $W(F)$  de característica  $p$  (um número primo ou zero). Então  $\frac{W(F)}{\mathcal{P}} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ .

**Demonstração:**

Como  $\frac{W(F)}{\mathcal{P}}$  é um domínio de integridade e  $(\langle a \rangle + 1)(\langle a \rangle - 1) = 0 \in W(F)$ , temos que  $\langle a \rangle - 1 \in \mathcal{P}$  ou  $\langle a \rangle + 1 \in \mathcal{P}$  e assim cada  $\langle a \rangle = 1 \pmod{\mathcal{P}}$  ou  $\langle a \rangle = -1 \pmod{\mathcal{P}}$ , para qualquer  $a \in \dot{F}$ . Como  $W(F)$  é aditivamente gerado por  $\langle a \rangle$ ,  $a \in \dot{F}$ , segue que o grupo  $\frac{W(F)}{\mathcal{P}}$  é cíclico (gerado pela imagem de  $\langle 1 \rangle$ ) e portanto  $\frac{W(F)}{\mathcal{P}} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ . ■



**Teorema 4.3.3** *Há uma correspondência natural um-a-um entre ideais primos de  $W(F)$  de característica zero e as diferentes ordens sobre o corpo  $F$ .*

**Demonstração:**

Para uma ordem  $\alpha$  de  $F$  (se existir uma), seja  $F_\alpha$  o fecho real de  $F$  relativo a ordem  $\alpha$ .

Sejam  $r_\alpha^* : W(F) \rightarrow W(F_\alpha)$  o homomorfismo induzido pela inclusão  $r : F \rightarrow F_\alpha$  e  $\mathcal{P}_\alpha = \ker r_\alpha^*$ . Pelo Teorema do Isomorfismo  $\frac{W(F)}{\mathcal{P}_\alpha} = \text{Im } r_\alpha^* = \mathbb{Z}$  (domínio). Logo  $\mathcal{P}_\alpha = \ker r_\alpha^*$  é um ideal primo de característica zero. Podemos ver que para todo  $a \in \dot{F}$ ,  $a \in P_\alpha \iff a \equiv 1 \pmod{\mathcal{P}_\alpha}$ .

De fato, como  $P_\alpha = \dot{F}^2 \cap F$  então  $a \in P_\alpha$  se, e somente se,  $a \in \dot{F}^2 \cap F \iff \langle a, -1 \rangle = 0$  em  $W(F_\alpha) \iff a \equiv 1 \pmod{\mathcal{P}_\alpha}$ . Este fato serve como motivação para construir a correspondência inversa: dado um ideal primo  $\mathcal{P}$  de característica zero (ou característica diferente de 2), vamos construir uma ordem  $\alpha_{\mathcal{P}}$  de  $F$ . Definimos o conjunto dos elementos positivos da seguinte forma:

$$P_{\mathcal{P}} = \{a \in F \mid \langle a \rangle \equiv 1 \pmod{(\mathcal{P})}\}.$$

Verifiquemos  $P_{\mathcal{P}}$  é uma ordem:

(i)  $0 \notin P_{\mathcal{P}}$ , é claro.

(ii) Seja  $a \in \dot{F}$  e  $a \notin P_{\mathcal{P}}$ . Então  $\langle a \rangle \not\equiv 1 \pmod{(\mathcal{P})}$  e assim  $\langle a \rangle \equiv -1 \pmod{(\mathcal{P})}$ . Isto implica que  $\langle -a \rangle \equiv 1 \pmod{(\mathcal{P})}$ , isto é,  $-a \in P_{\mathcal{P}}$ .

Além disso,  $P_{\mathcal{P}}$  é fechado para a multiplicação e para a adição:

(iii) Tome  $a, b \in P_{\mathcal{P}}$ , então  $\langle a \rangle \equiv 1 \equiv \langle b \rangle \pmod{(\mathcal{P})}$ . Como  $\langle a \rangle - 1 \in \mathcal{P}$ , então  $\langle ab \rangle - \langle b \rangle = \langle b \rangle (\langle a \rangle - 1) \in \mathcal{P}$  (pois este é ideal). Consequentemente  $\langle ab \rangle \equiv \langle b \rangle \pmod{(\mathcal{P})} \equiv 1 \pmod{(\mathcal{P})}$ , ou seja  $ab \in P_{\mathcal{P}}$ .

Seja  $c = a + b$ . Se  $c = 0$ , então  $a = -b$  e de  $\langle a \rangle \equiv \langle b \rangle \equiv 1 \pmod{(\mathcal{P})}$  temos  $1 \equiv -1 \pmod{(\mathcal{P})}$ ,

daí  $2 \in \mathcal{P}$  e portanto  $\mathcal{P}$  tem característica 2, contradição. Então  $c \neq 0$  e de  $\langle a \rangle + \langle b \rangle = \langle a + b \rangle (1 + \langle ab \rangle)$  temos  $2 \equiv 2 \langle c \rangle \pmod{\mathcal{P}}$ . Como  $\text{car } \mathcal{P} = 0$  segue que  $\langle c \rangle \equiv 1 \pmod{\mathcal{P}}$ , isto é,  $c \in P$  e isto conclui a demonstração de que  $\alpha_{\mathcal{P}}$  é uma ordem sobre  $F$ .

Afirmamos que as aplicações  $\alpha \xrightarrow{\theta} \mathcal{P}_{\alpha}$  e  $\mathcal{P} \xrightarrow{\varphi} \alpha_{\mathcal{P}}$  são inversas uma da outra.

De fato, seja  $\alpha$  uma ordem de  $F$  e  $\alpha' := (\varphi \circ \theta)(\alpha) = \alpha_{\mathcal{P}_{\alpha}}$ . Mostremos que  $P' := P_{\alpha'}$  e  $P := P_{\alpha}$  são iguais, acarretando que  $\alpha' = \alpha$ .

Para qualquer  $a \in P'$ ,  $\langle a \rangle \equiv 1 \pmod{\mathcal{P}_{\alpha}}$ , ou seja,  $\langle a, -1 \rangle \in \mathcal{P}_{\alpha} = \ker(r_{\alpha}^*)$ . Assim  $a \in P'$  se, e somente se,  $a \in \dot{F}^2 \cap F = P_{\alpha}$ . Logo  $\varphi \circ \theta = \text{id}$ .

Agora provemos que  $\theta \circ \varphi = \text{id}$ .

