

Rita de Cássia Fanhani Meira

Formas Quadráticas e Extensões
de Valorizações



1910001165



Formas Quadráticas e Extensões de Valorizações

Rita de Cássia Fanhani Meira

Orientador: Prof. Dr. Clotilzio Moreira dos Santos



t.1.165/03

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

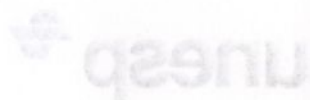
São José do Rio Preto – SP

Fevereiro - 2003

7511.4
M514R

10101039

Universidade Estadual Paulista "Júlio de Mesquita Filho"



Formas Quadráticas e Extensões de Valorizações

Rita de Cássia Fanhani Meira

Meira, Rita de Cássia Fanhani.

Formas quadráticas e extensões de valorizações / Rita de Cássia
Fanhani Meira. – São José do Rio Preto : [s.n.], 2003
76 f. ; 30 cm.

Orientador: Clotilzio Moreira dos Santos

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

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

CDU – 511.55



“ Tu és Senhor, o meu pastor
por isso nada em minha vida
faltará.”
salmo 22



Agradecimentos

A realização deste trabalho foi possível graças a colaboração de muitas pessoas.

Muito obrigado a todos que estiveram comigo neste caminho.

Em primeiro lugar, agradeço aos meus pais, Artur e Aparecida, por todo o apoio e incentivo que me deram ao longo da vida.

Aos meus amigos, especialmente aos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

Aos meus professores, especialmente aos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

A todos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

A todos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

A todos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

A todos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

A todos que estiveram comigo durante a graduação, por todo o apoio e incentivo que me deram ao longo da vida.

Aos meus pais,

Artur e Aparecida

dedico.

Agradecimentos

A realização deste trabalho só foi possível graças a colaboração de muitas pessoas.

Manifesto minha gratidão a todas elas e de forma particular:

Ao professor Dr. Clotilzio Moreira dos Santos, pela orientação e paciência na elaboração deste trabalho, pela amizade sincera e pelo incentivo nos estudos e na vida.

Aos meus pais, minha gratidão eterna pelo apoio nos momentos mais difíceis, por todo o carinho, amor, dedicação, preocupação, e por todas as suas orações.

Às minhas irmãs, Cristina e Tatiani, pelo carinho e por estarem sempre torcendo por mim.

Ao Leandro, por todo incentivo, apoio, carinho e compreensão.

À Patrícia, minha terceira irmã, por tudo o que já passamos juntas (por todas as risadas e por todos os momentos difíceis que enfrentamos), pela grande amizade, companheirismo, confiança e colaboração.

A todos os colegas pós-graduandos pelo companheirismo, em especial o Rodrigo, meu grande amigo.

À FAPESP pelo apoio financeiro.

E principalmente à Deus, por todas as maravilhas que Ele fez em minha vida. Obrigada Senhor por ter iluminado o meu caminho e por abençoar a minha vida.



Conteúdo

Introdução	2
1 Formas Quadráticas e Espaços Quadráticos	4
1.1 Formas Quadráticas	4
1.2 Diagonalização de Formas Quadráticas	7
1.3 Isotropia, Plano Hiperbólico e Decomposição de Formas Quadráticas	10
1.4 Produto de Kronecker de Espaços Quadráticos.	16
2 Anel de Witt	18
2.1 Construção do Anel de Witt	18
2.2 Anéis de Witt de Alguns Corpos	21
2.3 Teorema de Springer	23
2.4 Grupos de Witt dos Corpos p -Ádicos	29
3 Álgebra de Quatérnios	32
3.1 Conceitos Básicos Sobre Álgebra de Quatérnios	32



4	Radical de um Corpo	38
4.1	Radical de Kaplansky	38
5	Elementos Rígidos e Anéis de Valorização	46
5.1	Anéis de Valorizações $R_1(F)$ —compatíveis	47
6	Extensões de Valorizações	64
6.1	Extensões de Valorizações	64
	Bibliografia	73

Introdução

No estudo de formas quadráticas sobre corpos as técnicas de valorizações e ordens são de grande ajuda. Por outro lado, para se estudar formas quadráticas e determinar suas estruturas sobre álgebras de quatérnios ou álgebras centrais simples mais gerais, os problemas são bem mais complexos. Um método de estudo é tentar reproduzir alguns bons resultados já existentes na teoria de formas quadráticas sobre corpos. Para isto seria interessante que ordens ou valorizações sobre o corpo, que é o centro da álgebra, estendesse à álgebra toda. Mas isto não é possível sempre. Mesmo em casos simples há contra-exemplos. Para algumas valorizações henseliana ou de Krull é possível. As melhores valorizações, em se tratando do estudo de forma quadrática sobre corpos são as valorizações ditas compatíveis com o radical (Ver Definição 5.1.2). Assim, o principal objetivo deste trabalho é demonstrar que sobre um corpo Hilbertiano (corpos que admitem uma única álgebra de quatérnios com divisão, a menos de isomorfismo) existe valorização compatível com o radical e ela se estende de modo único a álgebra de quatérnios com divisão sobre o corpo em questão. Isto é feito no último capítulo. A partir disso, é possível determinar o anel de Witt das formas quadráticas sobre a álgebra de quatérnios, (ver [S]).

A idéia por trás disto é que um corpo F admite uma valorização discreta (isto é: o grupo de valores é $\mathbb{Z}$) se, e somente se, o anel de Witt de F é o anel de grupo $W(\overline{F}).[\Delta]$, onde Δ é um grupo com dois elementos e $\overline{F}$ é o corpo de resíduos. Este é o famoso Teorema de Springer, e ele afirma que o cálculo do anel de Witt de F se reduz ao cálculo do anel de Witt de $\overline{F}$. Além disso este anel de Witt é o anel de Witt do corpo de séries de potências formais sobre o corpo $\overline{F}$. Estes são os anéis de Witt mais simples. Mas isto ocorre se o radical de F



é trivial. O capítulo 4 é finalizado com infinitos corpos com o radical não trivial. Caso isto ocorra as melhores valorizações sobre F que reproduzem levemente o resultado anterior (qual seja $W(F) = W(\overline{F}).[\Delta]$) são as valorizações compatíveis com o radical. Este é o assunto do capítulo 5; um capítulo bastante técnico.

Como se vê, não gostaríamos de simplesmente citar o Teorema de Springer como motivador de extensões de valorizações, mesmo porque o assunto poderia ficar vago. Por outro lado, para desenvolvê-lo sucintamente e de modo simples, apenas para justificar os capítulos posteriores e não ser o foco central, foi tarefa árdua. Espero que tenhamos conseguido. Tratamos dele no capítulo 2 e como aplicação dele, nesse mesmo capítulo determinamos o grupo de Witt dos corpos p -ádicos. Assim o capítulo anterior trata de resumos de formas quadráticas sobre corpos e o começo do capítulo 2 sobre a construção do anel de Witt, para dar sustentação a este.

1.1. Formas Quadráticas

Em todo o capítulo V denotará um espaço vetorial de dimensão finita sobre um corpo F de característica diferente de 2.

Uma forma quadrática (ou simplesmente forma) sobre F é uma função $Q: V \rightarrow F$ (onde $\dim V = n$) tal que

$$(1) \quad q(v) = \alpha^2 q(v), \quad \forall \alpha \in F, \forall v \in V, \quad \alpha \neq 0, \quad \forall v \in V.$$

$$(2) \quad q(v) = \sum_{i=1}^n a_i v_i^2, \quad \text{para } q(v) = (q_1, \dots, q_n) \in F^n, \quad v = (v_1, \dots, v_n) \in V,$$

onde $Q(v) = (q_1, \dots, q_n)$ e $q_i = a_i v_i^2$ para $i = 1, \dots, n$. Se $Q(v) = (q_1, \dots, q_n)$ e $Q(w) = (q'_1, \dots, q'_n)$ são duas formas quadráticas sobre F e $Q(v) = Q(w)$ para todo $v \in V$, então $Q(v) = Q(w)$ para todo $v \in V$.



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 um *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 do 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 $M_q = (b(e_i, e_j))$, 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 σ 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 simétricas 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 $d(q) = \det(M_q) \in \frac{F^\times}{F^{\times 2}}$. Isto já mostra que o grupo $\frac{F^\times}{F^{\times 2}}$ 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 $M_q = C_{Can}^t M_{q_1} C_{Can}$.

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 $q(x_1, \dots, x_n) = \sum_{i=1}^n a_{ij} x_i x_j$. 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 q e q_1 são formas quadráticas isométricas e q representa d se, e somente se, 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 θ_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 $V = U + U^\perp$, 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 $d(q) = d(q_1).d(q_2)$.

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

(i) σ 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 $\beta_i \in \dot{F}$, 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 $\frac{\dot{F}}{F^2}$.

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 $b_{q_1}(x, y) = 0$ 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. Vejamos as demais:

(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 $d(q) = \det \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} = d_1 d_2 \neq 0$. 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 seja, $b = -a$ em $\frac{\dot{F}}{F^2}$. Logo $q \simeq \langle a, -a \rangle$. Sejam $q_1(x, y) = axy$ 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 $q \simeq \langle -1, c \rangle$. 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 $m\mathcal{H}$. 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 $r\mathcal{H} \subseteq (V, q)$.

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 $q \simeq q_\alpha \perp m\mathbb{H}$, onde q_α 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 $q \supset \mathcal{H}$, e como $\mathcal{H}$ 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 τ_v satisfaz:

1. τ_v é um endomorfismo de V .
2. τ_v restrita a $(Fv)^\perp$ é a aplicação identidade e $\tau_v(v) = -v$. Em particular, temos que τ_v é uma involução (ou seja: $\tau_v^2 = Id$).
3. τ_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 τ 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) $V = V_1 \otimes V_2 \xrightarrow{\sigma} V_1' \otimes V_2'$ dada por $\sigma(x \otimes y) = y \otimes x$ leva base em base e $q = q' \circ \sigma$.

(2) $(V_1 \otimes V_2) \otimes V_3 \xrightarrow{\sigma} V_1 \otimes (V_2 \otimes V_3)$ $(x \otimes y) \otimes z \rightarrow x \otimes (y \otimes z)$ σ 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 todos elementos não nulos em $M(F)$ não têm 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 $\varphi : M \rightarrow Groth(M)$ definida por $\varphi(a) = \overline{(a,0)}$, injeta M em $Groth(M)$, ou seja, φ 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



$\mathbb{H} = \langle 1, -1 \rangle$, 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 $q \equiv 3(\text{mod. } 4)$ então $W(F) \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$.

Demonstração:

(1) Se $q \equiv 1(\text{mod. } 4)$, então $1 = -1$ em $\frac{F}{F^2}$. Assim $\mathbb{H} = \langle 1, 1 \rangle = \langle s, s \rangle$, (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 $q \equiv 3(\text{mod. } 4)$ então $1 \neq -1$ em $\frac{F}{F^2}$, e podemos considerar $s = -1 \in \frac{F}{F^2}$. Daí $\mathbb{H} = \langle 1, s \rangle = \langle 1, -1 \rangle$. 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 $\langle 1, 1, 1 \rangle = \mathbb{H} + \langle d \rangle$, 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 $W(F) \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$.

2.3 Teorema de Springer

O Teorema de Springer nos permite classificar formas quadráticas sobre os *Corpos Locais* (corpos completos relativamente a uma valorização v). Um corpo Local F tal que o corpo de resíduos $\overline{F}$, referente a valorização em questão, é finito é dito *Corpo $\mathcal{P}$ -Ádicos*. É o caso dos completamentos p -ádicos do corpo dos números racionais $\mathbb{Q}$, para p um número primo positivo em $\mathbb{Z}$. Como aplicação do Teorema de Springer no próximo capítulo calcularemos o grupo de Witt de um corpo $\mathcal{P}$ -ádicos $\mathbb{Q}_p$. Para isto vamos precisar apenas do conceito de valorização não arquimediana e outros conceitos que seguem deste.

Definição 2.3.1 Se F é um corpo, uma aplicação $v : F \rightarrow \mathbb{Z}$ (que pode ser assumida sobrejetora) é dita uma *valorização* de F se

- (i) $v(xy) = v(x) + v(y)$, $x, y \in \dot{F}$,
- (ii) $v(x + y) \geq \min\{v(x), v(y)\}$, se $y \neq -x$, $\forall x, y \in \dot{F}$.

Definimos ainda $v(0) = \infty$ de modo que $Im(v) := v(F) = \mathbb{Z} \cup \{\infty\}$, e estendemos a adição de $\mathbb{Z}$ à $\mathbb{Z} \cup \{\infty\}$ por $x + \infty = \infty + x = \infty + \infty = \infty$.

O conjunto $A = \{x \in F \mid v(x) \geq 0\}$ é um sub-anel de F dito *anel de valorização*. Ele é um anel local com ideal maximal $\mathcal{P} = \{x \in F \mid v(x) \geq 1\}$. Este ideal é principal e é gerado por qualquer elemento π tal que $v(\pi) = 1$. Os geradores de $\mathcal{P}$ são determinados a menos de unidades do anel A , e são chamados de *uniformizadores* de A , ou de F . O corpo $\bar{F} = \frac{A}{\mathcal{P}}$ é chamado de *corpo de resíduos* de F (relativamente a valorização v). O grupo das unidades (= elementos inversíveis) de A é dado por $U = \{x \in A \mid x \notin \mathcal{P}\} = \{x \in A \mid v(x) = 0\}$. Todos elementos de $\dot{F}$ podem ser escritos de modo único na forma: $y = u \cdot \pi^{v(y)}$, onde $u \in U$. De fato se $y \in \dot{F}$, seja $v(y) = r \in \mathbb{Z}$. Então $v(y) = v(\pi^r)$. Daí $v(y \cdot \pi^{-r}) = v(y) - v(\pi^r) = 0$. Logo $y \cdot \pi^{-r} = u \in U$. Portanto $y = u \pi^{v(y)}$.

Temos uma sequência encaixada de ideais: $A \supset \mathcal{P} \supset \mathcal{P}^2 \supset \dots \supset (0)$, com $\bigcap \mathcal{P}^i = \{0\}$.

Definimos um *Corpo Local* como sendo um par (F, v) como acima, onde F é completo relativamente a valorização v . Isto significa que na métrica $d(x, y) = e^{-v(x-y)}$, toda *sequência de Cauchy* converge. (Note que nesta métrica, dois elementos x, y estão *próximos* se, e somente se, $x - y$ pertence a uma potência $\mathcal{P}^n$, para $n \in \mathbb{N}$ grande).

Uma situação típica do uso da completude de F é que se é dada uma sequência $x_1, x_2, \dots, x_n$ em A tal que $x_{i+1} \equiv x_i \pmod{\mathcal{P}}$ para todo i , então A possui um elemento $x (= \lim x_i)$ tal que $x \equiv x_i \pmod{\mathcal{P}^i}$ para todo i . De fato, esta propriedade pode ser tomada como definição de completamento.

Exemplos de corpos $\mathcal{P}$ -ádicos são os corpos de séries de potências formais $F = k((t))$, sobre um corpo finito k . Os elementos de F são da forma $\sum_{i=m}^{\infty} a_i X^i = X^m(a_m + a_{m+1}X + \cdots)$, $a_m \neq 0$, para algum $m \in \mathbb{Z}$. Os completamentos p -ádicos do corpo $\mathbb{Q}$ dos números racionais é outro exemplo, e seus elementos se escrevem do mesmo modo quando se troca X por p , e $0 \leq a_i < p$, $a_i \in \mathbb{Z}$.

Lema 2.3.2 *Sejam (F, v) um corpo local tal que a característica de $\overline{F}$ é distinta de 2 e $u \in U$. Então u é um quadrado em F se, e somente se, $\overline{u}$ é um quadrado em $\overline{F}$.*

Demonstração:

$[\Rightarrow]$ Se $u = \alpha^2$, $\alpha \in F$ é claro que $\overline{u} = \overline{\alpha}^2 \in \overline{F}^2 \Rightarrow u \in \overline{F}^2$.