Seja  $\mathcal{P}$  um ideal primo de característica zero em  $W(F)$ . Então  $\varphi(\mathcal{P})$  é a ordem  $\alpha_{\mathcal{P}}$  cujo conjunto dos elementos positivos é  $P_{\mathcal{P}} = \{a \in \dot{F} \mid \langle a \rangle \equiv 1 \pmod{\mathcal{P}}\}$  e  $\theta(\varphi(\mathcal{P})) := \mathcal{P}_{\alpha_{\mathcal{P}}} := \ker(r_{\alpha_{\mathcal{P}}}^*)$ . Assim  $q = \langle a_1, \dots, a_n \rangle \in \mathcal{P}_{\alpha_{\mathcal{P}}}$  se, e somente se,  $q = 0 \in W(F_{\alpha_{\mathcal{P}}}) \simeq \mathbb{Z}$  se, e somente se,  $\text{sign}_{\alpha_{\mathcal{P}}} q = 0$  se, e somente se,  $\sum_{i=1}^n \text{sign}_{\alpha_{\mathcal{P}}} \langle a_i \rangle = 0$ . Por definição,  $a_i \in P_{\mathcal{P}}$  para a metade dos índices  $i \in 1, 2, \dots, n$  e  $-a_i \in P_{\mathcal{P}}$  para a metade restante dos índices. Reordenando e colocando os  $a_i$ 's positivos na frente temos:

$q = \langle a_1, \dots, a_m, -a_{m+1}, \dots, -a_{2m} \rangle$ ,  $n = 2m$ ,  $a_1, \dots, a_m, -a_{m+1}, \dots, -a_{2m} \in P_{\mathcal{P}}$ . Assim,  $\langle a_i \rangle \equiv 1 \pmod{\mathcal{P}}$ ,  $i = 1, \dots, m$  e  $\langle a_i \rangle \equiv -1 \pmod{\mathcal{P}}$ ,  $i = m+1, \dots, 2m$ , o que implica que  $q \equiv m(1) + m(-1) \pmod{\mathcal{P}}$ . Portanto  $q \equiv 0 \pmod{\mathcal{P}}$ , ou seja  $q \in \mathcal{P}$ . Logo  $\mathcal{P}_{\alpha_{\mathcal{P}}} \subset \mathcal{P}$ . Agora o isomorfismo  $\frac{W(F)}{\mathcal{P}_{\alpha_{\mathcal{P}}}} \simeq \mathbb{Z} \simeq \frac{W(F)}{\mathcal{P}}$  nos dá que  $\mathcal{P}_{\alpha_{\mathcal{P}}} = \mathcal{P}$ .

Isto conclui o teorema. ■

Vamos agora considerar os ideais primos de característica  $p \neq 0$ . Primeiro vamos aproveitar os ideais primos de característica zero de  $W(F)$  (se existirem) e construir ideais de característica  $p > 0$  (incluindo 2). O teorema a seguir, garante que esses são todos os ideais primos do anel  $W(F)$ .



Para uma ordem  $\alpha$  de  $F$  e  $p > 0$  um número primo denote por  $\mathcal{P}_{\alpha,p}$  o núcleo da seguinte aplicação composta:

$$W(F) \xrightarrow{r^*} W(F_\alpha) \simeq \mathbb{Z} \xrightarrow{\pi} \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Em outras palavras,  $\mathcal{P}_{\alpha,p}$  consiste de todas as formas quadráticas  $q \in W(F)$  cuja assinatura relativa a ordem  $\alpha$  é um inteiro múltiplo de  $p$ .

É importante notar que  $\mathcal{P}_{\alpha,p}$  é o único ideal de característica  $p$  que contém  $\mathcal{P}_\alpha$ .

De fato, tome  $q \in \mathcal{P}_\alpha$ , então  $r_\alpha^*(q) = 0$  e  $\pi \circ r_\alpha^*(q) = 0$ , ou seja,  $q \in \mathcal{P}_{\alpha,p}$ . Seja agora  $\mathcal{P}$  um ideal que contém  $\mathcal{P}_\alpha$  e  $\frac{W(F)}{\mathcal{P}} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$  então para toda forma  $q \in \mathcal{P}_{\alpha,p}$ ,  $r_\alpha^*(q) = m \langle 1 \rangle$ ,  $m \in \mathbb{Z}$  : múltiplo de  $p$ . Então  $q + \mathcal{P} = 0 \in \frac{W(F)}{\mathcal{P}}$  pois  $\pi \circ r_\alpha^*(q) = 0 \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ . Logo  $q \in \mathcal{P}$ , ou seja,  $\mathcal{P}_{\alpha,p} \subset \mathcal{P}$ . Seja  $q \in \mathcal{P} \supset \mathcal{P}_\alpha$ , então  $q + \mathcal{P}_\alpha \subset W(F_\alpha) \simeq \mathbb{Z}$ . Como  $q \in \mathcal{P}$  então  $\pi(q + \mathcal{P}_\alpha) = 0$  em  $\frac{\mathbb{Z}}{p\mathbb{Z}}$  pois  $q = 0$  em  $\frac{W(F)}{\mathcal{P}} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ . Logo  $q \in \mathcal{P}_{\alpha,p}$  ou  $\mathcal{P} \subset \mathcal{P}_{\alpha,p}$ . A afirmação está provada.

**Teorema 4.3.4** *Spec  $W(F)$  consiste dos seguintes tipos de ideais primos:*

- (1)  $\mathcal{P}_\alpha$  onde  $\alpha$  percorre todas as ordens de  $F$ . Estes são todos ideais primos de característica 0.
- (2)  $\mathcal{P}_{\alpha,p}$ ,  $\alpha$  como em (1) e  $p$  um número primo. Estes são todos os ideais primos de característica  $p$ .

### Demonstração:

Precisamos somente verificar (2) acima.

Seja  $\mathcal{P}$  um ideal primo em  $W(F)$  de característica  $p \neq 2$ . Na demonstração do Teorema 4.3.3 temos construída uma ordem  $\alpha = \alpha_{\mathcal{P}}$  de  $\mathcal{P}$ . Afirmamos que  $\mathcal{P}_\alpha \subset \mathcal{P}$ . De fato, seja  $q$  uma forma em  $\mathcal{P}_\alpha$ , isto é,  $q$  tem assinatura nula relativo a  $\alpha$ . Então, na diagonalização de  $q$  metade das entradas são positivas (e a outra metade negativa) relativa a  $\alpha$ . As entradas positivas, por definição, são côngruas a  $1(mod.\mathcal{P})$  e as outras são côngruas a  $-1(mod.\mathcal{P})$ . Assim  $q \equiv 0(mod.\mathcal{P})$ , o que mostra que  $\mathcal{P}_\alpha \subset \mathcal{P}$  como afirmado.



Como  $\mathcal{P}_{\alpha,p}$  é o único ideal primo de característica  $p$  que contém  $\mathcal{P}_\alpha$ , concluímos que  $\mathcal{P} = \mathcal{P}_{\alpha,p}$ . Isto completa a classificação.  $\blacksquare$

## Capítulo 5

# Extensões de Assinaturas

### 5.1 Extensões de Assinaturas

Seja  $A$  uma  $F$ -álgebra comutativa de dimensão finita. Para  $a \in A$ ,  $tr(a)$  é o traço do  $F$ -endomorfismo "multiplicação por  $a$ ". Isto define uma aplicação  $F$ -linear, que no caso em que  $A$  é um corpo (contendo  $F$ ) é o traço usual definido para cada elemento da extensão  $A|_F$ , ou seja,  $tr_{A|_F}(a) = \sum a_i$ , onde  $a_i$  são as raízes distintas do polinômio minimal de  $a$  sobre  $F$ . Uma generalização da forma bilinear  $tr_* < 1 >$  definida anteriormente no transfer de Scharlau (ou reciprocidade de Frobenius) é  $b(x, y) = tr(xy)$  definida sobre  $A \times A$ . Da teoria de álgebra comutativa temos que se  $A$  é uma  $F$ -álgebra de dimensão finita  $n$ , então  $A$  é isomorfa a  $\frac{F[X]}{< p(x) >}$ , onde  $< p(x) >$  é o ideal principal de  $F[X]$ , gerado pelo polinômio  $p(x)$ . Agora seguem dois resultados clássicos.

**Teorema 5.1.1** (*Teorema Chinês do Resto*) [H, p. 131-132]

Sejam  $p_1, p_2, \dots, p_r \in K[X]$ ,  $A_i = < p_i >$  o ideal principal de  $K[X]$  gerado por  $p_i = p_i(X)$ , com  $(p_i, p_j) = 1$ ,  $i \neq j$ . Dados  $f_1, f_2, \dots, f_r \in K[X]$  o sistema de congruências  $f \equiv f_i \pmod{A_i}$ ,  $i = 1, 2, \dots, r$  tem uma única solução em  $K[X]$ , módulo  $\cap A_i = < p_1 p_2 \dots p_r >$ .

### Lema 5.1.2 (Sylvester)

Sejam  $(F, P)$  um corpo ordenado com fecho real  $\Delta$ ,  $b(x, y) = \text{tr}(xy)$  a forma traço definida sobre a  $F$ -álgebra  $A$  de dimensão finita. Seja  $p(X) \in F[X]$  tal que  $A \simeq \frac{F[X]}{\langle p(X) \rangle}$ . Então  $\text{sign}_p(b)$  é o número de zeros distintos de  $p(X)$  em  $\Delta$ . Em particular o número de zeros de  $p(X)$  depende apenas de  $P$  e não da escolha de  $\Delta$  (pois  $\text{sign}_p(b)$  é invariante).

### Demonstração:

Como  $\Delta^2$  é uma extensão de  $P$  a  $\Delta$  temos que  $\text{sign}(b) = \text{sign}_{\Delta^2}(b_\Delta)$ , onde  $b_\Delta = b \otimes \Delta$ . O espaço vetorial subjacente da forma bilinear  $b_\Delta$  é  $\frac{\Delta[X]}{\langle p(X) \rangle}$ . Como  $\Delta$  é real fechado, pelo Teorema Fundamental da Álgebra temos que  $p(X)$  se decompõe sobre  $\Delta$  em um produto de fatores lineares e/ou quadráticos:

$$p(X) = p_1(X)^{e_1} p_2(X)^{e_2} \dots p_r(X)^{e_r},$$

com grau de  $p_i(x) \leq 2$ . Pelo Teorema Chinês do Resto, existe um isomorfismo canônico de  $F$ -álgebras:

$$\frac{\Delta[X]}{\langle p(X) \rangle} \simeq \frac{\Delta[X]}{\langle p_1(X)^{e_1} \rangle} \times \dots \times \frac{\Delta[X]}{\langle p_r(X)^{e_r} \rangle} \quad (*)$$

Como a multiplicação neste produto cartesiano de  $\Delta$ -álgebras é feita coordenada a coordenada segue-se que  $b((Y_1, \dots, Y_r), (Z_1, \dots, Z_r)) = \text{tr}(Y_1 Z_1, \dots, Y_r Z_r)$ . Assim a decomposição de  $\frac{\Delta[X]}{\langle p(X) \rangle}$  em produto direto dado em (\*) é uma decomposição ortogonal em relação a  $b$ . Sendo assim

$$b = b_1 \perp b_2 \perp \dots \perp b_r,$$

onde  $b_i$  é a forma traço com espaço vetorial subjacente  $\frac{\Delta[X]}{\langle p_i(X)^{e_i} \rangle}$ . Como  $\text{sign}_p(b) = \sum \text{sign}(b_i)$ , basta verificar o teorema para a forma traço  $b_i$  definida sobre  $L_i = \frac{\Delta[X]}{\langle p_i(X)^{e_i} \rangle}$ . Dessa forma, temos 2 casos a considerar:  $p_i(X) = (X - \alpha)$  e  $p_i(X) = X^2 + \alpha X + \beta$ .

(A) Se  $L_i$  é da forma  $L_i = \frac{\Delta[X]}{\langle (X - \alpha)^e \rangle}$  considere a base  $B = \{1, X - \alpha, \dots, (X - \alpha)^{e-1}\}$  de  $L_i$ . Nesta base a matriz da forma traço  $(b_i)$  é dada por  $(b_i)_B =$



$[tr((X - \alpha)^j)(X - \alpha)^k)]_{e \times e}$ ,  $j, k = 0, 1, \dots, e - 1$ . Como  $tr((X - \alpha)^n)$  é o traço da matriz da função linear  $f : L_i \rightarrow L_i$ ,  $f(y) = (X - \alpha)^n y$  segue que

$$(b_i)_B = \begin{pmatrix} e & 0 & \dots & 0 \\ 0 & \ddots & \dots & 0 \\ \vdots & \dots & \dots & 0 \\ 0 & \dots & \dots & 0 \end{pmatrix}.$$

Em outras palavras,  $b_i = \langle e, 0, \dots, 0 \rangle$  e portanto  $sign_p(b_i) = 1$ .

(B) Se  $L_i$  é da forma  $L_i = \frac{\Delta[X]}{\langle (X^2 + \alpha X + \beta)^e \rangle}$  com  $\alpha^2 - 4\beta < 0$ , então  $L_i \simeq \frac{\Delta[X]}{\langle (X^2 - 1)^e \rangle}$

De fato sejam  $L = \frac{\Delta[X]}{\langle (X^2 + 1)^e \rangle}$ ,  $v$  a classe de  $X$  em  $L$  e  $u$  a classe de  $X$  em  $L_i$ . Queremos  $\psi : L \rightarrow L_i$  tal que  $0 = \psi((v^2 + 1)^e) = (\psi(v)^2 + 1)^e$ , onde  $\psi(v) = a + bu$ . Sendo  $B = \{1 = v_0, X = v_1, X(X^2 + 1) = v_2, (X^2 + 1)^2 = v_3, \dots, X(X^2 + 1)^{e-1} = v_{2e-1}\}$  base de  $L_i$ , depois de alguns cálculos encontramos:  $\psi(1) = 1, \psi(X) = \frac{\alpha + 2u}{\sqrt{4\beta - \alpha^2}}$ . Consequentemente  $\psi(X^2 + 1) =$

$4 \frac{u^2 + \alpha u + \beta}{4\beta - \alpha^2}$ . Faça  $\psi(X^i(X^2 + 1)^j) = \psi(X^i)\psi(X^2 + 1)^j$  e estendendo  $\psi$  a todo  $L$  por linearidade.

Deste modo  $\psi$  é um homomorfismo de anéis. O grau de  $\psi(v_i)$  é igual o grau de  $v_i$ ,  $v_i \in B$ .

Assim se  $f = \sum_{i=0}^{2e-1} a_i v_i \in L$  é tal que  $0 = \psi(f)$  então  $0 = \sum_{i=0}^{2e-1} a_i \psi(v_i)$ . Como para  $i \neq j$  ( $i, j = 0, 1, \dots, 2e - 1$ ),  $\psi(v_i), \psi(v_j)$  tem graus diferentes segue-se que  $a_i = 0$ , ( $i = 0, 1, \dots, 2e - 1$ ).

Logo  $\ker \psi = \{0\}$  e portanto  $\psi$  é injetora. Como  $L$  e  $L_i$  tem a mesma dimensão como  $\Delta$ -espaço vetorial segue-se que  $\psi : L \rightarrow L_i$  é um isomorfismo  $\Delta$ -espaços.