$[\Leftarrow]$ Agora consideremos $\overline{u} = \overline{b}^2$, $\overline{b} \in \overline{F}$. Desejamos construir uma sequência $(b_i) \in U$ tal que $b_i^2 \equiv u \pmod{\mathcal{P}^i}$ e $b_{i+1} \equiv b_i \pmod{\mathcal{P}^i}$, $i \geq 1$; pois se tivermos tal sequência, e tomarmos $b = \lim b_i$, então $b^2 - u = \lim b_i^2 - u = \lim (b_i^2 - u) = 0$. Logo $b^2 = u$, e $u \in \overline{F}^2$, pois F é completo.

A existência de b_1 é garantida pois $\overline{u} = \overline{b}^2 \in \overline{F}^2$. Como $u \in U$, também $b_1 = b \in U$. Temos que $b_1^2 \equiv u \pmod{\mathcal{P}}$. Suponhamos achados $b_i \in U$; $i \geq 1$ tal que $b_i^2 \equiv u \pmod{\mathcal{P}^i}$ e $b_i \equiv b_{i-1} \pmod{\mathcal{P}^{i-1}}$. Queremos determinar $b_{i+1} \in U$ tal que $b_{i+1}^2 \equiv u \pmod{\mathcal{P}^i}$ e $b_{i+1} = b_i + z\pi^i$, com $z \in A$ a determinar. De $b_i^2 - u = c\pi^i$, $c \in A$, segue-se que $b_{i+1}^2 - u = (b_i + z\pi^i)^2 - u(b_i^2 - u) + 2b_i z\pi^i + z^2\pi^{2i} \equiv \pi^i(c + 2b_i z) \pmod{\mathcal{P}^{i+1}}$. Como $\text{car}(\overline{F}) \neq 2$, $b_i \in U$, então basta achar $z \in A$ tal que $c + 2b_i z = \pi$. Daí segue-se que $z = (\pi - c)(2b_i)^{-1} \in A$. Logo $b_{i+1} \in U$ e $b_{i+1} \equiv b_i \pmod{\mathcal{P}^i}$.

Teorema 2.3.3 *[Levantamento de Raízes]*

Sejam (F, v) um corpo local com $\text{car}(\overline{F}) \neq 2$, e $f(X) = aX^2 + bX + c \in F[X]$. Se existe uma raiz $\overline{u}$ em $\overline{F}$ de $\overline{f}(X) = \overline{a}X^2 + \overline{b}X + \overline{c}$ então existe uma raiz u em F de $f(X)$.

Demonstração: Note que a recíproca é válida e sua demonstração é trivial.

Começemos a demonstração observando (e isto é tudo) que a mudança de variável X para $Y - \frac{b}{2a}$ leva $f(X)$ à $g(Y) = aY^2 - \frac{b^2 - 4ac}{4a}$. Além disso x_0 é raiz de f se, e somente se, $y_0 = x_0 + \frac{b}{2a}$ é raiz de g . Por outro lado, $g(Y)$ tem raiz y_0 se, e somente se, $h(Y) = \frac{1}{a}g(Y)$ tem raiz y_0 . Assim o cálculo de raízes de um polinômio de grau dois se resume ao cálculo de quadrados. Então basta demonstrarmos que se $\bar{h}(X) = X^2 + d \in \bar{F}[X]$ tem uma raiz $\bar{u} \in \bar{F}$ então $h(X) = X^2 + d$ tem uma raiz $u \in F$; e isto segue do Lema anterior.

■

Corolário 2.3.4 *Nas hipóteses do Lema anterior temos que um elemento não nulo $u\pi^m$ ($u \in U$, $m \in \mathbb{Z}$) é um quadrado em F se, e somente se, m é par e $\bar{u} \in \bar{F}^2$. Em particular, $\bar{u} = 1 \implies u \in U^2$.*

Este Corolário implica na existência de uma sequência exata de grupos. Primeiro definimos um homomorfismo de grupos de $\frac{\dot{F}}{\dot{F}^2}$ para $\frac{\dot{F}}{\dot{F}^2}$, onde a imagem de $\bar{u}$ é $u \in U$; um levantamento de $\bar{u}$. Este homomorfismo está bem definido pois se v é outro levantamento de $\bar{u}$, então $\overline{uv^{-1}} = \bar{1}$. Daí o Corolário anterior implica que $u \in v \cdot \dot{F}^2$.

Corolário 2.3.5 *Nas hipóteses do Teorema anterior temos que a sequência exata curta*

$$1 \rightarrow \frac{\dot{F}}{\dot{F}^2} \xrightarrow{i} \frac{\dot{F}}{\dot{F}^2} \xrightarrow{\bar{v}} \frac{\mathbb{Z}}{2\mathbb{Z}} \rightarrow 0 \quad (2.3.1)$$

se fatora.

Demonstração:

A exatidão é clara. Para a fatoração, defina $j : \frac{\mathbb{Z}}{2\mathbb{Z}} \rightarrow \frac{\dot{F}}{\dot{F}^2}$ que leva 1 em $\pi \dot{F}^2$.

■

Lema 2.3.6 A aplicação $i : \frac{\dot{F}}{F^2} \rightarrow \frac{\dot{F}}{F^2}$ induz os monomorfismos de grupos

$$i : W(\bar{F}) \rightarrow W(F) \text{ e } j : W(\bar{F}) \rightarrow W(F),$$

definidos por $i(\langle \bar{a}_1, \dots, \bar{a}_n \rangle) = \langle a_1, \dots, a_n \rangle$ e $j(\bar{q}) = \langle \pi \rangle . i(q)$.

Demonstração:

De fato, para todo corpo K , $\frac{\dot{K}}{K^2}$ é isomorfo a $S = \{ \langle a \rangle, a \in \dot{K} \}$ e S gera $W(K)$. Então definimos $i : W(\bar{F}) \rightarrow W(F)$ por $i(\langle \bar{a}_1, \dots, \bar{a}_n \rangle) = \langle a_1, \dots, a_n \rangle$. Vejamos que i está bem definida, por indução sobre n .

Denotemos $\langle a_1, \dots, a_n \rangle$ por q_n e $\langle \bar{a}_1, \dots, \bar{a}_n \rangle$ por $\bar{q}_n$.

Se $n = 1$ e $\langle \bar{a}_1 \rangle = \langle \bar{b}_1 \rangle$, $a_1, b_1 \in U$ então $\bar{a}_1 = \bar{b}_1 s^2$, $s \in U$, ou seja, $\bar{a}_1 = \overline{b_1 s^2}$. Isto implica que $(\frac{\bar{b}_1 s^2}{a_1}) = \bar{1}$. Pelo Corolário 2.3.4 $\frac{b_1 s^2}{a_1} = t^2$, ou seja, $b_1 s^2 = a_1 t^2$. Logo $\langle b_1 \rangle = \langle b_1 s^2 \rangle = \langle a_1 t^2 \rangle = \langle a_1 \rangle$.

Seja $q'_n = \langle b_1, \dots, b_n \rangle$ e suponhamos que $\bar{q}_{n-1} = \bar{q}'_{n-1}$. Então $q_{n-1} = q'_{n-1}$, para $n - 1 \geq 1$. Sejam $\langle \bar{a}_1, \dots, \bar{a}_n \rangle = \langle \bar{b}_1, \dots, \bar{b}_n \rangle$ em $W(\bar{F})$. Então $\langle \bar{a}_1, \dots, \bar{a}_n \rangle \simeq \langle \bar{b}_1, \dots, \bar{b}_n \rangle$. Pela observação 1.2.3, $\bar{b}_1 \in D_{\bar{F}} \langle \bar{a}_1, \dots, \bar{a}_n \rangle$. Logo existe $\bar{\alpha}_1 \in \bar{F}$ tal que $\bar{a}_1 \cdot \bar{\alpha}_1^2 + \bar{a}_2 \cdot \bar{\alpha}_2^2 + \dots + \bar{a}_n \cdot \bar{\alpha}_n^2 = \bar{b}_1$. Sem perda de generalidade podemos supor que $\bar{\alpha}_1 \neq 0$. Seja $\bar{c} = \bar{a}_2 \cdot \bar{\alpha}_2^2 + \dots + \bar{a}_n \cdot \bar{\alpha}_n^2 - \bar{b}_1$. Então o polinômio $\bar{a}_1 X^2 + \bar{c}$ tem uma raiz $\bar{\alpha}_1 \in \bar{F}$. Pelo Teorema 2.3.3 $a_1 X^2 + c$ tem uma raiz $\alpha_1 \in F$, ou seja $a_1 \alpha_1^2 + a_2 \alpha_2^2 + \dots + a_n \alpha_n^2 = b_1$. Pelo critério da representação e diagonalização de formas quadráticas existe $c_2, \dots, c_n \in U$ tais que $\langle a_1, a_2, \dots, a_n \rangle \simeq \langle b_1, c_2, \dots, c_n \rangle$. Daí $\langle \bar{b}_1, \bar{c}_2, \dots, \bar{c}_n \rangle = \langle \bar{a}_1, \bar{a}_2, \dots, \bar{a}_n \rangle = \langle \bar{b}_1, \dots, \bar{b}_n \rangle$ em $W(\bar{F})$. Cancelando $\langle \bar{b}_1 \rangle$ temos $\langle \bar{c}_2, \dots, \bar{c}_n \rangle = \langle \bar{b}_2, \dots, \bar{b}_n \rangle$. A hipótese de indução nos dá que $\langle c_2, \dots, c_n \rangle = \langle b_2, \dots, b_n \rangle$. Consequentemente $\langle a_1, a_2, \dots, a_n \rangle \simeq \langle b_1, c_2, \dots, c_n \rangle \simeq \langle b_1, b_2, \dots, b_n \rangle$. ■

Desde que todo elemento x de $\dot{F}$ é da forma $x = u\pi^\alpha$, $u \in U$, $\alpha \in \mathbb{Z}$, toda forma quadrática sobre F , pode ser escrita como $q = q_1 \perp \langle \pi \rangle q_2$, onde $q_1 = \langle u_1, \dots, u_r \rangle$ e $q_2 = \langle u_{r+1}, \dots, u_n \rangle$, com $u_i \in U$.

As formas quadráticas $\partial_1(q) = \bar{q}_1 (= \langle \bar{u}_1, \dots, \bar{u}_r \rangle)$ e $\partial_2(q) = \bar{q}_2 \in W(\bar{F})$ são chamadas de *primeira e segunda classes residuais de q* .

Teorema 2.3.7 [Springer]

Seja F um corpo local tal que $c(\bar{F}) \neq 2$. Então

1. Se toda forma quadrática de dimensão n sobre $\bar{F}$ é isotrópica então toda forma quadrática de dimensão $2n - 1$ sobre F é isotrópica.
2. A forma quadrática q sobre F é isotrópica se, e somente se, uma das formas quadráticas residuais de q é isotrópica sobre $\bar{F}$.
3. $\partial = (\partial_1, \partial_2) : W(F) \longrightarrow W(\bar{F}) \oplus W(\bar{F})$ definida por $\partial(q_1 + \langle \pi \rangle q_2) = (\bar{q}_1, \bar{q}_2)$ é um isomorfismo de grupos.
4. $q = q'$ em $W(F)$ se, e somente se, $\partial_i(q) = \partial_i(q')$, $i = 1, 2$.

Demonstração:

(1) Seja $q = q_1 \perp \langle \pi \rangle q_2$ de dimensão $2n - 1$. Então q_1 ou q_2 tem dimensão $m \geq n$. Suponhamos que seja q_1 . Pelo Teorema 1.3.4, $\bar{q}_1$ contém $\mathbb{H}$. Logo $\bar{q}_1 = \mathbb{H} \perp \bar{q}'$, $\bar{q}' = \langle \bar{c}_3, \dots, \bar{c}_m \rangle$. Assim $q_1 = i(\bar{q}_1) = i(\bar{q}') = \langle c_3, \dots, c_m \rangle = q_3$. Como $\dim q_1 \neq \dim q_3$ isto implica que q_1 é isotrópica. O mesmo argumento vale para q_2 , caso $\dim q_2 \geq n$.

(2) Seja $q = q_1 \perp \langle \pi \rangle q_2$, $q_1 = \langle u_1, \dots, u_r \rangle$ e $q_2 = \langle u_{r+1}, \dots, u_n \rangle$. Se $\bar{q}_i$ é isotrópica (para $i = 1$ ou 2), então $\bar{q}_i = \mathbb{H} \perp \langle \bar{c}_3, \dots, \bar{c}_s \rangle$, para algum s . Pelo Lema anterior $q_i \simeq \mathbb{H} \perp \langle c_3, \dots, c_s \rangle$: isotrópica. Logo q é isotrópica.

Reciprocamente, se q é isotrópica então q contém $\mathbb{H}$. Se $\mathbb{H} = \langle u_1 \rangle \perp \langle \pi \rangle \langle u_2 \rangle$ então $d(\mathbb{H}) = u_1 u_2 \pi \neq -1$. Pelo Teorema 1.3.2(2) temos uma contradição. Logo q_1 ou q_2 contém $\mathbb{H}$. Daí q_1 ou q_2 é isotrópica, e portanto $\bar{q}_1$ ou $\bar{q}_2$ é isotrópica.

(3) A aplicação $\partial = (\partial_1, \partial_2)$ é injetora pois se $\partial(q_1 \perp \langle \pi \rangle q_2) = \partial(q'_1 \perp \langle \pi \rangle q'_2)$ então $(\bar{q}_1, \bar{q}_2) = (\bar{q}'_1, \bar{q}'_2) \iff \bar{q}_i = \bar{q}'_i \in W(\bar{F})$, $i = 1, 2$. Pelo Lema anterior $\bar{q}_i = \bar{q}'_i \in W(\bar{F})$, $i = 1, 2$. Isto implica que $\bar{q}_1 = \bar{q}'_1$ e $\langle \pi \rangle \cdot \bar{q}_2 = \langle \pi \rangle \cdot \bar{q}'_2$. Daí $q_1 \perp \langle \pi \rangle \cdot q_2 = q'_1 \perp \langle \pi \rangle \cdot q'_2$. Para demonstrar que ∂ é sobrejetora basta demonstrar que $\partial \circ (i, j) = id_{W(\bar{F}) \oplus W(\bar{F})}$, e isto é evidente.

(4) Segue do item (iii) e do Lema anterior. ■

2.4 Grupos de Witt dos Corpos p -Ádicos

Vamos aplicar o Teorema de Springer para determinar o grupo de Witt dos completamentos p -ádicos do corpo dos números racionais, onde $p \in \mathbb{N}$ é um número primo $\neq 2$. Para isto basta verificar que $\mathbb{Q}_p$ é um corpo local que o resto segue do Teorema de Springer e do Teorema 2.2.5. Já vimos que todo elemento de $\mathbb{Q}_p$ se escreve na forma $X = p^m u$, onde $m \in \mathbb{Z}$ e u é uma unidade do anel de valorização. Como $\mathbb{Q}$ é denso em $\mathbb{Q}_p$ existe $\frac{a}{b} \in \mathbb{Q}$, $\text{mdc}(a, b) = 1$ tal que $u \equiv \frac{a}{b} \pmod{p}$. Como p não divide b existe $c \in \mathbb{Z}$ tal que $bc \equiv 1 \pmod{p}$. Daí $u \equiv \frac{ac}{bc} \pmod{p} \equiv ac \pmod{p}$, com $ac \in U$. Dividindo ac por p temos que $ac = a_0 + pa_2$, $0 < a_0 < p$, $a_2 \in \mathbb{Z}$. Consequentemente $u = a_0 + u_1 \cdot p^r$, com $a_0 \in \mathbb{Z}$, $0 < a_0 < p$, $u_1 \in U$ e $r \in \mathbb{N}$. Por indução temos:

$$\mathbb{Q}_p = \{p^m (\sum_{k=0}^{\infty} a_k p^k), a_k \in \mathbb{Z}, 0 \leq a_k < p, a_0 \neq 0\},$$

O anel de valorização é $\mathbb{Z}_p = \{\sum_{k=0}^{\infty} a_k p^k, a_k \in \mathbb{Z}, 0 \leq a_k < p, a_0 \neq 0\}$,

O grupo das unidades é dado por $U_p = \{a_0 + a_1p + a_2p^2 + \dots, a_0 \neq 0, 0 \leq a_i < p\}$, e o ideal maximal é: $M_p = \{p(a_1 + a_2p + a_3p^2 + \dots), a_i \in \mathbb{Z}, 0 \leq a_i < p\}$. Assim o lema seguinte é óbvio.

Lema 2.4.1 *Seja $p \neq 2$, então $\overline{\mathbb{Q}}_p \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$.*

Demonstração:

A aplicação $\varphi : \mathbb{Z}_p \longrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}}$ definido por $\varphi(x) = a_0 + p\mathbb{Z}$ induz um isomorfismo $\overline{\mathbb{Q}}_p \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$.

■

Finalmente temos o

Teorema 2.4.2 *As estruturas aditivas dos anéis de Witt dos corpos p -ádicos são:*

1. $W(\mathbb{Q}_p) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^4$ se $p \equiv 1 \pmod{4}$.
2. $W(\mathbb{Q}_p) \simeq (\frac{\mathbb{Z}}{4\mathbb{Z}})^2$ se $p \equiv 3 \pmod{4}$.

Demonstração:

(1) e (2) Seja $F = \frac{\mathbb{Z}}{p\mathbb{Z}}, p \neq 2$. Pelo Teorema de Springer temos que $W(\mathbb{Q}_p) \simeq (W(F))^2$, aditivamente. O resto segue do Teorema 2.2.5. ■

Observação 2.4.3 (1) *Pode-se verificar facilmente que os isomorfismos de grupos dados em (1) e (2) não são isomorfismos de anéis.*

(2) *Apesar de não ter sido necessário calcular o grupo de classes de quadrados de $\frac{\mathbb{Q}_p}{\mathbb{Q}_p^2}$ para calcular o grupo $W(\mathbb{Q})$ é fácil determinar este grupo. Como todo elemento de $\mathbb{Q}_p$ se escreve na forma $p^\alpha u$, pelo Corolário 2.3.4 temos que $p^\alpha u \in \mathbb{Q}_p^2$ se, e somente se, α é par e $\bar{u}$ é um*

quadrado em $\overline{\mathbb{Q}_p}$. Pelo Lema 2.4.1 $\overline{\mathbb{Q}_p}$ é isomorfo a $K := \frac{\mathbb{Z}}{p\mathbb{Z}}$. Como K é finito, o grupo de classes de quadrados de K é representado por 1 e s , onde s é um gerador do grupo cíclico $\dot{K}$. Segue-se que o grupo constituído pelas distintas classes de quadrados de $\mathbb{Q}_p$ estão reunidas no conjunto $\{1, s, p, ps\} \cdot \dot{\mathbb{Q}_p}^2$. Resumidamente $\frac{\dot{\mathbb{Q}_p}}{\dot{\mathbb{Q}_p}^2} = \{1, p, s, sp\}$.

As tábuas para os grupos multiplicativos $\frac{\dot{\mathbb{Q}_p}}{\dot{\mathbb{Q}_p}^2}$ para $p > 2$ são muito simples pois são grupos abelianos onde todos os elementos tem ordem 2. Assim o grupo $\frac{\dot{\mathbb{Q}_p}}{\dot{\mathbb{Q}_p}^2}$, para $p > 2$ primo, é o grupo de Klein, isomorfo a $(\frac{\mathbb{Z}}{2\mathbb{Z}})^2$.

Algebra de Quatérnios

Neste capítulo vamos estudar a Álgebra de Quatérnios, uma estrutura algébrica natural do tempo quadrático. Relacionamos a existência de álgebras não associativas de tempo quadrático com as formas quadráticas ternárias.

3.1 Conceitos Básicos Sobre Álgebra de Quatérnios

Definição 3.1.1 Sejam F um corpo e $\alpha, \beta \in F$. Dizemos a álgebra de quatérnios $H = (F, \alpha, \beta)$ como sendo a álgebra sobre F gerada por i, j tal que $i^2 = \alpha, j^2 = \beta$ e $ij = -ji$.

Notamos que F possui uma estrutura de espaço vetorial sobre $(F, +, \cdot)$. Então que $H = (F, \alpha, \beta)$ é uma álgebra H sobre F comutativa. Observe também que $i^2 = \alpha(1)(1) = -i^2 j^2 = -\alpha\beta(1)$.

A álgebra de quatérnios $H = (F, \alpha, \beta)$ é o subálgebra natural das quaterniões reais quando $\alpha = \beta = 1$.

Definição 3.1.2 1. Uma F álgebra H é dita *central* se $Z(H) = F$ ($= F(1)$).

2. Uma F álgebra H é dita *simple* se H não possui ideais bilaterais próprios.

Capítulo 3

Álgebra de Quatérnios

Neste capítulo veremos que uma álgebra de quatérnios tem uma estrutura natural de espaço quadrático. Relacionaremos a divisibilidade da álgebra com anisotropia de sua forma quadrática *norma*.

3.1 Conceitos Básicos Sobre Álgebra de Quatérnios

Definição 3.1.1 Sejam F um corpo e $a, b \in F$. Definimos a *álgebra de quatérnios* $D := (\frac{a,b}{F})$ como sendo a álgebra sobre F gerada por i, j tais que $i^2 = a$, $j^2 = b$ e $ij = -ji = k$.

Note que como F -espaço vetorial D tem dimensão quatro e base $\{1, i, j, k\}$. Desde que $ij = -ji$, a álgebra D não é comutativa. Observe também que $k^2 = (ij).(ij) = -i^2.j^2 = -a.b \in F$.

A álgebra de quatérnios $D = (\frac{-1,-1}{\mathbb{R}})$ é o anel de divisão usual dos quatérnios reais, denotado por $\mathcal{H}$.

Definição 3.1.2 1. Uma F -álgebra D é dita *central* se $Z(D) = F$ ($= F.1_D$).

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

3. Uma F -álgebra que satisfaz (i) e (ii) é dita *central simples*.

O próprio F é uma F -álgebra central simples. Para uma álgebra de quatérnios temos:

Proposição 3.1.3 *Toda álgebra de quatérnios é central simples.*

Demonstração:

Seja $D = (\frac{a,b}{F})$ uma álgebra de quatérnios sobre o corpo F , com F -base $\{1, i, j, k\}$. Denotemos o centro de D por $Z(D)$. De $ij = -ji$ e $ik = -ki$, temos que $i, j, k \notin Z(D)$. Assim se $x = x_0 + x_1i + x_2j + x_3k \in Z(D)$, as equações $xi = ix$, $xj = jx$ e $xk = kx$ nos dão que $Z(D) = F.1_D = F$.

Agora considere $J \subseteq D$ um ideal bilateral. Se $J \neq \{0\}$ é suficiente mostrar que existe $\alpha \neq 0$, tal que $\alpha \in (J \cap F)$. Seja $0 \neq x = \alpha + \beta i + \gamma j + \delta k \in J$. Suponhamos que β, γ ou δ é não nulo. Por exemplo, se $\beta \neq 0$ então $xj = \alpha j + \beta k + \gamma b + \delta bi \in J$ e $jx = \alpha j - \beta k + \gamma b - \delta bi \in J$. Daí $xj - jx = 2\beta k + 2\delta bi \in J$. Como $c(F) \neq 2$, tem-se que $\beta k + \delta bi \in J$. Daí $(\beta i + \delta k)b = (\beta k + \delta bi)j \in J$. Como b é inversível $y = \beta i + \delta k \in J$. Por hipótese $yi + iy = 2a\beta \in J \cap F$. Raciocínio análogo se aplica caso γ ou δ é não nulo. Portanto $J = D$. ■

Definição 3.1.4 *Seja $D = (\frac{a,b}{F})$ com base $\{1, i, j, k\}$. Um quatérnio $v = \beta i + \gamma j + \delta k \in D$ é dito quatérnio puro. O conjunto dos quatérnios puros de D será denotado por D_0 .*

A proposição abaixo mostra que a noção de pureza é independente da escolha da base $\{1, i, j, k\}$.

Proposição 3.1.5 *Sejam $D = (\frac{a,b}{F})$ e $0 \neq v \in D$. Então $v \in D_0$ se, e somente se, $v \notin F$ e $v^2 \in F$.*

Demonstração:

($\Rightarrow$) Seja $v = \alpha + \beta i + \gamma j + \delta k$. Então:

$$v^2 = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha(\beta i + \gamma j + \delta k). \quad (3.1.1)$$

Se $v \in D_0$ então $\alpha = 0$. Assim, $v^2 = a\beta^2 + b\gamma^2 - ab\delta^2 \in F$ e claramente $v \notin F$.

($\Leftarrow$) Se $v \notin F$ então ou $\beta \neq 0$ ou $\gamma \neq 0$ ou $\delta \neq 0$. De $v^2 \in F$ e pela equação (1) tem-se que $\alpha = 0$, isto é, v é um quatérnio puro. ■

Consideremos $D = (\frac{a,b}{F})$, $a, b \in \dot{F}$ uma álgebra de quatérnios, com a base $B = \{1, i, j, k\}$. Vamos demonstrar que D tem uma estrutura natural de espaço quadrático.

Dado $x = \alpha + \beta i + \gamma j + \delta k \in D$, o *conjugado* de x é definido e denotado por $\bar{x} := \alpha - \beta i - \gamma j - \delta k$.

As seguintes propriedades são de fáceis verificações:

$$(1) \overline{x+y} = \bar{x} + \bar{y}. \quad (2) \overline{xy} = \bar{y}\bar{x}. \quad (3) \overline{\bar{x}} = x. \quad (4) r \in F, \overline{r\bar{x}} = r\bar{x}.$$

$$(5) \text{ Se } x \in D_0 \text{ então } \bar{x} = -x.$$

Definição 3.1.6 Para $x \in D = (\frac{a,b}{F})$, definimos a *norma* de x por $N(x) = x\bar{x}$ e o *traço* de x por $T(x) = x + \bar{x}$.

Note que das igualdades $\overline{T(x)} = \overline{x + \bar{x}} = \bar{x} + \overline{\bar{x}} = \bar{x} + x = x + \bar{x} = T(x)$ e $\overline{N(x)} = \overline{x\bar{x}} = \bar{x}\bar{\bar{x}} = \bar{x}x = x\bar{x} = N(x)$, concluímos que a norma e o traço de qualquer elemento de D são escalares.

Definição 3.1.7 Nas condições acima $N : D \rightarrow F$ é uma forma quadrática chamada de *forma norma* ou *forma norma reduzida* de D . A forma bilinear associada é dada por $b_N(x, y) = \frac{1}{2}T(x\bar{y})$.

Agora vamos verificar que $B = \{1, i, j, k\}$ é uma base ortonormal do espaço quadrático (D, N) e nesta base $N \simeq \langle 1, -a, -b, ab \rangle$.

Sejam $x, y \in D_0$, então $b(x, y) = \frac{1}{2}(x\bar{y} + y\bar{x}) = \frac{1}{2}(-xy - yx) = -\frac{1}{2}(xy + yx)$. Logo $b(x, y) = 0 \Leftrightarrow xy = -yx$. Como $ij = -ji$, $ik = -ki$ e $kj = -jk$, segue-se que i, j, k são ortogonais dois a dois. Além disso, se x é puro, $b(x, 1) = \frac{1}{2}(x\bar{1} + 1\bar{x}) = \frac{1}{2}(x - x) = 0$. Logo 1 é ortogonal à i, j e k , isto é, $B = \{1, i, j, k\}$ é uma base ortogonal para (D, N) .

Corolário 3.1.8 *O espaço quadrático (D, N) é regular, tem base ortogonal $B = \{1, i, j, k\}$ e N é isométrico a $\langle 1, -a, -b, ab \rangle \simeq \langle 1, -a \rangle \otimes \langle 1, -b \rangle$.*

Demonstração:

Tem-se $N(i) = i\bar{i} = -i^2 = -a$, $N(j) = j\bar{j} = -j^2 = -b$, $N(k) = k\bar{k} = -k^2 = a.b$. Assim se $x = \alpha + \beta i + \gamma j + \delta k \in A$ então $N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 = \langle 1, -a, -b, ab \rangle(x)$, ou seja, na base B temos a seguinte diagonalização de $N : \langle 1, -a, -b, ab \rangle$. ■

Observação 3.1.9 : Para os quatérnios reais $\mathcal{H} = (\frac{-1, -1}{R})$, tem-se $N(\alpha + \beta i + \gamma j + \delta k) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$. Logo N é a norma euclidiana usual de $\mathbb{R}^4$.

Proposição 3.1.10 *Seja $D = (\frac{a, b}{F})$. Então*

1. Para todos $x, y \in D$, $N(x.y) = N(x).N(y)$.
2. $x \in D$ é inversível se, e somente se, $N(x) \neq 0$ (isto é, se, e somente se, x é anisotrópico).
Em particular, $D_F(N) - \{0\}$ é um subgrupo multiplicativo de $\dot{F}$.

Demonstração:

$$(1) N(xy) = xy.\overline{xy} = xy.\bar{x}.\bar{y} = x(y\bar{y})\bar{x} = x\bar{x}y\bar{y} = N(x).N(y).$$

(2) Se existe x^{-1} , então $N(x).N(x^{-1}) = N(x.x^{-1}) = N(1) = 1$. Logo $N(x) \neq 0$. Reciprocamente, se $N(x) \neq 0$ então $x.\bar{x} = N(x) = N(x).1$. Segue-se que $x.\frac{\bar{x}}{N(x)} = \frac{\bar{x}}{N(x)}.x =$

$$1. \text{ Logo } x^{-1} = \frac{\bar{x}}{N(x)}.$$

Por (1) $D_F(N)$ é fechado. Se $a = N(x)$, $b = N(y)$ são não nulos, então por (1) e (2) $ab^{-1} = N(x)N(y)^{-1} = N(x)N(y^{-1}) = N(xy^{-1}) \in D_F(N) - \{0\}$. Logo $D_F(N) - \{0\}$ é um subgrupo de $\dot{F}$. ■

Definição 3.1.11 Dizemos que uma álgebra de quatérnios $D = (\frac{a,b}{F})$ se *fatora* se ela satisfaz uma das condições equivalentes do Teorema a seguir.

Teorema 3.1.12 Para $D = (\frac{a,b}{F})$ as seguintes afirmações são equivalentes:

1. $D \simeq M_2(F)$ (isomorfismo de F -álgebras).
2. D não tem divisão.
3. (D, N) é um espaço quadrático isotrópico. Logo hiperbólico.

Demonstração:

(1) $\Rightarrow$ (2) Como $M_2(F)$ tem divisores de zero segue-se que D tem divisores de zero. Logo D não tem divisão (isto é, nem todo elemento não-nulo de D é inversível).

(2) $\Rightarrow$ (1)

Pelo Teorema de Wedderburn "Toda álgebra simples D é isomorfa a uma álgebra de matrizes $M_m(D_1)$, onde D_1 é uma álgebra de divisão sobre F ". Segue-se que neste caso $\dim D = 4$ e $\dim D = m^2 \cdot \dim D_1$. Se $m = 1$ então $\dim D_1 = 4$ e $D \simeq M_1(D_1) \simeq D_1$, que é um absurdo (pois D_1 é uma álgebra com divisão e D não o é). Se $m = 2$ então $\dim_F D_1 = 1$; assim $D_1 \simeq F$ e $D \simeq M_2(F)$.