Assim podemos considerar  $L_i = \frac{\Delta[X]}{\langle (X^2 + 1)^e \rangle}$ . Na base  $B$  a forma traço  $b_i$  tem a matriz  $(b_i)_B = (tr(v_j v_k))$ , onde  $tr(v_j v_k)$  é o traço do endomorfismo linear  $f : L_i \rightarrow L_i$ ,  $f(y) = v_j v_k y$ .

Calculando cada um destes traços formamos a matriz

$$(b_i)_B = \begin{pmatrix} 2e & 0 & \cdots & 0 \\ 0 & -2e & \cdots & 0 \\ \cdots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Em outras palavras,  $b_i = \langle 2e, -2e, 0, \dots, 0 \rangle$  (na base  $B$ ). Assim  $\text{sign}_P(b_i) = 0$ , e a demonstração está concluída. ■

**Lema 5.1.3** [B, Chaps 1 – 2 § 2 Proposition 1b, p.96]

*Sejam  $A, B$  anéis comutativos e  $P$  um ideal primo minimal de  $A$ . Se  $f : A \rightarrow B$  é um homomorfismo de anéis tal que  $\ker f \subset P$ , então existe um ideal  $J$  de  $B$  tal que  $P = f^{-1}(J)$ .*

No capítulo anterior vimos que existe uma correspondência 1 a 1 entre as ordens de um corpo  $F$  e os ideais primos de  $W(F)$  de característica zero. Estes, por sua vez são precisamente os núcleos das aplicações assinaturas de  $W(F)$  em  $W(F_\alpha) \simeq \mathbb{Z}$ , ( $F_\alpha$  : fecho real de  $F$  relativo a ordem  $\alpha$ ). Logo existe uma correspondência natural entre as ordens de um corpo  $F$  e as assinaturas de  $W(F)$ . Vamos denotar por  $\text{sign}_P$  a assinatura de  $W(F)$  correspondente a ordem  $P$  de  $F$ .

**Definição 5.1.4** (*Extensões de Assinatura e Ordens*)

Sejam  $f : W(F) \rightarrow W(L)$  um homomorfismo e  $\sigma$  uma assinatura de  $W(F)$ , (isto é: um homomorfismo de  $WF$  em  $\mathbb{Z}$ ). Dizemos que  $\sigma$  se estende a uma assinatura  $\sigma'$  de  $W(L)$  relativamente a  $f$ , se  $\sigma'(f(q)) = \sigma(q)$ , para todo elemento  $q \in W(F)$ . No caso em que  $L \supset F$  e  $f = r^* : W(F) \rightarrow W(L)$  é o homomorfismo induzido pela aplicação inclusão de  $F$  em  $L$  dizemos simplesmente que  $\sigma'$  é uma extensão de  $\sigma$ .

Se  $P$  é uma ordem de  $F$  e  $Q$  é uma ordem de  $L$ ,  $L \supseteq F$ , diz-se que  $Q$  estende  $P$  (ou  $Q$  é uma extensão de  $P$ ) a  $L$  se  $Q \cap F = P$ . Esta extensão será denotada por  $(L, Q)_{|(F, P)}$ .

Considere novamente  $L|_F$  uma extensão de corpos. Na literatura é comum os autores denotarem o núcleo do homomorfismo induzido pela inclusão  $r^* : W(F) \rightarrow W(L)$  por  $W(L|_F)$ . Com estas notações temos:

**Lema 5.1.5** *Sejam  $(F, P)$  um corpo ordenado,  $L|_F$  uma extensão de  $F$ . A ordem  $P$  tem uma extensão a  $L$  se, e somente se,  $\text{sign}_P(W(L|_F)) = 0$*

### Demonstração:

Seja  $Q$  uma extensão de  $P$  a  $L$ . Se  $q = \langle a_1, \dots, a_n \rangle$  pertence a  $W(F)$  então  $r^*(q) = \langle a_1, a_2, \dots, a_n \rangle \in W(L)$ . Logo  $\text{sign}_Q r^*(q) = \text{sign}_P(q)$  e portanto se  $q \in W(L|_F)$  então  $\ker r^* \subset \ker \text{sign}_P$ . Pelo Lema anterior, existe um ideal primo  $J$  de  $W(L)$  tal que  $r^{*-1}(J) = \ker \text{sign}_P$ . Pelo Teorema 4.3.4 segue que  $r^{*-1}(J) = J_P (\ker \text{sign}_P)$ . Pelo Teorema 4.3.3 a ordem  $Q$  correspondente a  $J$  é dada por:

$$Q = \{\alpha \in L \mid \langle 1, -\alpha \rangle \in J\}$$

Resta verificar que  $P = Q \cap F$ . Seja  $\alpha \in P$  então  $\alpha \in \dot{F}$  e  $\langle 1, -\alpha \rangle \in J$ , ou seja,  $\alpha \in F \cap Q$ . Reciprocamente, se  $\alpha \in F \cap Q$  então  $\alpha \in F$  e  $r^*(\langle 1, -\alpha \rangle) = \langle 1, -\alpha \rangle \in J$ . Assim  $\alpha \in F \cap r^{*-1}(J) = J_P$ , ou  $\alpha \in P$ . Logo  $Q \cap F = P$ . ■

**Corolário 5.1.6** *Seja  $(F, P)$  um corpo ordenado e  $L$  uma extensão de  $F$ .*

- (i) *Se  $[L : F]$  é ímpar, sempre existe uma extensão de  $P$  a  $L$ .*
- (ii) *Se  $L = F(\sqrt{d})$ ,  $d \in P$ , também existe uma extensão de  $P$  a  $L$ .*

### Demonstração:

O Teorema de Springer para extensões de grau ímpar nos dá que  $W(L|_F) = 0$ . Logo  $\text{sign}_P(W(L|_F)) = 0$  e (i) está provado. Agora se  $L = F(\sqrt{d})$ , pelo Teorema 3.2.2, obtemos





$W(L|_F) = W(F) < 1, -d >$ . Como  $d$  é positivo segue que  $\text{sign}_p(W(L|_F)) = 0$ . Logo (ii) é válido. ■

A demonstração do Lema seguinte depende da teoria de anéis semi-simples. Como só vamos usá-la num ponto, preferimos só enunciá-la em vez de conceituar e desenvolver parte da teoria de anéis semi-simples para tão pouco uso.

**Lema 5.1.7** *[K, Lema 4.1]*

*Seja  $L|_F$  uma extensão finita de grau  $n$ . Então existe um  $L$ -isomorfismo de anéis*

$$L \otimes_F L \simeq L_1 \times L_2 \times \dots \times L_r$$

*onde  $L_1 = L$  e  $L_2, \dots, L_r$  são extensões algébricas de  $L$  com grau menor que  $n$ .*

**Lema 5.1.8** *Seja  $(F, P)$  um corpo ordenado com fecho real  $\Delta$ . Tome  $L = F(\alpha)$  uma extensão algébrica simples e seja  $\varphi$  a forma traço de  $L$  sobre  $F$ . Assuma  $r = \text{sign}_p(\text{tr}(xy)) > 0$ . Então existem no máximo  $r$  extensões  $R_i$  de  $P$  a  $L$ . (Eles são dados pelos  $F$ -mergulhos  $\sigma_i : L \rightarrow \Delta$ , isto é,  $R_i = \sigma_i^{-1}(\Delta^2)$ ).*

Pelo Lema 5.1.2  $r$  é o número de zeros em  $\Delta$  do polinômio minimal  $p(x)$  de  $\alpha$ , e é também o número de  $F$ -mergulhos  $\sigma_i : L \rightarrow \Delta$ . Claramente  $R_i = \sigma_i^{-1}(\Delta^2)$  são extensões de  $P$ , desde que facilmente, verifica-se que  $R_i$  satisfaz as propriedades de ordem e além disso,  $R_i \cap F = P$ . Assuma agora que exista outra extensão  $Q$ . então existem  $a_i \in L$  com  $\sigma(a_i) \notin \Delta^2$ , ou seja  $a \notin R_i$  e  $a_i \in Q$ . Por repetidas aplicações de 5.1.6 a ordem  $Q$  estende a  $L(\sqrt{a_1}, \dots, \sqrt{a_r}) = F(\beta)$ , onde  $\beta$  é um elemento primitivo sobre  $F$  com polinômio minimal  $q(x)$ . Pelo Lema 5.1.2,  $q(x)$  tem um zero em  $\Delta$ . Portanto, existe um  $F$ -mergulho  $\sigma : F(\beta) \rightarrow \Delta$ . Seja  $\sigma|_L = \sigma_j$ , então temos a seguinte contradição:  $\sigma_j(a_j) = \sigma(a_j) = (\sqrt{\sigma(a_j)})^2 \in \Delta^2$ . ■

**Teorema 5.1.9** (i) *Sejam,  $(L, R)_{|(F, P)}$  uma extensão algébrica de corpos ordenados e  $\Delta$  um fecho real de  $(F, P)$ . Então existe um mergulho  $L \rightarrow \Delta$  que preserva a ordem.*

(ii) Sejam  $\Delta$ ,  $E$  fechos reais do corpo ordenado  $F$ . Então existe exatamente um  $F$ -isomorfismo  $E \cong \Delta$  que, necessariamente preserva a ordem.

(iii) na situação de 5.1.8, os  $R_i$  são todos diferentes. Então  $P$  tem exatamente  $r$  extensões a  $L$ .

### Demonstração:

(i) Consideremos o conjunto  $\mathcal{F}$  de todos os corpos intermediários  $F \subset M \subset L$ , tal que existe um mergulho  $(M, M \cap R) \rightarrow (\Delta, \Delta^2)$  que preserva a ordem. Ordenando  $\mathcal{F}$  pela inclusão, pelo Lema de Zorn, existe um corpo maximal  $M_0$  em  $\mathcal{F}$ . Pelo Lema anterior  $M_0 = L$ .

(ii) De acordo com (i) existe um  $F$ -isomorfismo  $\sigma : E \rightarrow F$ . Seja  $\tau : E \rightarrow F$  o segundo. Como  $\tau(E^2) \subset \Delta^2$ , a aplicação  $\tau$  preserva a ordem como  $\sigma$ . Tome  $\alpha \in E$  com polinômio minimal  $p(x)$  e conjugados  $\alpha_1, \dots, \alpha_r$  em  $E$ . Sem perda de generalidade  $\alpha_1 \prec \dots \prec \alpha_r$ . Desde que  $\sigma$  e  $\tau$  estão preservando as ordens temos:

$$\sigma(\alpha_1) \prec \dots \prec \sigma(\alpha_r), \tau(\alpha_1) \prec \dots \prec \tau(\alpha_r).$$

Então  $\sigma(\alpha_i) = \tau(\alpha_i)$  e em particular  $\sigma(\alpha) = \tau(\alpha)$ , pois um dos  $\sigma(\alpha_r)$  é  $\sigma(\alpha)$ .

(iii) Assuma que  $R_i = R_j = R$ , para  $i \neq j$ . Seja  $E$  o fecho real de  $(L, R)$ . Por (ii) os mergulhos  $\sigma_i \neq \sigma_j$ , podem ser estendidos à aplicação  $E \rightarrow \Delta$ , e isto é impossível por (ii). Isto conclui o teorema. ■

Um resultado fundamental para nós é o teorema a seguir:

**Teorema 5.1.10** Sejam  $(F, P)$  um corpo ordenado e  $L$  uma extensão finita de  $F$ . Então  $\text{sign}_P(\text{tr}_* < 1 >) \geq 0$ . Além disso tem-se que a ordem  $P$  se estende a  $L$  se, e somente se,  $\text{sign}_P(\text{tr}_* < 1 >) > 0$ .

## Demonstração:

Façamos por indução em  $n = [L : F]$ . Para  $n = 1$  a tese é evidente pois  $tr_* < 1 > = < 1 >$ . Suponhamos  $n > 1$ . Se  $P$  não pode ser estendida a  $L$  então pelo Lema 5.1.5  $sign_P(W(L|_F)) \neq 0$ . Seja  $q \in W(L|_F)$  com  $sign_P(q) \neq 0$ . Pela reciprocidade de Frobenius  $q.tr_*( < 1 >) = tr_*(r^*(q)) = 0$ . Daí  $sign_P(q.tr_* < 1 >) = sign_P(q).sign_P(tr_* < 1 >) = 0$ . Logo  $sign_P(tr_* < 1 >) = 0$ . Se  $P$  possui pelo menos uma extensão  $Q$  a  $L$  então  $sign_P(tr_* < 1 >) = sign_Q(tr_* < 1 >_L)$ , onde  $(tr_* < 1 >_L = r^*(tr_* < 1 >))$ .

Por definição temos que a forma  $n$ -dimensional  $tr_* < 1 >_L$  tem  $L \otimes_F L$  como espaço subjacente (isto é:  $tr_* < 1 >_L: L \otimes_F L \rightarrow L$ ). Pelo Lema 5.1.7, segue-se que existe um  $L$ -isomorfismo de anéis  $L \otimes_F L \simeq L_1 \times L_2 \times \dots \times L_r$ , onde  $L_1 = L$  e  $L_i$  é uma extensão algébrica de  $L$  com grau  $[L_i : L] = n_i < n$ . Como as operações de  $L_1 \times L_2 \times \dots \times L_r$  são efetuadas coordenada à coordenada segue-se que esta decomposição de  $L \otimes_F L$  é ortogonal, ou seja:

$$(L \otimes_F L, tr_* < 1 >_L) = (L_1, tr_1) \perp (L_2, tr_2) \perp \dots \perp (L_r, tr_r)$$

onde  $tr_i: L_i \rightarrow L$  é a restrição da forma  $tr_* < 1 >_L$  a  $L_i$ . Logo  $tr_i$  é a forma traço de extensão  $L_i|_L$  e podemos escrever  $tr_* < 1 >_L = tr_{L_i|_L} < 1 >$ . Como  $L_i = L$  tem a forma traço igual a  $< 1 >$ , a assinatura é 1. Sendo  $[L_i : L] < n$ , a hipótese de indução nos dá que os outros  $tr_i$  têm assinatura maior ou igual a zero. Assim  $sign(tr_* < 1 >) > 0$ . ■