(3) $\iff$ (2) Segue da Proposição 3.1.10(2), pois $N(x) = x\bar{x}$. Resta mostrar que se N é isotrópica, então N é hiperbólica.

Se N é isotrópica pelo Teorema 1.3.4(2) $\langle 1, -a, -b, ab \rangle \simeq \mathbb{H} \perp \langle c, d \rangle$. Calculando o determinante obteremos $1 = -cd$ e daí $d = -c$. Logo $N \simeq \mathbb{H} \perp \langle c, -c \rangle = 2\mathbb{H}$: hiperbólica.

■

Exemplos

A álgebra $(\frac{1, -1}{F})$ se fatora pois sua forma norma $\langle 1, -1, 1, -1 \rangle$ é hiperbólica.

Se $a \in \dot{F}$, então ambas as álgebras $(\frac{1, a}{F})$ e $(\frac{a, -a}{F})$ se fatoram, pelo item 3 do Teorema.

Se F é um corpo finito então $(\frac{a, b}{F})$ se fatora, para quaisquer $a, b \in \dot{F}$. De fato pelo Lema 2.2.4(2), toda forma binária sobre F é universal; e pelo Teorema 1.3.6 segue-se que toda forma de dimensão três (ou mais) é isotrópica.

Capítulo 4

Radical de um Corpo

4.1 Radical de Kaplansky

Pode-se dizer que as formas de Pfister surgiram ao mesmo tempo que o advento dos anéis de Witt. Mas só em 1981 J.L. Yucas, em um trabalho que é parte de sua tese de Doutorado tem demonstrado várias de suas propriedades (ver [Y]). Algumas destas propriedades que serão necessárias neste trabalho serão adaptada e reproduzidas aqui.

A noção de radical de um corpo F foi introduzida em 1969 por I. Kaplansky em [K]. A definição original é equivalente a $R(F) = \bigcap_{a \in F^*} D < 1, a >$. Portanto, I. Kaplansky definiu o radical de um corpo usando apenas 1-forma de Pfister. Mais tarde J.L. Yucas no trabalho supracitado, generaliza esta definição para n -formas de Pfister, para $n \in \mathbb{N}$ qualquer.

Uma n -forma de Pfister φ , sobre um corpo F é uma forma quadrática do tipo $< 1, a_1 > \otimes < 1, a_2 > \otimes \dots \otimes < 1, a_n >$, onde $a_1, a_2, \dots, a_n \in F^*$, e $n \geq 1$. A única 0-forma de Pfister é a forma quadrática $< 1 >$. Uma notação prática é: $\varphi := \ll a_1, a_2, \dots, a_n \gg$. A forma quadrática φ' tal que $\ll a_1, a_2, \dots, a_n \gg \simeq < 1 > \perp \varphi'$ é dita *vizinhança de Pfister* de $\varphi = \ll a_1, a_2, \dots, a_n \gg$. Em analogia com os quatérnios puros (para $n = 2$), também se diz que φ' é a *parte pura* da n -forma de Pfister φ .



Por exemplo, para $a_1, a_2 \in \dot{F}$, $\ll a_1, a_2 \gg = \langle 1, a_1, a_2, a_1 a_2 \rangle$ é uma 2-forma de Pfister e $\langle a_1, a_2, a_2 a_3 \rangle$ é a vizinhança de Pfister de $\ll a_1, a_2 \gg$.

As formas de Pfister mais conhecidas são as 1-formas e as 2-formas de Pfister, ditas *formas* (quadráticas) *normas*. As 1-formas $\langle 1, a \rangle$ estão relacionadas com as extensões quadráticas $K = F(\sqrt{-a})$, $a \in F^*$. Notemos que se $x = \alpha + \beta\sqrt{-a}$, então $n_{K|F}(x) = x\bar{x} = \langle 1, a \rangle(\alpha, \beta)$. As 2-formas normas $\ll a, b \gg$ são formas normas de álgebras de quatérnios como vistas no capítulo anterior. Os resultados fundamentais sobre estas formas quadráticas é que o conjunto dos elementos representados por elas formam um subgrupo de $\dot{F}$, e se uma n -forma de Pfister é isotrópica então ela é hiperbólica ([Lam, (X, Corol.1.7)]). Para o caso de formas de Pfister de dimensão 2 ou 4, a demonstração é simples, pois aqui, podemos usar a noção de elemento conjugado da extensão quadrática associada a forma norma $\langle 1, a \rangle$, ou da álgebra de quatérnios associada a forma norma $\ll a, b \gg$. Assim,

Proposição 4.1.1 *Seja $\varphi = \langle 1, a \rangle$ ou $\varphi = \ll a, b \gg$, $a, b \in \dot{F}$. Então $D\varphi$ é um subgrupo de $\dot{F}$.*

Demonstração:

Se $\varphi = \ll a, b \gg$ o resultado segue da Proposição 3.1.10(2). Se $\varphi = \langle 1, a \rangle$, então $D\varphi = \{\alpha^2 + a\beta^2 \in \dot{F}, \alpha, \beta \in F\} = \{N(x) = x\bar{x} \neq 0, x = \alpha + \beta\sqrt{-a} \in F(\sqrt{-a})\}$. Como $N : F(\sqrt{-a}) \rightarrow F$ é multiplicativa, o resultado segue. ■

Seja $P_n(F)$ o conjunto das classes de isometrias das n -formas de Pfister. O subconjunto $D_F\varphi$ é um subgrupo de $\dot{F}$, qualquer que seja $\varphi \in P_n(F)$.

Definição 4.1.2 *Para cada $n \in \mathbb{N}, n \geq 1$ o n -ésimo radical do corpo F é denotado por $R_n(F)$ e é definido por*

$$R_n(F) := \bigcap_{\varphi \in P_n(F)} D(\varphi),$$



$$e \quad R_0(F) = \dot{F}^2.$$

Como $D(\varphi) \subseteq D(\psi)$, $\forall \varphi \in P_n(F)$ e $\psi \in P_{n+1}(F)$ temos a sequência de subgrupos

$$\dot{F}^2 \subseteq R_1(F) \subseteq R_2(F) \subseteq \cdots \subseteq R_n(F) \subseteq \cdots \subseteq \dot{F}.$$

Para o que segue só precisaremos do radical $R_1(F)$ e por isso só desenvolveremos a teoria para este, apesar de que a maioria dos resultados valem para $R_n(F)$ para $n \geq 2$.

Proposição 4.1.3 *Para $r \in \dot{F}$ as seguintes proposições são equivalentes:*

1. $r \in R_1(F)$,
2. $\psi = \langle\langle -r, a \rangle\rangle$ é hiperbólico, (isto é: $\psi = 0 \in W(F)$) para qualquer $a \in \dot{F}$,
3. $D \langle 1, -r \rangle = \dot{F}$, ou seja $\langle 1, -r \rangle$ é universal.

Demonstração:

(1) $\Rightarrow$ (2) Para qualquer $\varphi = \langle 1, a \rangle \in R_1(F)$ a hipótese nos dá que $r \in D\varphi$. Pela Proposição 1.2.5 $\varphi \simeq \langle r, x \rangle$, $x \in \dot{F}$. Calculando o determinante encontramos $x = ra$. Logo $\varphi \simeq \langle r, ra \rangle \simeq \langle r \rangle \varphi$. Então $\langle 1, -r, a, -ra \rangle = 0$ em $W(F)$.

(2) $\Rightarrow$ (3) Tome $a \in \dot{F}$. Por hipótese $\psi = \langle\langle -r, a \rangle\rangle = 0$ em $W(F)$. Logo $\langle 1, -r \rangle \simeq \langle -a, ra \rangle$. Assim $-a \in D(\langle -a, ra \rangle) = D(\langle 1, -r \rangle)$, $\forall a \in \dot{F}$. Portanto $\langle 1, -r \rangle$ é universal.

(3) $\Rightarrow$ (1) Seja $r \in \dot{F}$ tal que $D(\langle 1, -r \rangle) = \dot{F}$. Logo para qualquer $a \in \dot{F}$, $\langle 1, -r \rangle \simeq \langle a, -ra \rangle$. Então $\langle 1, -r, -a, ra \rangle = 0$ em $W(F)$. Daí $\langle 1, -a \rangle = \langle r, -ra \rangle \in W(F)$, para qualquer $a \in \dot{F}$. Logo $r \in D(\langle r, -ra \rangle) = D(\langle 1, -a \rangle)$, $\forall -a \in \dot{F}$. Por definição $r \in R_1(F)$.

■

Lema 4.1.4 *Sejam $a, b \in \dot{F}$. Então $b \in D <1, a>$ se, e somente se, $b.R_1(F) \subset D <1, a>$.*

Demonstração:

Como $D <1, a>$ é um grupo que contém $R_1(F)$ então $b \in D <1, a> \implies b.R_1(F) \subset D <1, a>$. Desde que $1 \in R_1(F)$ a recíproca é evidente. ■

Os corpos locais p -Ádicos $\mathbb{Q}_p$, corpo dos números racionais $\mathbb{Q}$ e o corpo dos números reais $\mathbb{R}$ são exemplos de corpos com o radical trivial. Se F é um corpo finito então $R_1(F) = \dot{F}$, pois toda forma binária é universal, (Veja Lema 2.2.4). Logo $R_1(F)$ não é trivial.

Para finalizar este capítulo vamos construir exemplos de corpos contidos em $\mathbb{Q}_p$, com oito classes de quadrados e com radicais não triviais. Para isto usaremos os seguintes lemas que podem ser encontrados em textos de Teoria dos Conjuntos e Teoria dos Números.

Lema 4.1.5 Zorn

Seja E um conjunto parcialmente ordenado tal que toda cadeia em E possui limite superior. Então E possui elemento maximal.

Lema 4.1.6 1. *Seja $p > 1$ um número primo em $\mathbb{Z}$ tal que $p \equiv 1(\text{mod}.4)$. Então existe $a, b \in \mathbb{Z}$ tais que $a^2 + b^2 = p$.*

2. *Sejam $a, m \in \mathbb{Z}$ tais que $\text{mdc}(a, m) = 1$. Então existem infinitos números primos na progressão $an + m$.*

Lema 4.1.7 *Sejam F_0, F dois corpos tais que $F_0 \subset F$ e $S = \{\alpha_i, i \in I\}$ um conjunto de elementos contidos em $F \setminus F_0$. Então a família $\mathcal{F}$ de subcorpos de F que não contém S possui um subcorpo maximal.*

Demonstração:

Como $F_0 \in \mathcal{F}$, $\mathcal{F}$ não é vazia. Ordenemos $\mathcal{F}$ por inclusão. Se T é um subconjunto totalmente ordenado de $\mathcal{F}$, então $K = \bigcup_{F_j \in T} F_j$ é um subcorpo de F que não contém S . Logo $K \in \mathcal{F}$ e como $K \supset F_t, \forall F_t \in T$, K é um limite superior para o conjunto de corpos $F_t \in T$. Pelo Lema de Zorn $\mathcal{F}$ possui um elemento maximal. ■

Também é simples de se demonstrar que

Lema 4.1.8 *Sejam $F \supset K$ e $\alpha \in F$. Então K é um subcorpo maximal de F que não contém α se, e somente se, $\alpha \notin K$ e $\alpha \in K(\beta)$, para qualquer $\beta \in F \setminus K$.*

Lema 4.1.9 *Sejam F um corpo com corpo primo F_0 e $\alpha \in F$ algébrico sobre F_0 . Se K é um subcorpo maximal de F que não contém α , então F é uma extensão algébrica de K .*

Demonstração:

Seja $\beta \in F$ transcendente sobre K . Desde que $\beta \notin K$, pelo Lema 4.1.8 $\alpha \in K(\beta)$. Sejam $\alpha = \frac{p(\beta)}{q(\beta)}$, $p(X), q(X) \in K[X]$, $q(\beta) \neq 0$ e $f(X) = a_0 + a_1X + \dots + a_nX^n \in F_0[X]$ o polinômio minimal de α . Então

$$0 = f(\alpha) = a_0 + a_1 \frac{p(\beta)}{q(\beta)} + \dots + a_n \frac{p(\beta)^n}{q(\beta)^n}.$$

Multiplicando esta igualdade por $q(\beta)^n$ temos

$$0 = a_0 q(\beta)^n + a_1 p(\beta) q(\beta)^{n-1} + \dots + a_n p(\beta)^n.$$

Logo β é raiz do polinômio $h(X) = a_0 q(X)^n + a_1 p(X) q(X)^{n-1} + \dots + a_n p(X)^n \in K[X]$, contradição. ■

De agora até o fim deste capítulo vamos considerar p um número primo em $\mathbb{Z}$ tal que $p \equiv 1 \pmod{4}$, equivalentemente, -1 é um quadrado módulo p . Pelo Lema 2.3.2 isto é equivalente



a $-1 \in \dot{Q}_p^2$. Vamos denotar uma solução de $X^2 = -1$ em Q_p por $\pm i$. Desde que $i \notin Q$ (corpo primo de Q_p) existe um subcorpo maximal de Q_p que não contém i . Vamos fixar um deles e denotar por F .

Lema 4.1.10 *Seja $b \in F$ tal que $b \in \dot{Q}_p^2$ (isto é: $b \equiv 1 \pmod{p}$). Veja Lema 2.3.2). Então b ou (exclusivo) $-b$ é um quadrado em F .*

Demonstração:

Note que como $-1 \in \dot{Q}_p^2$ então $b \in \dot{Q}_p^2$ e $-b \in \dot{Q}_p^2$. Logo $\sqrt{b}$ e $i\sqrt{b}$ pertencem a $\dot{Q}_p$. Se estes elementos estão contidos em F , então $\sqrt{b} \cdot i\sqrt{b} = ib \in F$. Daí $i = (ib)b^{-1} \in F$, contradição.

Por outro lado se $\sqrt{b} \notin F$, por definição de F segue-se que $i \in F(\sqrt{b})$ (Lema 4.1.8). Seja $i = \alpha + \beta\sqrt{b}$, $\alpha, \beta \in F$. Então $(\alpha + \beta\sqrt{b})^2 = \alpha^2 + b\beta^2 + 2\alpha\beta\sqrt{b} = -1$. Daí $\alpha\beta = 0$ e $\alpha^2 = -1$ ou $b\beta^2 = -1$. Como $\alpha \in F$, $\alpha \neq \pm i$ e portanto $b\beta^2 = -1$, ou seja, $\beta\sqrt{b} = \sqrt{-1} = i$. Finalmente $i\sqrt{b} = \beta(\sqrt{b}) \cdot \sqrt{b} = \beta b \in F$. ■

Lema 4.1.11 *Seja F o subcorpo maximal de Q_p que não contém i , considerado anteriormente. Então $\frac{\dot{F}}{\dot{F}^2} = \{\pm 1, \pm s, \pm p, \pm sp\}$, onde $s \in \mathbb{Z}$ não é um quadrado módulo p . (ou seja: $\bar{s}$ é um gerador do grupo cíclico $\dot{Q}_p$).*

Demonstração:

Seja $s \in \mathbb{Z}$ um gerador do grupo cíclico $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Já vimos na Notação 2.4.3(2) que $A = \{1, s, p, ps\}$ é um conjunto de representantes para $\frac{\dot{Q}_p}{\dot{Q}_p^2}$. Como $p \in F$ segue-se que $A \subset \frac{\dot{F}}{\dot{F}^2}$. Além disso, por hipótese $-1 \notin \dot{F}^2$ e portanto $-1 \neq 1$ em $\dot{F}^2$. Se $-1 = s \in \frac{\dot{F}}{\dot{F}^2}$ então $-s = 1 \in \dot{F}^2 \subset Q_p^2$. Como $-1 \in \dot{Q}_p^2$ (pois $p \equiv 1 \pmod{4}$), segue-se que $s \in \dot{Q}_p^2$, absurdo. Logo $\{\pm 1, \pm s, \pm p, \pm ps\}$ é um conjunto constituído de classes distintas módulo $\dot{F}^2$.