**Exemplo 5.1.11** Seja  $E = F(\sqrt{a})$ ,  $a \in \dot{F} \setminus \dot{F}^2$ .

A forma quadrática  $tr_* < 1 >: E \rightarrow F$  tem forma bilinear associada  $b: E \times E \rightarrow F$  definida por  $b(x, y) = tr(xy)$ . Assim, em relação a  $F$ -base  $\{1, \sqrt{a}\}$  de  $E$  temos:

$$M_{tr \langle \rangle} = \begin{pmatrix} b(1, 1) & b(1, \sqrt{a}) \\ b(\sqrt{a}, 1) & b(\sqrt{a}, \sqrt{a}) \end{pmatrix} = \begin{pmatrix} tr(1) & tr(\sqrt{a}) \\ tr(\sqrt{a}) & tr(a) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2a \end{pmatrix}.$$

Logo  $tr_* < 1 > \simeq \langle 2, 2a \rangle$ . Assim, se  $F$  é ordenado por  $P_{\succeq}$  temos que  $sign_P(tr_* < 1 >) > 0$  se, e somente se,  $a \in P$ . Neste caso a ordem  $\succeq_P$  é estendível a  $E$ , de dois modos: em uma ordem  $\sqrt{a}$  é positivo e na outra ordem  $\sqrt{a}$  é negativo. ■



**Exemplo 5.1.12** Pelo Corolário 5.1.6(i) existe uma extensão da ordem usual ( $\leq$ ) de  $\mathbb{Q}$  à  $\mathbb{Q}(\sqrt[3]{a})$ , onde  $a = 2$  ou  $a = -2$ . De fato pelo Teorema 5.1.10 é suficiente demonstrarmos que  $\text{sign}(\text{tr}_* \langle 1 \rangle) > 0$ .

Para isto seja  $E = \mathbb{Q}(\sqrt[3]{a})$ , considere a base  $B = \{1, \sqrt[3]{a}, \sqrt[3]{a^2}\}$  de  $E$  sobre  $\mathbb{Q}$ . Temos que a forma quadrática  $\text{tr}_* \langle 1 \rangle (x, y) = \text{tr}(x \cdot y)$  na base  $B$  tem a seguinte matriz:

$$M_{\text{tr}_* \langle 1 \rangle} = \begin{pmatrix} \text{tr}(1) & \text{tr}(\sqrt[3]{a}) & \text{tr}(\sqrt[3]{a^2}) \\ \text{tr}(\sqrt[3]{a}) & \text{tr}(\sqrt[3]{a^2}) & \text{tr}(\sqrt[3]{a}) \\ \text{tr}(\sqrt[3]{a^2}) & \text{tr}(\sqrt[3]{a}) & \text{tr}(a\sqrt[3]{a}) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3a \\ 0 & 3a & 0 \end{pmatrix},$$

onde  $a = 2$  ou  $a = -2$ .

Logo  $\text{tr}_* \langle 1 \rangle (x_1, x_2, x_3) = (x_1 \ x_2 \ x_3) M_{\text{tr}_* \langle 1 \rangle} (x_1 \ x_2 \ x_3)^t = 3x_1^2 + 6ax_2x_3$ . Como  $Q.1$  é ortogonal a  $(\mathbb{Q} \cdot \sqrt[3]{a} + \mathbb{Q} \cdot \sqrt[3]{a^2})$  e  $\text{tr} \langle 1 \rangle$  restrito a  $\mathbb{Q} \cdot \sqrt[3]{a} + \mathbb{Q} \cdot \sqrt[3]{a^2}$  é dada por  $6ax_2x_3$  isométrico a  $\mathbb{H}$  (Teorema 1.3.2(4)), temos que  $\text{tr} \langle 1 \rangle = \langle 3 \rangle \perp \mathbb{H}$ . Logo  $\text{sign}(\text{tr}_* \langle 1 \rangle) = 1$  e a ordem usual de  $\mathbb{Q}$  se estende a  $\mathbb{Q}(\sqrt[3]{a})$ , onde  $a = 2$  ou  $a = -2$ . ■

**Exemplo 5.1.13** Sejam  $F, \preceq$  um corpo ordenado e  $a \in F \setminus F^2$ ,  $0 \prec a$ . Então  $K = F(\sqrt[n]{a}, n = 1, 2, \dots)$  possui uma única extensão da ordem  $\preceq$  de  $F$ . Desde que  $\sqrt{a} \in K$ ,  $a$  é positivo em todas as ordens de  $K$ . Assim as ordens de  $K$  estão em correspondência bijetiva com as ordens de  $F$  em que  $a$  é positivo.

De fato, denote por  $F_m$  o corpo  $F_m := F(\sqrt{a}, \sqrt[4]{a}, \dots, \sqrt[2^m]{a})$ , para cada  $m = 1, 2, \dots$ .

Note que cada um dos elementos  $\sqrt{a}, \sqrt[4]{a}, \dots, \sqrt[2^{m-1}]{a}$  é um quadrado em  $F_m$ . Logo eles são positivos em qualquer ordem de  $F_m$ . Pelo exemplo 5.1.11 existe apenas uma ordem de  $F_1$  tal que  $\sqrt{a}$  é positivo nesta ordem. Como  $F_{m-1} \subset F_m = F_{m-1}(\sqrt[2^m]{a})$ , por indução sobre  $m$  existem apenas duas ordens de  $F_m$  que estende  $\preceq$ ; uma em que  $\sqrt[2^m]{a}$  é positivo e a outra em que  $\sqrt[2^m]{a}$  é negativo.

Desde que  $K = \bigcup_{m=1}^{\infty} F_m$  é um corpo (pois  $\{F_m, m \in \mathbb{N}\}$  é uma cadeia ordenada pela

inclusão), cada ordem de  $K$  induz uma ordem em  $F_m$ . Mostremos que  $K$  possui apenas uma ordem que estende  $\preceq$ , a saber, aquela em que  $\sqrt[m]{a}$  é positivo,  $\forall m \geq 1$ .

Seja  $\preceq_m$  a única ordem de  $F_m$  que estende  $\preceq$  na qual  $\sqrt[m]{a}$  é positivo. Note que  $\sqrt[s]{a}$  sendo um quadrado em  $F_m$  para  $s = 1, 2, \dots, m-1$ , eles também são positivos. Seja  $P \subset K$  o conjunto  $P = \bigcup P_m$ , onde  $P_m$  é o conjunto dos elementos positivos da ordem de  $F_m$  que estende  $\preceq$  tal que  $\sqrt[s]{a} \in P_m$ ,  $s = 1, 2, \dots, m$ . Desde que  $P \subset P_1 \subset P_2 \dots$  é muito fácil verificar que  $P$  é uma ordem de  $K$  que estende  $P$ . Agora sejam  $\preceq_1$  e  $\preceq_2$  duas ordens de  $K$  que estendem  $\preceq$ . Como  $K$  é uma reunião de uma cadeia de corpos e  $\preceq_1$ ,  $\preceq_2$  são iguais sobre  $F$  existe  $i \in \mathbb{N}$  tal que  $\preceq_1 = \preceq_2$  sobre  $F_i$  e distintas sobre  $F_{i+1}$ . Seja  $\preceq'$  as restrições de  $\preceq_1$  e  $\preceq_2$  sobre  $F_i$ . Como  $F_{i+1}$  é uma extensão quadrática de  $F_i$  só existem duas extensões de  $\preceq'$  sobre  $F_{i+1}$ ; uma em que  $\sqrt[i+1]{a}$  é positivo e a outra em que  $\sqrt[i+1]{a}$  é negativo. Então estas duas extensões são precisamente  $\preceq_1$  e  $\preceq_2$ . Se  $\sqrt[i+1]{a} \prec_1 0$  em  $F_{i+1}$ , então  $\sqrt[i+1]{a} \prec_1 0$  em  $K$  e  $\sqrt[i+1]{a}$  é um quadrado em  $K$ , (contradição). Do mesmo modo temos uma contradição caso  $\sqrt[i+1]{a} \prec_2 0$  em  $F_{i+1}$ . Como  $\sqrt[m]{a} \in K^2$ ,  $\forall m = 1, 2, \dots$  o exemplo está completo. ■

Efetuada mais alguns cálculos, pode-se estender o Teorema 5.1.10 para toda forma quadrática sobre  $L$ , ou seja:

**Teorema 5.1.14** *Sejam  $(F, P)$  um corpo ordenado e  $L|_F$  uma extensão finita. Então para toda forma quadrática  $\phi$  sobre  $L$ ,  $\text{sign}_P(\text{tr}_*\phi) = \sum_{R \supset P} \text{sign}_R(\phi)$ , onde a soma é dada sobre todas as extensões  $R$  de  $P$ . Em particular, o número de extensões é igual a  $\text{sign}_P(\text{tr}_* \langle 1 \rangle)$ .*

### Demonstração:

Podemos assumir  $\phi = \langle \alpha \rangle$ ,  $\alpha \in L$ . Seja  $\Delta$  um fecho real de  $(F, P)$  e  $E = F(\sqrt{-1})$ . Então  $\text{sign}_P(\text{tr}_* \langle \alpha \rangle) = \text{sign}(\text{tr}_* \langle \alpha \rangle)_\Delta$ . O espaço vetorial subjacente de  $(\text{tr}_* \langle \alpha \rangle)_F$  é  $L \otimes_F \Delta$ . Pelo Lema 5.1.7,  $L \otimes_F \Delta = \Delta \times \dots \times \Delta \times E \times \dots \times E$ , com  $r$  fatores  $\Delta$ . Esta decomposição é ortogonal e os fatores  $E$  são tais que  $(E, q_E)$  são planos hiperbólicos, onde  $q_E$  é a restrição de  $\text{tr}_* \langle \alpha \rangle_\Delta$  à  $E$ .  $\text{tr}_* \langle \alpha \rangle_\Delta$  restrita à  $E$  é positivo ou negativo dependendo se  $\alpha$  é positivo ou

se  $\alpha$  é negativo na ordem correspondente. Pelo Teorema 5.1.9(iii) a extensão  $P$  corresponde exatamente aos fatores  $\Delta$  e isto demonstra o teorema. ■



## Capítulo 6

# O Espaço das Ordens de um Corpo

### 6.1 O Espaço das Ordens de um Corpo

Neste capítulo faremos um breve estudo sobre o conjunto das ordens de um corpo  $F$ . Este conjunto será denotado por  $X_F$ , ou seja,

$$X_F := \{P \mid P \text{ ordem de } F\}$$

Queremos primeiramente, construir uma topologia canônica sobre  $X_F$ . Toda ordem  $P$  define de modo único uma função assinatura,  $\text{sign}_P : F^* \longrightarrow \{\pm 1\}$ ,  $\text{sign}_P(x) = 1$  se, e somente se,  $x \in P$ . O conjunto de todas aplicações  $s : F^* \longrightarrow \{\pm 1\}$  será denotado por  $\Pi_{F^*} \{\pm 1\}$ , ou mais resumidamente por  $\Pi \{\pm 1\}$ . Como  $P$  é completamente determinado por  $\text{sign}_P$ , temos uma injeção  $X_F \longrightarrow \Pi \{\pm 1\}$ . Tomemos  $\{\pm 1\}$  com a topologia discreta e  $\Pi \{\pm 1\}$  com a topologia produto.

Como  $\{\pm 1\}$  é Hausdorff e compacto, pelo Teorema de Tychonov temos que  $\Pi \{\pm 1\}$  é compacto e Hausdorff.

Consideremos  $X_F$  um subconjunto de  $\Pi \{\pm 1\}$  e dotado com a topologia induzida. O conjunto  $X_F$  é chamado espaço das ordens de  $F$ .



Por conveniência, lembremos que um conjunto  $\mathcal{B}$  de abertos de um espaço topológico  $X$  é chamado subbase se todo aberto de  $X$  pode ser expresso como união de intersecções finitas de elementos de  $\mathcal{B}$ . A topologia em  $\Pi\{\pm 1\}$  é definida tomando a seguinte subbase:

$$\pi_a^{-1}(\varepsilon) = H(a, \varepsilon) = \{f : F^* \longrightarrow \{\pm 1\} | f(a) = \varepsilon\}$$

onde  $a \in F^*$ ,  $\varepsilon = \pm 1$  e  $\pi_a = \Pi\{\pm 1\} \longrightarrow \{\pm 1\}$  é a projeção sobre o  $a$ -ésimo fator.

Como a seguinte união é disjunta:

$$\Pi\{\pm 1\} = H(a, \varepsilon) \cup H(a, -\varepsilon)$$

os conjuntos  $H(a, \varepsilon)$  são abertos e fechados.

Um espaço topológico é chamado totalmente desconexo se qualquer dois pontos podem ser separados por subconjuntos disjuntos abertos e fechados. Temos o seguinte: se  $f, g \in \Pi\{\pm 1\}$  e  $f(a) \neq g(a)$  então  $f$  e  $g$  são separados por  $H(a, \varepsilon)$  e  $H(a, -\varepsilon)$ . Assim  $\Pi\{\pm 1\}$  é um espaço booleano, isto é, Hausdorff, compacto e totalmente desconexo.

**Teorema 6.1.1**  $X_F$  é um subconjunto fechado de  $\Pi\{\pm 1\}$ . Assim  $X_F$  é um espaço booleano com a respectiva topologia induzida.

### Demonstração:

Mostremos que  $X_F^c$  é aberto. Tome a aplicação  $s : F^* \longrightarrow \{\pm 1\}$  que não é definida por uma ordem. Dessa forma, pelo menos uma das seguintes condições ocorre:

- (1)  $s(a) = s(b) = 1$ , mas  $s(a + b) = -1$
- (2)  $s(a) = s(b) = 1$ , mas  $s(ab) = -1$
- (3) Existe  $a \in \dot{F}$  tal que  $s(a) = s(-a) = \varepsilon$  ( $\varepsilon = 1$  ou  $-1$ ).

Consideremos que ocorre (1), então  $a, b \in s^{-1}(1)$  implica que  $a + b = c \notin s^{-1}(1)$  e daí,  $s \in H(a, 1) \cap H(b, 1) \cap H(c, -1)$ . Mas  $(H(a, 1) \cap H(b, 1) \cap H(c, -1)) \cap X_F = \emptyset$  pois se  $P \in X_F$ ,  $\text{sign}_P(a) = \text{sign}_P(b) = 1$  então  $\text{sign}(c) = 1$ , contradição.

Se ocorre (2), temos  $a, b \in s^{-1}(1)$  mas  $c = ab \notin s^{-1}(1)$  e novamente  $s \in H(a, 1) \cap H(b, 1) \cap H(c, -1)$  e  $(H(a, 1) \cap H(b, 1) \cap H(c, -1)) \cap X_F = \emptyset$ .