Considere agora $b \in \dot{F}$, qualquer. Como $F \subset \mathbb{Q}_p$, $b = p^\alpha u$, para algum $\alpha \in \mathbb{Z}$ e $u \in U_p$. Assim $b\dot{F}^2 = pu\dot{F}^2$ ou $u\dot{F}^2$ e portanto basta demonstrarmos que $u \equiv 1$ ou s módulo $\dot{F}^2$. Temos que $u \equiv 1$ ou $u \equiv s \pmod{\overline{\mathbb{Q}_p^2}}$, ou seja, u ou us^{-1} é côngruo a $1 \pmod{\overline{\mathbb{Q}_p^2}}$. Pelo Lema 2.3.2 u ou us^{-1} é um quadrado em $\dot{\mathbb{Q}_p}$. Pelo Lema 4.1.10 $u \in \{\pm 1, \pm s\}\dot{F}^2$. Assim $b\dot{F}^2 \in \{\pm 1, \pm s, \pm p, \pm ps\}\dot{F}^2$. ■

Observação 4.1.12 *Li Delang demonstra em [De, Corol.4] que o número cardinal de subcorpos maximais de $\mathbb{Q}_p$ que não contém i é pelo menos $2^{\aleph}$.*

Teorema 4.1.13 *Sejam $p \in \mathbb{Z}$ um número primo congruente a 1 módulo 4 e F um subcorpo de $\mathbb{Q}_p$ que não contém $i = \sqrt{-1}$. Então F tem 8 classes de quadrados, admite uma única 2-forma de Pfister anisotrópica e $R_1(F) = \{1, -1\}$.*

Demonstração:

Que F admite 8 classes de quadrados já sabemos pelo Lema 4.1.11. Para demonstrar que $-1 \in R_1(F)$, é suficiente demonstrar que $D_F < 1, 1 > = \dot{F}$, (Proposição 4.1.3). Como $\dot{F}^2 \subset D_F(q)$ para qualquer forma quadrática q , basta demonstrarmos que $\{\pm 1, \pm s, \pm p, \pm ps\} \subset D_F < 1, 1 > = \{x^2 + y^2 \neq 0, x, y \in F\}$. Note que $< 1, 1 >$ é exatamente a forma norma da extensão quadrática $F(\sqrt{-1})$ (de F), ou seja: $< 1, 1 > (x, y) = N_{F(\sqrt{-1})}(x + yi)$. Como $\mathbb{Z} \subset F$, pelo Lema 4.1.6(1) temos que $p \in D_F < 1, 1 >$, e como $-1 = N_{F(\sqrt{-1})}(i)$, temos que $\{1, -1, p, -p\} \in D_F < 1, 1 >$, (pois $D_F < 1, 1 >$ é um subgrupo de $\frac{\dot{F}}{\dot{F}^2}$). Pelo Teorema de Lagrange resta demonstrar que $s \in D_F < 1, 1 >$. Como $\text{mdc}(p, s) = 1$, pelo Lema 4.1.6(2) e o Teorema Chines do Resto existem primos $q \in \mathbb{Z}$ satisfazendo

$$\begin{cases} q \equiv s \pmod{p} \\ q \equiv 1 \pmod{4}. \end{cases}$$

Pelo Lema 4.1.6(1) $x^2 + y^2 = q$ é solúvel em $\mathbb{Q}$, e como $\mathbb{Q} \subset F$ concluímos que $q \in D_F \subset \langle 1, 1 \rangle$. Agora basta trocar s por q (pois s é apenas um gerador de $\dot{\mathbb{Q}}_p \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$). Isto demonstra que $-1, 1 \in R_1(F)$.

Se existe uma solução da equação $x^2 + sy^2 = p$ sobre F , então existe uma solução de $x^2 + sy^2 = p$ sobre $\mathbb{Q}_p$, ou seja, $p \in D_{\mathbb{Q}_p}(\langle 1, s \rangle)$. Isto contradiz o Teorema de Springer. Logo $\langle 1, s \rangle$ não é universal. Pela Proposição 4.1.3 temos que $-s \notin R_1(F)$. O mesmo argumento aplicado sobre os outros elementos nos dá que s, p e $-p$ não pertencem a $R_1(F)$. Logo $R_1(F) = \{1, -1\}\dot{F}^2$.

Para finalizar seja $q = \langle 1, a, b, ab \rangle$ uma forma quadrática anisotrópica sobre F . Como $R_1(F) = \{1, -1\} \subset D \langle 1, x \rangle$ temos que $|D \langle 1, x \rangle| \geq 4, \forall x \in \dot{F}$. Além disso $a, b \notin R_1(F)$, senão q seria isotrópica. Se $a = \pm s$ então $D \langle 1, a \rangle = \{\pm 1, \pm s\}$ (pois $\langle 1, a \rangle$ não é universal). Pelo Teorema 1.3.6 $b \in \{\pm p, \pm ps\}$. Se $a = \pm p$ então $b \in \{\pm s, \pm ps\}$, pelas mesmas razões. Em todos os casos obteremos: $q \simeq q_1 := \langle 1, s, p, ps \rangle$ ou $q \simeq q_2 := \langle 1, s, -p, -ps \rangle$ ou $q \simeq q_3 := \langle 1, -s, p, -ps \rangle$ ou $q \simeq q_4 := \langle 1, -s, -p, ps \rangle$. Mostremos que $q_i \simeq q_j$ para todos $i, j = 1, 2, 3, 4$.

Como $-1 \in D \langle 1, s \rangle$ temos que $\langle 1, s \rangle \simeq \langle -1, x \rangle$ e calculando o determinante destas formas obtemos $x = -s$. Logo $\langle 1, s \rangle \simeq \langle -1, -s \rangle$. Multiplicando por $\langle p \rangle$ e somando $\langle 1, s \rangle$ à ambos os membros da isometria obtemos: $q_1 \simeq q_2$. As isometrias $q_1 \simeq q_3$ e $q_1 \simeq q_4$ são demonstradas de modo análogo. Logo existe uma única 2-forma de Pfister sobre F a menos de isometria. Isto conclui o Teorema. ■

Capítulo 5

Elementos Rígidos e Anéis de Valorização

O *Teorema de Springer* afirma que se F é um corpo com uma valorização discreta, $\bar{F}$ o corpo de resíduos de característica diferente de dois e π um gerador do ideal maximal do anel de valorização, então toda forma quadrática sobre F tem uma decomposição na forma $q = q_1 \perp \langle \pi \rangle q_2$, onde q_1 e q_2 representam apenas unidades do anel de valorização. Em outras palavras, o anel de Witt de F , $W(F)$, é isomorfo ao anel de grupo $W(\bar{F})[\Delta]$, onde Δ é um grupo com dois elementos. Consequentemente a forma binária $\langle 1, \pi \rangle$ representa apenas elementos em $\dot{F}^2 \cup \pi \dot{F}^2$. Szymiczek [Sz] tem chamado os elementos $a \in \dot{F}$ tais que $x^2 + ay^2$ representa apenas elementos em $\dot{F}^2 \cup a\dot{F}^2$ de elementos rígidos. É fácil checar que se F admite uma valorização v com ideal maximal M tal que $1 + M \subseteq \dot{F}^2$ então qualquer elemento de $\dot{F}$ cujo valor não é divisível por dois é rígido. Outros autores (ver [AEJ] e [Wa]) perceberam que se T é um subgrupo de $\dot{F}$ contendo $\dot{F}^2$, a existência de elementos $a \in \dot{F}$ que são T -rígidos, isto é, $T + aT \subseteq T \cup aT$ implica na existência de uma valorização v de F tal que $1 + M_v \subseteq T$. Se F possui elementos $R_1(F)$ -rígidos então F admite uma valorização que não é 2-divisível e $1 + M \subset R_1 F$.

Agora vamos fazer uma série de construções técnicas para demonstrar que a



existência de um elemento $R_1(F)$ -rígido no corpo implica na existência de um anel de valorização $R_1(F)$ -compatível. Será demonstrado que um corpo Hilbertiano possui uma valorização compatível com o radical. No próximo capítulo pretendemos mostrar que se A é uma álgebra de quatérnios com divisão sobre um corpo Hilbertiano F , uma valorização $R_1(F)$ -compatível de F se estende à álgebra de quatérnios. Será dado exemplos que mostram que este fato não é sempre verdadeiro.

5.1 Anéis de Valorizações $R_1(F)$ -compatíveis

Definição 5.1.1 Diz-se que $a \in \dot{F}$ é $R_1(F)$ -rígido se: $R_1(F) + aR_1(F) \subseteq R_1(F) \cup aR_1(F)$. Se a e $-a$ são $R_1(F)$ -rígidos diz-se que a é $R_1(F)$ -birrígido. Se a não é $R_1(F)$ -birrígido dizemos que a é $R_1(F)$ -básico. O subconjunto constituído por estes elementos é denotado por $B(R_1(F))$

Um anel de valorização de um corpo F é um subanel A de F tal que x ou $x^{-1} \in A$, para todos $x \in \dot{F}$. Este anel possui um único ideal maximal M e o grupo de unidades é precisamente $A \setminus M$. O corpo de frações de A é F e existe uma valorização natural associada à A , $v : F \rightarrow G$, $G = \frac{F}{U}$. A adição de G é a operação de multiplicação. Esta definição estende a definição dada em 2.3.1.

Definição 5.1.2 Seja A um anel de valorização do corpo F . Dizemos que A é $R_1(F)$ -compatível (ou compatível com o radical $R_1(F)$) se $1 + M \subseteq R_1(F)$. Da mesma forma, uma valorização v de F é dita $R_1(F)$ -compatível se $1 + M_v \subseteq R_1(F)$.

Note que: Como $R_1(F)$ é um subgrupo de $\dot{F}$, x é $R_1(F)$ -rígido se, e somente se, $1 + xR_1(F) \subset R_1(F) \cup xR_1(F)$.

Proposição 5.1.3 : *Seja A um anel de valorização de um corpo F com ideal maximal M*



e grupo das unidades U . Se $R_1(F)$ contém $1 + M$ então qualquer elemento de $\dot{F} \setminus UR_1(F)$ é $R_1(F)$ -rígido.

Demonstração:

Seja $x \in \dot{F} \setminus UR_1(F)$ e seja $t \in R_1(F)$. Como $x \in \dot{F} \setminus UR_1(F)$ então x não é unidade em A (senão $xt = u \in U \implies x = ut^{-1} \in UR_1(F)$), assim xt ou $(xt)^{-1} \in M$. Se $xt \in M$ então $1 + xt \in 1 + M \subset R_1(F)$, agora se $(xt)^{-1} \in M$ então $1 + (xt)^{-1} \in 1 + M \subset R_1(F)$. Logo $1 + xt \in xtR_1(F)$ e portanto $1 + xt \in xR_1(F)$ (pois $t \in R_1(F)$). Desta maneira, $1 + xt \in R_1(F) \cup xR_1(F)$ e portanto $1 + xR_1(F) \subset R_1(F) \cup xR_1(F)$. Logo x é $R_1(F)$ -rígido. ■

Para um subgrupo H de $\dot{F}$ definimos:

$$O_1 = O_1(H) = \{x \in F \mid x \notin H \text{ e } 1 + x \in R_1(F)\};$$

$$O_2 = O_2(H) = \{x \in H \mid x.O_1 \subseteq O_1\};$$

$$O(H) = O_1 \cup O_2 \text{ e}$$

$$U(H) = \{x \in O_2 \mid x^{-1} \in O_2\}.$$

Lema 5.1.4 *Seja H um subgrupo de $\dot{F}$ contendo $B(R_1(F))$. Se $-y \notin R_1(F)$ então $R_1(F) + yR_1(F) \subset H \cup yR_1(F)$.*

Demonstração:

Temos que mostrar que $\exists r_1, r_2 \in R_1(F)$ tal que $r_1 + yr_2 \in yR_1(F)$. Se $\exists r_1, r_2 \in R_1(F)$ com $r_1 + yr_2 \notin H$ então $(-r_1 - yr_2)$ é $R_1(F)$ -rígido. Logo $R_1(F) + (-r_1 - yr_2)R_1(F) \subset R_1(F) \cup (-r_1 - yr_2)R_1(F)$. Além disso $-yr_2 = r_1 - r_1 - yr_2 \in R_1(F) + (-r_1 - yr_2)R_1(F) \subset R_1(F) \cup (-r_1 - yr_2)R_1(F)$. Como $-y \notin R_1(F)$ segue que $-yr_2 \in (-r_1 - yr_2)R_1(F)$. Então $yr_2 = (r_1 + yr_2).r_3$, com $r_1, r_2, r_3 \in R_1(F)$. Logo $y \cdot \frac{r_2}{r_3} = r_1 + yr_2$. Assim $yR_1(F) = r_1 + yr_2$ e então $r_1 + yr_2 \in yR_1(F)$. Consequentemente $r_1 + yr_2 \in H \cup yR_1(F)$, e portanto $R_1(F) + yR_1(F) \subset H \cup yR_1(F)$. ■

Proposição 5.1.5 *Seja H um subgrupo de $\dot{F}$ contendo $B(R_1(F))$. Se A é um anel de valorização de F então:*

- (1) $UR_1(F) \subset H$.
- (2) $O_1 \subset M$.
- (3) *As seguintes condições são equivalentes:*
 - (a) $A = F$.
 - (b) $H = \dot{F}$.
 - (c) *O grupo de valores Γ é 2-divisível (isto é, $\Gamma = 2\Gamma$.)*
- (4) $1 + M \subset R_1(F)$
- (5) *Se $-1 \notin R_1(F)$ então A não é diádico.*
- (6) *Se para cada t em $R_1(F)$, $\exists x \in F$ tal que $1 - tx^2 \notin H$ então $R_1(F) = (1 + M)\dot{F}^2$.*

Demonstração:

(1) É suficiente mostrar que $U \subset H$, pois $R_1(F) \subset H$. Se $x \notin H$ então x é $R_1(F)$ -rígido. Assim $1 + x \in R_1(F) \cup xR_1(F)$, isto é, podemos considerar dois casos, ou $1 + x \in R_1(F)$, ou $1 + x \in xR_1(F)$.

Caso 1: Se $1 + x \in xR_1(F)$ então $x \notin O_1$. Como $x \notin H$ então $x \notin O_2$. Logo $x \notin O_1 \cup O_2 = A$, e portanto $x \notin U$ (pois $U \subset A$ e $x \notin A$).

Caso 2: Se $1 + x \in R_1(F)$ então $1 + x^{-1} \in x^{-1}R_1(F) = xR_1(F)$. Assim $x \notin A$ e portanto $x \notin U$. Logo $U \subset H$.

(2) Vamos tomar $x \notin M$. Se $x \in U$ então $x \in H$ por (1). Logo $x \notin O_1$. Se $x \notin U$ então $x \notin A = O_1 \cup O_2$, pois $x \notin M$ e $A = M \cup U$. Consequentemente $x \notin O_1$. Portanto $O_1 \subset M$.

(3)(a) $\Rightarrow$ (c) é óbvio.

(b) $\Rightarrow$ (a). Se $H = \dot{F}$ então $O_1 = \{0\}$ e $O_2 = \dot{F}$. Logo $A = O_1 \cup O_2 = \{0\} \cup \dot{F} = F$.