Se ocorre (3) existe  $a \in F$  tal que  $s(a) = 1$  ( $a \notin s^{-1}(-1)$ ) e  $s(-a) = 1$  ( $-a \notin s^{-1}(-1)$ ) e assim,  $s \in H(a, 1) \cap H(-a, 1)$  e  $(H(a, 1) \cap H(-a, 1)) \cap X_F = \emptyset$ . Logo  $X_F$  é um subconjunto fechado de  $\{\pm 1\}$ . Assim  $X_F$  com a topologia induzida de  $\Pi\{\pm 1\}$  é booleano.

Finalmente como para todo  $a \in F$ ,  $H(a, 1) \cap X_F = H(a) = \{P \in X_F \mid a \in P\}$  e  $H(a, -1) \cap X_F = H(-a)$  concluímos que a topologia induzida por  $\Pi\{\pm 1\}$  em  $X_F$  coincide com a topologia inicialmente considerada. ■

Definimos agora a seguinte aplicação :  $\hat{\phi} : X_F \longrightarrow \mathbb{Z}$ ,  $P \longrightarrow \text{sign}(\phi)$ , onde  $\phi$  é uma forma quadrática sobre  $F$  ou um elemento do anel de Witt.

**Teorema 6.1.2** *A aplicação  $\hat{\phi}$  é contínua. A topologia de  $X_F$  é a topologia mais fraca tal que todas  $\hat{\phi}$  são contínuas.*

### Demonstração:

Claramente, usaremos a topologia discreta sobre  $\mathbb{Z}$ . Como soma de funções contínuas é contínua, basta-nos mostrar para  $\phi = \langle \alpha \rangle$ :

$$\hat{\phi}^{-1}(i) = \emptyset, \text{ se } i \neq \pm 1$$

$$\hat{\phi}^{-1}(1) = H(\alpha)$$

$$\hat{\phi}^{-1}(-1) = H(-\alpha).$$

Como estes conjuntos são abertos, a afirmação está provada. ■

**Definição 6.1.3** *Para uma extensão de corpos  $L|_F$ , temos a seguinte aplicação canônica:*

$$\varepsilon = \varepsilon_{L|_F} : X_L \longrightarrow X_F, R \longrightarrow R \cap F$$



**Teorema 6.1.4** (i) A aplicação  $\varepsilon_{L|F}$  é contínua e fechada para toda extensão de corpos  $L|F$

(ii) A aplicação  $\varepsilon_{L|F}$  é aberta para toda extensão finita  $L|F$

### Demonstração:

(i) Para  $\alpha \in F$  claramente temos  $\varepsilon^{-1}(H_F(\alpha)) = H_L(\alpha)$ . Então  $\varepsilon$  é contínua. Como  $X_L$  é compacto, segue que  $\varepsilon$  é fechada (isto é, aplicações que levam conjuntos fechados em conjuntos fechados).

(ii) Temos que mostrar que a imagem de um aberto é aberto. Uma base de um conjunto aberto é a coleção de conjuntos abertos e fechados:

$$H(\alpha_1, \dots, \alpha_n) := H(\alpha_1) \cap \dots \cap H(\alpha_n)$$

Seja  $R$  uma ordem de  $L$ . Então  $R \in H(\alpha_1, \dots, \alpha_n)$  se e só se,  $\text{sign}_R \langle \alpha_1, \dots, \alpha_n \rangle \neq 0$  (Onde  $\phi = \langle \alpha_1, \dots, \alpha_n \rangle$  denota a forma quadrática  $\langle 1, \alpha_1 \rangle \otimes \dots \otimes \langle 1, \alpha_n \rangle$ . Note que  $\text{sign} \langle \alpha_1, \dots, \alpha_n \rangle = 2^n$  se todos  $\alpha_i$  são positivos e é igual a 0 se um dos  $\alpha_i$  é negativo).

Aplicando agora a fórmula traço de 5.1.14  $\text{sign}(\text{tr}_* \phi) = \sum_{R \supset P} \text{sign}_R(\phi)$ .

Como  $\text{sign}_R(\phi) \geq 0$  para todo  $R$ , segue que  $\text{sign}(\text{tr}_* \phi) \neq 0$  se, e somente se, existe uma extensão  $R$  de  $P$  com  $\text{sign}_R(\phi) \neq 0$ . E assim,  $\varepsilon_{L|F}(H(\alpha_1, \dots, \alpha_n)) = \{P \mid \text{sign}(\text{tr}_* \phi) \neq 0\}$ , como este conjunto é aberto e fechado, nossa afirmação está provada. ■

### Exemplo 6.1.5

Vamos dar um exemplo de um corpo com um conjunto não contável de ordens.

Seja  $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$  a extensão de  $\mathbb{Q}$  obtida por adjunção das raízes quadradas de todos os números primos positivos. Denote por  $X(F)$  o conjunto de todas as ordens de  $F$ . Já vimos que existem duas ordens sobre  $\mathbb{Q}(\sqrt{p})$  ( $p > 0$  um número primo em  $\mathbb{Z}$ ) que estendem a ordem original de  $\mathbb{Q}$ . Assim existem quatro ordens sobre  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$  ( $p$  e  $q$  primos positivos em  $\mathbb{Z}$ ) que estendem a ordem original de  $\mathbb{Q}$ , etc. Cada ordem de  $F$  fica determinada quando

se especifica que  $\sqrt{p}$  é positivo ou negativo (ou seja: tem sinal 1 ou -1). Denotemos o produto cartesiano de infinitos fatores de  $\{0, 1\}$  por  $\prod_{i=1}^{\infty} \{0, 1\}$  e definimos  $\varphi : X(F) \rightarrow \prod_{i=1}^{\infty} \{0, 1\}$ , por:  $\varphi(\preceq) = (a_1, a_2, a_3, \dots)$ , onde  $a_i = 1$  se  $\sqrt{p_i}$  é positivo na ordem  $\preceq$  e  $a_i = 0$ , caso contrário, ( $p_i$  é o  $i$ -ésimo primo). Então  $\varphi$  é uma bijeção e como  $\prod_{i=1}^{\infty} \{0, 1\}$  não é contável temos que  $X(F)$  não é contável. ■

**Notação 6.1.6** *T. C. Craven demonstra em ([C], Corolário 4) que  $X(F)$  é homeomorfo ao conjunto de Cantor.*



# Bibliografia

[B] BOURBAKI, N.: *Algèbre Commutative*, chaps1-2, Hermann, Paris, 1961.

[C] CRAVEN, T. C. The Boolean Space of Orderings of a Field. T.A.M.S., **1975**, *209*, 225-235.

[ELW] ELMAN, R., LAM, T. Y., WADSWORTH, A. R. Orderings Under Fields Extensions. J. reine angew. Math., **1985**, *25(3)*, 7-27.

[H] HUNGERFORD, T.W.: *Álgebra*. Springer-Verlag New York Berlin Heidelberg, 1974.

[K] KNEBUSH, M. On the Uniqueness of Real Closure and the Existence of Real Places. Comm. Helv., **1972**, *47*, 260-269.

[L] LAM, T. Y. *The Algebraic Theory of Quadratic Forms*; Mathematics Lecture Note Series; Reading, W. A. Benjamin, 1980.

[S] SCHARLAU, W.: *Quadratic and Hermitian Forms*, Springer-Verlag Berlin Heidelberg New York, 1985.