(c) $\Rightarrow$ (b) Se Γ é 2-divisível então $U\dot{F}^2 = \dot{F}$. Mas $U\dot{F}^2 \subset UR_1(F) \subset H$ por (1). Logo $\dot{F} \subset H$. Como H é um subgrupo de $\dot{F}$ temos que $H \subset \dot{F}$. Portanto $H = \dot{F}$.

(4) Seja $x \in M$. Se $x \in O_1$ então $1 + x \in R_1(F)$. Logo $1 + M \subset R_1(F)$. Agora, se $x \notin O_1$ então $x \in O_2$ (pois $x \in M \subset A = O_1 \cup O_2$). Daí $x \in H$. Desta maneira, podemos considerar o seguinte:

(i) Se Γ é 2-divisível então $A = F$ por (3) e neste caso $M = \{0\}$. Logo $1 + M \subset R_1(F)$.

(ii) Se $A \neq F$ então $x^{-1} \notin A$ (pois $x \in M$). Daí $x^{-1} \in H \setminus A$, e então $x^{-1} \notin O_2$, isto é, $x^{-1} \cdot O_1$ não está contido em O_1 . Portanto $\exists y \in O_1$ tal que $x^{-1}y \notin O_1$, ou seja, $1 + x^{-1}y \notin R_1(F)$. Além disso $x^{-1}y \notin H$, e então $x^{-1}y$ é $R_1(F)$ -rígido, ou seja, $1 + x^{-1}y \in R_1(F) \cup x^{-1}yR_1(F)$. Como $1 + x^{-1}y \notin R_1(F)$ então $1 + x^{-1}y \in x^{-1}yR_1(F)$, e ainda, como $R_1(F) \subset H$ segue que $x^{-1}yR_1(F) \cap H = \emptyset$. Desse modo $1 + x^{-1}y \notin H$. Desde que $-1 \in H$ segue que $-y \notin H$. Podemos ver também que $-y \in O_1$ pois $-1 \in O_2$ e $y \in O_1$. Logo $-y = -1 \cdot y \in O_1$. Assim, pela definição de O_1 temos que $1 - y \in R_1(F)$ e $1 + x^{-1}y = 1 + x^{-1} - x^{-1} + x^{-1}y = 1 + x^{-1} - x^{-1}(1 - y) \in (1 + x^{-1})R_1(F) - x^{-1}R_1(F)$. Como $x \in M$, obtemos $1 + x \in U \subset H$ e $1 + x^{-1} = x^{-1}(1 + x) \in H$. Pelo Lema 5.1.4 temos que $-(1 + x^{-1})(-x^{-1}) \in R_1(F)$. Daí $1 + x \in x^2R_1(F) \subset R_1(F)$.

(5) A não é diádico se $2 \notin M$. Vamos supor que $2 \in M$, então $-1 = 1 - 2 \in 1 + M \subset R_1(F)$ (absurdo, pois contradiz a hipótese). Logo A não é diádico.

(6) Por hipótese para cada $t \in R_1(F)$, $\exists x \in F$ tal que $tx^2 - 1 \notin H$. Além disso $1 + tx^2 - 1 = tx^2 \in R_1(F)$. Por (2) temos que $tx^2 - 1 \in O_1 \subset M$. Consequentemente $tx^2 \in 1 + M$ e daí $t \in (1 + M)\dot{F}^2$. Logo $R_1(F) \subset (1 + M)\dot{F}^2$. A inclusão $(1 + M)\dot{F}^2 \subset R_1(F)$ segue de (4). Portanto, $R_1(F) = (1 + M)\dot{F}^2$. ■



Lema 5.1.6 *Sejam a, x elementos de $\dot{F}$ tais que $a \notin R_1(F)$ e x, ax são $R_1(F)$ -rígidos. Se $1 + a, 1 - x \in R_1(F)$ então $1 + ax \in R_1(F)$.*

Demonstração:

Temos que $1 + ax = 1 - x + x + ax \in (1 - x)R_1(F) + x(1 + a)R_1(F) \subset R_1(F) + xR_1(F)$. Desde que ax é $R_1(F)$ -rígido segue-se que $1 + ax \in R_1(F) + axR_1(F) \subset R_1(F) \cup axR_1(F)$. Como $a \notin R_1(F)$, obtemos $xR_1(F) \cap axR_1(F) = \emptyset$. Logo $1 + ax \in R_1(F)$. ■

Proposição 5.1.7 *Seja H um subgrupo de $\dot{F}$ contendo $B(R_1(F))$. Então as seguintes proposições são válidas:*

- (1) O_2 é um monóide multiplicativo e $U(H)$ é um subgrupo de $\dot{F}$.
- (2) *Seja $x \in \dot{F} \setminus H$. Então $R_1(F) \cap xR_1(F) = \emptyset$. Além disso, $x \in O_1(H)$ se e somente se, $x^{-1} \notin O_1(H)$.*
- (3) *Seja $x \in H \setminus O_2(H)$. Então existem $y, z \in O_1(H)$ tais que $xyz = 1$, isto é, $x^{-1} = yz \in O_1(H).O_1(H)$.*
- (4) *Se $x \in O_1(H)$ então $-\frac{x}{1+x} \in O_1(H)$.*
- (5) *Se A é um anel de valorização de F tal que $(1 + M)\dot{F}^2 = R_1(F)$ então $M = O_1(U)$ e $U = O_2(U)$. Em particular $A = O(U)$.*

Demonstração:

- (1) O_2 é um monóide multiplicativo.

De fato, para quaisquer $a, b \in O_2, a \in H$ e $b \in H$. Logo $ab \in H$. Para qualquer $x \in O_1$, tem-se que $ax \in O_1$ e $bx \in O_1$, pois $a, b \in O_2$. Logo $ab.x = a(bx) \in O_1$ e assim $ab \in O_2$. Portanto O_2 é fechado para multiplicação. Então O_2 é um monóide, pois $1 \in O_2$. É evidente que o conjunto das unidades de O_2 constituem um subgrupo. Logo $U(H)$ é um subgrupo.

(2) Desde que $x \in \dot{F} \setminus H$ e $R_1(F) \subset H$ temos que $R_1(F) \cap xR_1(F) = \emptyset$. Como $B(R_1(F)) \subset H$ e $x \notin H$ segue que x é $R_1(F)$ -rígido, isto é, $1+x \in R_1(F) \cup xR_1(F)$. Logo $1+x \in R_1(F)$ ou $1+x \in xR_1(F)$. Se $1+x \in R_1(F)$ então $1+x^{-1} \in x^{-1}R_1(F)$, ou seja, se $x \in O_1$ então $x^{-1} \notin O_1$. Agora se $1+x \in xR_1(F)$ então $1+x^{-1} \in R_1(F)$, ou seja, se $x \notin O_1$ então $x^{-1} \in O_1$. Portanto $x \in O_1$ se e somente se $x^{-1} \notin O_1$.

(3) Seja $x \in H \setminus O_2$ então $\exists y \in O_1$ tal que $xy \notin O_1$. Como $x \in H$ e $y \notin H$ temos que $xy \notin H$, consequentemente por (2) $z = (xy)^{-1} \in O_1$ pois $xy \notin O_1$. Logo, $x^{-1} = yz \in O_1 \cdot O_1$.

(4) Por hipótese $x \notin H$ e $1+x \in R_1(F) \subset H$. Desde que $-1 \in B(R_1(F)) \subset H$ temos que $-\frac{x}{1+x} = -x \cdot \frac{1}{1+x} = -x \cdot (1+x)^{-1} \notin H$. Portanto, $1 + (-\frac{x}{1+x}) = \frac{1+x-x}{1+x} = \frac{1}{1+x} \in R_1(F)$, mostra que $-\frac{x}{1+x} \in O_1$.

(5) Por definição $O_1(U) = \{x \in F \mid x \notin U \text{ e } 1+x \in (1+M)\dot{F}^2\}$ e $O_2(U) = \{x \in U \mid x.O_1 \subseteq O_1\}$.

Vamos mostrar que $M = O_1(U)$. É óbvio que $M \subseteq O_1(U)$. Seja $a \in O_1(U)$. Então $a \notin U$ e $1+a \in (1+M)\dot{F}^2 = R_1(F)$. Se $a \notin M$ então $a \notin A$. Daí $a^{-1} \in M$, ou seja, $1+a^{-1} \in (1+M)\dot{F}^2 = R_1(F)$. Logo $1+a = a(1+a^{-1}) \in a(1+M)\dot{F}^2 = aR_1(F)$, assim $1+a \in R_1(F) \cap aR_1(F)$. Portanto $a \in R_1(F) \subset B(R_1(F)) \subset U$, absurdo! Logo $a \in M$ e assim $O_1(U) \subset M$. Agora provemos que $U = O_2(U)$.

Também é óbvio que $O_2(U) \subset U$. Seja $x \in U$. Desde que $O_1(U) = M$ segue-se que $x.O_1(U) = x.M \subseteq M = O_1(U)$, $\forall x \in U$. Logo $x \in O_2(U)$ e assim $U \subset O_2(U)$. Portanto $U = O_2(U)$. ■

Definição 5.1.8 Dizemos que $O(H)$ é *preaditivo* se $1 + O_1(H) \subset O_2(H)$.

Proposição 5.1.9 Se $O(H)$ é *aditivamente fechado*, mais geralmente se $O(H)$ é um *anel de valorização* então $O(H)$ é *preaditivo*.

Demonstração:

Por definição temos que $1 + O_1 \subset R_1(F) \subset H$. Por hipótese $1 + O_1 \subset O(H)$. Logo $1 + O_1 \subset H \cap (O(H)) = O_2$. Portanto $O(H)$ é preaditivo. ■

Lema 5.1.10 *As duas seguintes proposições são equivalentes:*

1. $O(H)$ é preaditivo.

2. $O_1(H).O_1(H) \subset 1 - R_1(F)$, isto é, se $x, y \in O_1(H)$ então $1 - xy \in R_1(F)$.

Além disso, se $O(H)$ é preaditivo, ainda temos:

3. Se $x \in \dot{F}$ satisfaz $1 + x \in O_2(H)$ e $y \in O_1(H)$ então $1 - xy \in R_1(F) \cap O_2(H)$.

Demonstração:

(1) $\iff$ (2)

Primeiro demonstraremos que a equivalência a seguir é válida:

$$1 + O_1 \subset O_2 \iff \text{se } x, z \in O_1 \text{ então } 1 + (1 + x).z \in R_1(F) \quad (*)$$

($\implies$) Seja $x, z \in O_1$ então por hipótese $1 + x \in O_2$. Logo $(1 + x) \cdot z \in O_1$ e assim $1 + (1 + x).z \in R_1(F)$.

($\impliedby$) Por hipótese $x \in O_1$, queremos mostrar que $1 + x \in O_2$. Para qualquer $x \in O_1$, temos que $1 + x \in O_2$ se, e somente se, $(1 + x).y \in O_1, \forall y \in O_1$. Desse modo, precisamos mostrar que $\forall y \in O_1, (1 + x).y \notin H$ e $1 + (1 + x).y \in R_1(F)$. Como $1 + (1 + x).z \in R_1(F)$ por hipótese, resta verificar que $(1 + x).y \notin H$. Desde que $x, y \in O_1$ segue que $1 + x \in R_1(F) \subset H$ e $y \notin H$. Logo $(1 + x).y \notin H$. Portanto (*) vale.

$$\text{Se } x, y \in \dot{F} \setminus \{-1\} \text{ então } x = -\frac{y}{1+y} \iff y = -\frac{x}{1+x}. \quad (**)$$

Usando a Proposição 5.1.7.(4) e quando (**) ocorre, $x \in O_1$ se, e somente se $y \in O_1$. Além disso $\forall z \in O_1$ temos que $1 + z \in R_1(F)$. Logo $z \neq -1$ pois $0 \notin R_1(F)$. Consequentemente



$\exists y = -\frac{z}{1+z} \in O_1$, pois $z \in O_1$. Então podemos escrever $z = -\frac{y}{1+y}$, para algum $y \in O_1$. Portanto vemos que (*) é equivalente à: "Se $x, y \in O_1$ então $1 + (1+x) \cdot (-\frac{y}{1+y}) \in R_1(F)$ ". E ainda, como $y \in O_1$ então $1+y \in R_1(F)$ e $y \neq -1$. Assim $1 - xy = (1+y)(1 + (1+x)(-\frac{y}{1+y})) \in R_1(F)$.

(3) Suponhamos $1+x \in O_2$ e $y \in O_1$. Desde que $y \in O_1$, pela Proposição 5.1.7.(4) segue-se que $-\frac{y}{1+y} \in O_1$. Portanto $1+x \in O_2$ implica que $(1+x) \cdot (-\frac{y}{1+y}) \in O_1$. Daí $1 + (1+x) \cdot (-\frac{y}{1+y}) \in R_1(F)$. Por (1) $1+O_1 \subset O_2$, logo $1 + (1+x) \cdot (-\frac{y}{1+y}) \in O_2$. Assim $1 + (1+x) \cdot (-\frac{y}{1+y}) \in R_1(F) \cap O_2$. Além disso, como $y \in O_1$ temos que $1+y \in R_1(F)$ e $1+y \in O_2$ pois $O(H)$ é preaditivo. Logo $1+y \in R_1(F) \cap O_2$. Portanto $1 - xy = (1+y)(1 + (1+x)(-\frac{y}{1+y})) \in R_1(F) \cap O_2$. ■

Lema 5.1.11 *Suponha que $O(H)$ é preaditivo. Então:*

1. $(O_1.O_1) \cap H \subseteq O_2$.
2. Se $x \in F \setminus O(H)$ então $x^{-1} \in O(H)$.
3. $-1 \in O_2$

Demonstração:

(1) Sejam $x, y \in O_1$ satisfazendo $xy \in H$. Vamos tomar $z \in O_1$, isto é, $1 + xyz \in R_1(F)$ pois $xyz \notin H$ é claramente satisfeito. Por hipótese $O(H)$ é preaditivo então $1+x \in O_2$ e $y \in O_1$. Daí pelo Lema 5.1.10.(3), $1 - xy \in R_1(F) \cap O_2$. Consequentemente, o Lema 5.1.10.(3) implica que $1 + xyz = 1 - (-xy) \cdot z \in R_1(F) \cap O_2$ desde que $1 - xy \in O_2$ e $z \in O_1$. Assim $1 + xyz \in R_1(F)$ e portanto $xyz \in O_1$. Logo, $xy \in (O_1.O_1) \cap H \subseteq O_2$.

(2) Queremos mostrar que se $x \notin O_1 \cup O_2$ então $x^{-1} \in O_1 \cup O_2$. Se $x \notin H$ então $x \notin O_2$. Pela Proposição 5.1.7.(2) se $x \notin O_1$ então $x^{-1} \in O_1$. Logo se $x \notin O_1 \cup O_2$ então $x^{-1} \in O_1 \cup O_2$. Podemos assumir agora $x \in H$, daí $x \notin O_1$. Como $x \in H$ então $x^{-1} \in H$. Além disso, se $x \in H$

e $x \notin O_2$ temos pela Proposição 5.1.7.(3) que $\exists x^{-1} \in O_1.O_1$. Logo $x^{-1} \in (O_1.O_1) \cap H$, daí pelo item (1) desse Lema $x^{-1} \in O_2$. Assim se $x \notin O_1 \cup O_2$ então $x^{-1} \in O_1 \cup O_2$. Portanto concluímos que se $x \notin O(H)$ então $x^{-1} \in O(H)$.

(3) Desde que $-1 \in H$, por (2) segue-se que $-1 \in O_2$. ■

Note que se $O(H)$ é preaditivo então $O(H)$ é um anel de valorização. Daí, se $(1+M)\dot{F}^2 = R_1(F)$ a Proposição 5.1.7 garante que $M_{O(H)} = O_1(U_{O(H)})$ e $U_{O(H)} = O_2(U_{O(H)})$.

Teorema 5.1.12 *Suponha que $O(H)$ é preaditivo. Então $O(H)$ é um anel de valorização $R_1(F)$ -compatível com $UR_1(F) \subseteq H$.*

Demonstração:

Primeiro mostraremos que $O(H)$ é fechado para multiplicação. Se $x, y \in O_2$ então $xy \in O_2$ pois O_2 é um monóide multiplicativo. Logo $xy \in O_1 \cup O_2 = O(H)$. Se $x \in O_1$ e $y \in O_2$ então por definição de O_2 temos que $xy \in O_1$. Logo $xy \in O(H)$. Dessa maneira, resta mostrar que se $x, y \in O_1$ então $xy \in O(H)$. Se $xy \in H$ então $xy \in (O_1.O_1) \cap H$. Daí pelo Lema 5.1.11.(1) $xy \in O_2$, logo $xy \in O(H)$. Com isso podemos assumir $xy \notin H$. Pelo Lema 5.1.11.(3) temos que $-1 \in O_2$, assim $-x \in O_1$. Deste modo pelo Lema 5.1.10.(2), $1+xy = 1 - (-x)y \in R_1(F)$. Isso nos mostra que $xy \in O_1$, assim $xy \in O(H)$. Portanto $O(H)$ é fechado para multiplicação.

Em seguida mostraremos que $1 + O(H) \subseteq O(H)$ pois precisaremos deste resultado para mostrar que $O(H)$ é aditivamente fechado. Desse modo, devemos mostrar que $1+z \in O(H), \forall z \in O(H)$. Se $z = -1$ então $1+(-1) = 0 \in O(H)$. Logo podemos assumir $z \neq -1$. Pela preaditividade, se $z \in O_1$ então $1+z \in O_2$. Assim $1+z \in O(H)$. Daí podemos tomar $z \in O_2$. Como $-1 \in O_2$, temos que $1 - (1+z) = -z \in O_2$. Consequentemente o Lema 5.1.10.(3) implica que $(*) 1 + (1+z) \cdot y \in R_1(F) \cap O_2 \subseteq R_1(F)$, sempre que $y \in O_1$. Se $1+z \in H$ então $1+z \in O_2$ já que $(1+z) \cdot y \in O_1$ (pois $(1+z) \cdot y \notin H$ e $1 + (1+z) \cdot y \in R_1(F)$). Logo $1+z \in O(H)$. Assumamos agora $1+z \notin H$. Temos que $1 + (1+z) \cdot (-\frac{1}{1+z}) = 0 \notin R_1(F)$, daí por $(*) (-\frac{1}{1+z}) \notin O_1$. Da Proposição 5.1.7.(2) conclui-se que $-(1+z) \in O_1$. Como $-1 \in O_2$, temos que $1+z \in O_1$ (pois



$-1 \cdot (-(1+z)) \in O_1$). Logo $1+z \in O(H)$.

Mostraremos agora que $O(H)$ é aditivamente fechado. Sejam $x, y \in O(H)$, e mostremos que $x+y \in O(H)$. Podemos tomar $x \neq 0$ e $y \neq 0$ (pois se $x=0$ e $y=0$ então $x+y=0 \in O(H)$). Pelo Lema 5.1.11.(2) xy^{-1} ou yx^{-1} estão em $O(H)$. Vamos assumir que $yx^{-1} \in O(H)$, então $1+yx^{-1} \in O(H)$ (pois acabamos de provar acima que $1+O(H) \subseteq O(H)$). Como $O(H)$ é fechado para multiplicação, temos que $x+y = x \cdot (1+yx^{-1}) \in O(H)$. Portanto $O(H)$ é fechado para adição. Pelo Lema 5.1.11.(2) temos que $O(H)$ é um anel de valorização de F . Desse modo a Proposição 5.1.5.(1) nos mostra que $UR_1(F) \subset H$.

Para concluir precisamos somente mostrar que $O(H)$ é $R_1(F)$ -compatível. Seja $x \in O(H) \setminus U$ (logo $x \in M$). Devemos mostrar que $1+x \in R_1(F)$. Se $x \in O_1$ isto é verdade por definição. Então assumimos $x \in O_2$. Como $x \in O_1 \cup O_2 = O(H)$, pelo Lema 5.1.11.(2) $x^{-1} \notin O_1 \cup O_2$. Assim $x^{-1} \notin O_2$. Como $x \in O_2$ temos que $x \in H$. Logo $x^{-1} \in H$. Assim $x^{-1} \in H \setminus O_2$. Pela Proposição 5.1.7.(3) tem-se que $x = yz$ para algum $y, z \in O_1$. Desde que $-1 \in O_2$ segue-se que $-y \in O_1$. O Lema 5.1.10.(2) implica que $1+x = 1+yz = 1 - (-y)z \in R_1(F)$. Portanto $O(H)$ é um anel de valorização $R_1(F)$ -compatível. ■

Corolário 5.1.13 *Suponha que $\hat{H}$ é um subgrupo de $\hat{F}$ tal que $R_1(F) \subseteq H \subseteq \hat{H}$. Suponha também que $O(H)$ é um anel de valorização de F $R_1(F)$ -compatível. Então $O(\hat{H})$ é um anel de valorização de F $R_1(F)$ -compatível contendo $O(H)$.*

Demonstração:

Como $H \subseteq \hat{H}$ concluímos que $((\hat{F} \setminus \hat{H}) \cap O(H)) = ((\hat{F} \setminus \hat{H}) \cap O_1(H)) = O_1(\hat{H}) \quad (\#)$

Pelo Teorema 5.1.12 para mostrar que $O(\hat{H})$ é um anel de valorização de F $R_1(F)$ -compatível basta mostrar que $O(\hat{H})$ é preaditivo. Sejam $x, y \in O_1(\hat{H})$. Então $x \notin \hat{H}$, $y \notin \hat{H}$, $1+x \in R_1(F)$ e $1+y \in R_1(F)$. Como $H \subseteq \hat{H}$ segue que $x \notin H$ e $y \notin H$. Logo $x, y \in O_1(H)$. Como $O(H)$ é preaditivo então pelo Lema 5.1.10, $x, y \in O_1(H)$ implica que $1-xy \in R_1(F)$. Portanto $x, y \in O_1(\hat{H})$ implica que $1-xy \in R_1(F)$. Assim pelo Lema 5.1.10 podemos concluir que $O(\hat{H})$



é preaditivo. Logo $O(\hat{H})$ é um anel de valorização de F $R_1(F)$ -compatível.

Agora só resta mostrar que $O(H) \subset O(\hat{H})$. Seja $x \in O(H)$. Se $x \notin \hat{H}$ então $x \in (\dot{F} \setminus \hat{H}) \cap O(H)$. Logo por (#) $x \in O_1(\hat{H}) \subset O(\hat{H})$. Agora se $x \in \hat{H}$ então $x \in \hat{H} \cap O(H)$. Seja $y \in O_1(\hat{H}) \subset O_1(H)$. Daí $y \in O(H)$ e $y \notin \hat{H}$. Assim $xy \in O(H)$ e $xy \notin H$. Logo $xy \in (\dot{F} \setminus \hat{H}) \cap O(H)$, e então por (#) $xy \in O_1(\hat{H})$. Por definição de $O_2(\hat{H})$ temos que $x \in O_2(\hat{H})$, pois $y \in O_1(\hat{H})$ e $xy \in O_1(\hat{H})$. Portanto $x \in O(\hat{H})$, e assim concluímos que $O(H) \subset O(\hat{H})$. ■

Proposição 5.1.14 *Se existe um elemento $u \in U \setminus R_1(F)$ então $O(H)$ é um Anel de Valorização de F $R_1(F)$ -compatível.*

Demonstração:

Pelo Teorema 5.1.12 só precisamos que $O(H)$ seja preaditivo e pelo Lema 5.1.10 basta mostrar que " $x, y \in O_1(H)$ implica que $1 - xy \in R_1(F)$ ".

Seja $x \in O_1(H)$ então $x \notin H$ e $1+x \in R_1(F)$. Como $x \notin H$ segue-se que $x \notin B(R_1(F)) \subseteq H$. Assim x é $R_1(F)$ -birrígido. O mesmo vale para $y \in O_1(H)$. Desta maneira $1 - xy = (1+x) - x(1+y) \in R_1(F) + (-x)R_1(F) \subset R_1(F) \cup (-x)R_1(F)$ (*). Por hipótese $\exists u \in U \setminus R_1(F)$, assim $u \notin R_1(F)$. Logo $u^{-1} \notin R_1(F)$. Além disso, xu^{-1} e $yu \in O_1$ (por definição de $U(H)$). Daí $xu^{-1} \notin H$, $yu \notin H$, $1+xu^{-1} \in R_1(F)$ e $1+yu \in R_1(F)$. Como $xu^{-1} \notin H$ segue-se que $xu^{-1} \notin B(R_1(F)) \subseteq H$. Assim xu^{-1} é $R_1(F)$ -birrígido. O mesmo vale para yu . Logo $1 - xy = 1 - xu^{-1}uy \in R_1(F) + (-xu^{-1})R_1(F) \subset R_1(F) \cup (-xu^{-1})R_1(F)$ (**). Agora $u \notin R_1(F)$ significa que $xR_1(F) \cap (xu^{-1})R_1(F) = \emptyset$. Então por (*) e (**) temos que $1 - xy \in R_1(F)$. ■

Lema 5.1.15 *Suponha que $u \in H$ satisfaz $u \notin R_1(F)$ e $1 - u^{-1} \notin R_1(F)$. Então $u \in O_2(H)$.*

Demonstração:

Basta mostrar que $u \in O_2$, ou seja, $\exists x \in O_1$ tal que $ux \in O_1$ (pois $u \in H$ por hipótese). Como $u \notin R_1(F)$ e $1 - u^{-1} \notin R_1(F)$ não podemos ter $u = 1 + u - 1 \in R_1(F) \cup (u - 1)R_1(F)$. De fato, por hipótese $u \notin R_1(F)$. Então resta verificar que $u \notin (u - 1)R_1(F)$. Se $u \in (u - 1)R_1(F)$ então $u = (u - 1) \cdot r$, $r \in R_1(F)$. Daí $u = ur - r$ e assim $u = \frac{r}{r - 1} = r' \in R_1(F)$. Logo $u \in R_1(F)$, absurdo! Portanto $u \notin (u - 1)R_1(F)$.

Desta maneira $u = 1 + (u - 1) \notin R_1(F) \cup (u - 1)R_1(F)$. Logo $(u - 1)$ não é $R_1(F)$ -rígido. Assim $u - 1 \in B(R_1(F)) \subset H$.

Seja $x \in O_1$ então $x \notin H$ e $1 + x \in R_1(F)$. Como $x \notin H$ segue-se que x é $R_1(F)$ -rígido, ou seja, $1 + x \in R_1(F) \cup xR_1(F)$. Como $u, u - 1 \in H$ temos que ux e $(u - 1)x \notin H$. Desse modo ambos são $R_1(F)$ -rígidos. Portanto $1 + ux \in R_1(F) \cup uxR_1(F)$ e $1 + ux = (1 + x) + (u - 1)x \in R_1(F) \cup (u - 1)xR_1(F)$. Além disso $1 - u^{-1} \notin R_1(F)$ implica que (*) $uxR_1(F) \cap (u - 1)xR_1(F) = \emptyset$ (pois se $\exists z \in uxR_1(F) \cap (u - 1)xR_1(F)$ então $z = uxr = (u - 1)xr'$, daí $r = \frac{u - 1}{u} \cdot r'$ e $\frac{r}{r'} = (1 - u^{-1})$, logo $(1 - u^{-1}) \in R_1(F)$, absurdo!) Portanto por (*) $1 + ux \in R_1(F)$, isto é, $ux \in O_1$ (pois $ux \notin H$). Consequentemente $u \in O_2$.

■

Proposição 5.1.16 *Suponha que existe um elemento $a \in \dot{F} \setminus R_1(F)$ tal que $-a$ não é $R_1(F)$ -rígido. Então $O(H)$ é um anel de valorização de F , $R_1(F)$ -compatível.*

Demonstração:

Como $-a$ não é $R_1(F)$ -rígido temos que $a \in B(R_1(F)) \subseteq H$ e existe $t \in R_1(F)$ tal que (*) $1 - at \notin R_1(F) \cup (-a)R_1(F)$. Seja $u := at$, então $u \in H$ (pois $a \in H$ e $t \in R_1(F) \subset H$); $u \notin R_1(F)$ (pois $a \notin R_1(F)$); $(1 - u) \notin R_1(F)$ por (*); $(1 - u) \notin (-u)R_1(F)$ (pois se $(1 - u) \in (-u)R_1(F)$ então $1 - u = -ur$, com $r \in R_1(F)$. Daí $u - ur = 1 \Rightarrow u(1 - r) = 1 \Rightarrow u = \frac{1}{1 - r} \Rightarrow u = 1 - r^{-1} \Rightarrow r^{-1} = 1 - u \in R_1(F)$, absurdo). E $1 - u^{-1} \notin R_1(F)$ (pois se $1 - u^{-1} \in R_1(F)$). Então $1 - u^{-1} = r', r' \in R_1(F)$. Segue-se que $u^{-1} = 1 - r' \Rightarrow u = \frac{1}{1 - r'} \Rightarrow$

$u = 1 - \frac{1}{r'} \Rightarrow u - 1 = r'' \in R_1(F)$, o que é um absurdo). Por essa razão o Lema 5.1.15 implica que $u, u^{-1} \in O_2$, assim $u \in U(H)$. Como $u \notin R_1(F)$ aplicando a Proposição 5.1.14 concluímos que $O(H)$ é um anel de valorização de F $R_1(F)$ -compatível. ■

Definição 5.1.17 Dizemos que $R_1(F)$ é *excepcional* se $B(R_1(F)) = \pm R_1(F)$ e $-1 \in R_1(F)$ ou $R_1(F)$ é aditivamente fechado.

Teorema 5.1.18 *Seja H um subgrupo de $\dot{F}$ contendo $B(R_1(F))$. Então existe um subgrupo $\hat{H}$ de $\dot{F}$ tal que $H \subseteq \hat{H}$, $[\hat{H} : H] \leq 2$ e $O(\hat{H})$ é um anel de valorização de F $R_1(F)$ -compatível tal que $UR_1(F) \subseteq \hat{H}$. Além disso, $\hat{H} = H$, a menos que $R_1(F)$ seja excepcional.*

Demonstração:

Se $\exists \hat{H}$ com $O(\hat{H})$ é um anel de valorização de F $R_1(F)$ -compatível então pelo Teorema 5.1.12 $UR_1(F) \subseteq \hat{H}$.

Se $\exists a \in \dot{F} \setminus R_1(F)$ tal que $-a$ não é $R_1(F)$ -rígido a Proposição 5.1.16 garante que $O(H)$ é um anel de valorização de F $R_1(F)$ -compatível. Neste caso basta tomar $\hat{H} = H$.

Agora vamos supor que não existe $a \in \dot{F} \setminus R_1(F)$ tal que $-a$ não é $R_1(F)$ -rígido. Então a Proposição 5.1.16 não implica que $O(H)$ seja um anel de valorização de F , $R_1(F)$ -compatível. Vamos mostrar que neste caso $R_1(F)$ é excepcional. Temos que qualquer $b \in \dot{F} \setminus (-R_1(F))$ é $R_1(F)$ -rígido e $\forall b \in \dot{F} \setminus R_1(F)$, $-b$ é $R_1(F)$ -rígido (*). Logo todo $b \in \dot{F} \setminus (\pm R_1(F))$ é $R_1(F)$ -birrígido e $B(R_1(F)) = \pm R_1(F)$. Suponha agora na adição que $-1 \notin R_1(F)$, então por (*) 1 é $R_1(F)$ -rígido, ou seja, $R_1(F) + 1R_1(F) \subseteq R_1(F) \cup 1R_1(F) = R_1(F)$. Logo $R_1(F) + R_1(F) \subseteq R_1(F)$, e portanto $R_1(F)$ é aditivamente fechado. Assim $R_1(F)$ é excepcional.

Se $O(H)$ é preaditivo o Teorema 5.1.12 garante que $O(H)$ é um anel de valorização de F $R_1(F)$ -compatível. Novamente basta fazer $\hat{H} = H$, pois $O(H)$ tem a propriedade desejada. Então vamos assumir que $O(H)$ não é preaditivo (em particular $R_1(F)$ é excepcional). Logo $\exists a, b \in O_1(H)$ tal que $1 - ab \notin R_1(F)$ pelo Lema 5.1.10.(2). Como $a \in O_1(H)$ segue-se que $a \notin H \supset R_1(F)$. Portanto a é $R_1(F)$ -birrígido. Desta maneira

$1 - ab = (1 + a) - a(1 + b) \in R_1(F) + (-a)R_1(F) \subseteq R_1(F) \cup (-a)R_1(F)$. Logo $1 - ab \in (-a)R_1(F)$ (pois $1 - ab \notin R_1(F)$). Analogamente $1 - ab \in (-b)R_1(F)$. Assim $1 - ab = -at$ e $1 - ab = -bt_1$; $t, t_1 \in R_1(F)$. Logo $-at = -bt_1$, isto é, $at = bt_1$; $t, t_1 \in R_1(F)$. Além disso, como $R_1(F)$ é grupo podemos concluir que $aR_1(F) = bR_1(F)$, portanto

$$1 - ab \in (-a)R_1(F) \text{ e } aR_1(F) = bR_1(F) \quad (**).$$

Seja $\hat{H} := H \cup aH$, vamos mostrar que $\hat{H}$ é grupo.

(i) $\hat{H}$ é fechado para a multiplicação.

De fato. Seja $x, y \in \hat{H}$. Se $x, y \in H$ então $xy \in H$ (pois H é grupo). Logo $xy \in \hat{H}$. Tomemos agora $x, y \in aH$. Como $a^2 \in R_1(F) \subset H$ temos que $xy \in H \subset \hat{H}$. Finalmente se $x \in H$ e $y \in aH$, então $xy \in aH \subset \hat{H}$. Logo $\hat{H}$ é fechado.

(ii) Todo elemento de $\hat{H}$ possui elemento inverso. Se $x \in H$ então $x^{-1} \in H \subset \hat{H}$, pois H é grupo. Se $x = ah$, $h \in H$, então $x^{-1} = a^{-1}h^{-1}$. Portanto $x^{-1} = \frac{a}{a^2} \cdot h^{-1} = a \cdot (a^{-2}h) \in aH \subseteq \hat{H}$. Logo $x^{-1} \in \hat{H}$, qualquer que seja $x \in \hat{H}$.

A seguir mostraremos que $-a \in U(\hat{H})$, isto é, $-a$ e $-a^{-1} \in O_2(\hat{H})$, o que conclui a demonstração do Teorema pela Proposição 5.1.14, uma vez que $-a \notin (\pm R_1(F))$. Seja $z \in O_1(\hat{H}) \subset O(\hat{H})$ então $z \notin \hat{H}$ e $1 + z \in R_1(F)$. Temos que mostrar que $-az, -a^{-1}z \in O_1(\hat{H}, R_1(F))$, isto é, $1 - az$ e $1 - a^{-1}z$ estão em $R_1(F)$ (desde que $-az \notin \hat{H}$ e $-a^{-1}z \notin H$), pois com isso mostramos que $-a$ e $-a^{-1}$ estão em $O_2(\hat{H})$. Se $z = 0$ então $1 - a \cdot 0 = 1 \in R_1(F)$ e $1 - a^{-1} \cdot 0 = 1 \in R_1(F)$. Logo podemos assumir $z \neq 0$. Se $1 - az \notin R_1(F)$ então (**) mostra que $zR_1(F) = aR_1(F)$. Assim $zt = at_1$; $t, t_1 \in R_1(F)$, e então $z = a \cdot \frac{t_1}{t} = at_2$; $t_2 \in R_1(F)$, ou seja, $z \in aR_1(F) \subset aH \subset \hat{H}$. Isto contradiz o fato de $z \notin \hat{H}$, portanto $1 - az \in R_1(F)$. Finalmente suponhamos que $1 - a^{-1}z \notin R_1(F)$, isto é, $-a^{-1}z \notin O_1(\hat{H}, R_1(F))$. Pela Proposição 5.1.7.(2), $-az^{-1} \in O_1(\hat{H})$. Agora $1 - (-az^{-1})(-bz) = 1 - ab \notin R_1(F)$. Por (**) temos que $1 - ab \in -az^{-1}R_1(F)$. Além disso (**) também implica que $1 - ab \in -aR_1(F)$. Portanto concluímos que $-z \in R_1(F)$ e assim $z \in R_1(F)$, pois $R_1(F)$ é grupo. Logo $z \in R_1(F) \subset H \subset \hat{H}$ (absurdo pois $z \notin \hat{H}$). Portanto $1 - a^{-1}z \in R_1(F)$. ■

No próximo Teorema usaremos o conceito de *u-invariante de F* que é definido por $u(F) = \max\{\dim \varphi, \text{onde } \varphi \text{ percorre todas as formas anisotrópicas sobre } F\}$. Se não existir este número dizemos que $u(F) = \infty$. O *u-invariante de F* pode ser caracterizado também das duas seguintes maneiras:

$$u(F) = \min\{n \mid \text{formas de } \dim > n \text{ sobre } F \text{ são isotrópicas}\};$$

$$u(F) = \min\{n \mid \text{formas de } \dim \geq n \text{ sobre } F \text{ são universais}\}.$$

Por exemplo $u(\mathbb{R}) = \infty$, pois $m < 1 >$ é anisotrópica para qualquer $m > 1$. Se F é quadraticamente fechado então $u(F) = 1$. Se F é um corpo finito então $u(F) = 2$, como pode ser deduzido facilmente do Lema 2.2.4 e Teorema 1.3.6.

O próximo teorema garante que a grande maioria dos corpos onde se concentram os problemas mais difíceis de formas quadráticas possui uma valorização com as características desejadas.

Teorema 5.1.19 *Seja F um corpo com $4 \leq u(F) < \infty$. Então existe uma valorização v de F $R_1(F)$ -compatível tal que o grupo de valores Γ não é 2-divisível.*

Demonstração:

Como $\dot{F}^2 \subset R_1(F)$ segue da Proposição 5.1.5 que é suficiente construir um anel de valorização $O(H)$ onde H é um subgrupo próprio de $\dot{F}$.

Se $D < 1, \alpha > = \dot{F}, \forall \alpha \in \dot{F}$, então $q = < a, b >$ é universal. Assim $u(F) \leq 2$, o que é um absurdo, por hipótese. Logo $\exists H = D < 1, \alpha > \neq \dot{F}$, para algum $\alpha \in \dot{F}$.

Desde que $-\alpha \in \dot{F} \setminus R_1(F)$ temos dois casos a considerar:

(i) Se existe um elemento $a \in \dot{F} \setminus R_1(F)$ tal que $-a$ não é $R_1(F)$ -rígido então a Proposição 5.1.16 e a Proposição 5.1.5.(3) garantem que $O(H)$ tem a propriedade desejada.

(ii) Se $-a$ é $R_1(F)$ -rígido para todo elemento $a \in \dot{F} \setminus R_1(F)$, considere $H = -R_1(F) \cup R_1(F)$. Como $u(F)$ é finito segue que F não é ordenado (senão $n < 1 >$ seria anisotrópica $\forall n > 0$),



assim $H \neq \dot{F}$. Agora vamos provar que $-1 \in R_1(F)$. Se $-1 \notin R_1(F)$ pela hipótese (ii), 1 é $R_1(F)$ -rígido. Assim $R_1(F) \subset D < 1, 1 > \subset R_1(F) + R_1(F) \subseteq R_1(F) \cup R_1(F) = R_1(F)$. Logo $R_1(F) = D < 1, 1 >$. De [L, (XI, Teorema 1.6)] segue que $D < 1, 1 > = D(\infty)$, assim $R_1(F) = D(\infty)$. Como F não é ordenado temos que $R_1(F) = \dot{F}$. (De fato -1 é soma de quadrados desde que $n < 1 >$ é isotrópica para algum $n > 0$; e para qualquer $a \in F$, $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2 \in R_1(F)$.) Então qualquer 1-forma de Pfister é universal e assim $u(F) \leq 2$ (absurdo! pois $4 \leq u(F) < \infty$). Logo $-1 \in R_1(F)$. Assim $H = R_1(F)$, pois $H = -R_1(F) \cup R_1(F)$ e $-1 \in R_1(F)$, e também $-aR_1(F) = aR_1(F), \forall a \in \dot{F}$. Portanto a é $R_1(F)$ -birrígido, $\forall a \in \dot{F}$, logo $B(R_1(F)) = \pm R_1(F)$. Pelo Teorema 5.1.18 existe um subgrupo $\hat{H}$ de $\dot{F}$ tal que $H = R_1(F) \subset \hat{H}, [\hat{H} : H] \leq 2$ e $O(\hat{H})$ é um anel de valorização de F $R_1(F)$ -compatível. Para terminar a demonstração basta provar que $\hat{H} \neq \dot{F}$. Se $\hat{H} = H$ então $\hat{H} \neq \dot{F}$. Agora, se $\hat{H} = H \cup bH, b \notin H = R_1(F)$ então do Teorema 4.1.3.(2) concluímos que $D < 1, -b > \neq \dot{F}$. Como $-1 \in R_1(F)$ temos que $\hat{H} = R_1(F) \cup bR_1(F) \subset D < 1, b > = D < 1, -b > \neq \dot{F}$. Portanto $\hat{H} \neq \dot{F}$. ■

Corolário 5.1.20 *Seja $\psi = \langle\langle a_1, a_2 \rangle\rangle, (n \geq 2)$ uma 2-forma Pfister anisotrópica sobre F . Se $D\psi \cap (M_v \setminus M_v^2) \neq \emptyset$ então a_2 pode ser tomado em $M_v \setminus M_v^2$, e $D < 1, a_2 > = R_1(F) \cup a_2 R_1(F)$.*

Demonstração:

Vamos provar primeiro que m é $R_1(F)$ -rígido para todo $m \in M_v \setminus M_v^2$. Seja $x^2 + my^2 \neq 0$. Desde que $z = \frac{my^2}{x^2}$ ou $z^{-1} \in A_v$, temos que $x^2(1 + m(\frac{y}{x})^2) \in U_v^1 \dot{F}^2$, ou $my^2(1 + \frac{x^2}{my^2}) \in mU_v^1 \dot{F}^2$. Como $R_1(F) = U_v^1 \dot{F}^2$ pela Proposição 5.1.5.(6), temos que $D < 1, m > = R_1(F) \cup mR_1(F)$.

Se $a_i \in U_v$, para todo $i = 1, 2$ então de [L, (X, Proposição (1.5))] temos que $D\psi' \subset U_v$. Como $D\psi = \bigcup_{a \in D\psi'} D < 1, a >$, existe $a \in U_v$ tal que $-m = x^2 + ay^2$, para algum $m \in M_v \setminus M_v^2$, ou seja, $-ay^2 = x^2 + m$, então $-a = x^2 \cdot y^{-2} + my^{-2} \in D < 1, m >$. Assim $-a \in D < 1, m > \cap U_v = R_1(F)$. De [L, (X, Proposição (1.5))] existe um elemento $b_2 \in \dot{F}$ tal que $\psi = \langle\langle a, b_2 \rangle\rangle$. Pela Proposição 4.1.3 ψ é F -hiperbólico, o que é um absurdo. Portanto a_2 pode

ser tomado em $M_v \setminus M_v^2$ e $D < 1, a_2 \rangle = R_1(F) \cup a_2 R_1(F)$. ■

Definição 5.1.21 Um corpo F é dito *Hilbertiano* se ele possui uma única álgebra de quatérnios com divisão, a menos de isomorfismo, equivalentemente, se ele possui uma única forma quadrática anisotrópica do tipo $\langle 1, a, b, ab \rangle$, a menos de isometria.

Exemplos destes corpos são os corpos de séries de potências sobre um corpo finito; corpos locais p -ádicos. Estes possuem o radical trivial. O Teorema 4.1.13 e Observação 4.1.12 dão uma infinidade de exemplos de corpos Hilbertianos com radicais não triviais.

Se F é um corpo Hilbertiano ordenado prova-se que $R_1(F) = D < 1, 1 \rangle =$ (somas de quadrados) e $\psi = \langle\langle 1, 1 \rangle\rangle = 4 < 1 \rangle$. Logo $(\frac{-1, -1}{F})$ é a única álgebra de quatérnios sobre F a menos de isomorfismo.

Lema 5.1.22 Seja $\psi = \langle\langle a_1, a_2 \rangle\rangle$ uma forma quadrática anisotrópica sobre um corpo Hilbertiano F . Então $D\psi' = \dot{F} \setminus R_1(F)$, onde $\psi' \simeq \langle a_1, a_2, a_1 a_2 \rangle$.

Demonstração:

Seja $r \in R_1(F)$. Se $-r \in D\psi'$, existem $a, x \in \dot{F}$ tais que $\psi' \simeq \langle -r, a, x \rangle$, com $-rax = 1$. Daí $x = -ra$ e $\psi' \simeq \langle -r, a, -ra \rangle$. Logo $\psi \simeq \langle 1, -r, a, -ra \rangle = \langle\langle -r, a \rangle\rangle$. Pela Proposição 4.1.3.(2) ψ é hiperbólica, absurdo. Então segue-se que $D\psi' \subset \dot{F} \setminus R_1(F)$.

Reciprocamente se $c \in \dot{F} \setminus R_1(F)$ então existe uma 1-forma de Pfister $\varphi = \langle 1, b_1 \rangle$ sobre F tal que $-c \notin D\varphi$. Assim $\varphi + \langle c \rangle \varphi$ é anisotrópica (Proposição 4.1.3). Como F é Hilbertiano, temos que $\varphi + \langle c \rangle \varphi \simeq \psi = 1 + \psi'$. Cancelando $\langle 1 \rangle$ temos que $\varphi' + \langle c \rangle \varphi \simeq \psi'$. Assim $c \in D\psi'$. ■



Capítulo 6

Extensões de Valorizações

6.1 Extensões de Valorizações

Uma característica fundamental da teoria de valorizações sobre corpos é que para corpos $F \subseteq K$, todas as valorizações de F tem uma extensão para K (possivelmente muitas extensões diferentes). Contudo, não temos esta propriedade de um modo geral, em se tratando de extensões de valorizações sobre anéis com divisão. Alguns resultados particulares são conhecidos, como por exemplo quando o grupo de valores esta contido em $\mathbb{R}$. Neste capítulo, usando uma técnica apresentada por A. R. Wadsworth em [W], demonstraremos que se F é um corpo Hilbertiano então F possui uma valorização compatível com o radical e esta valorização se estende à única álgebra de quatérnios com divisão sobre F , desde que F seja Hilbertiano.

Para o Teorema que vem a seguir precisaremos de quocientes g/n , onde g pertence a um grupo totalmente ordenado G e n é um número natural não nulo. Para dar uma estrutura ao conjunto destes elementos considere G um grupo totalmente ordenado pela relação $\preceq$ e seja $\overline{G}$ o conjunto dos pares (g, n) com $g \in G$ e $n \in \mathbb{N}$, $n > 0$. A relação

$$(g, n) \sim (h, m) \text{ se e somente se } mg = nh$$



para todos $g, h \in G$ e $n, m \in \mathbb{N}^*$ é uma relação de equivalência sobre o conjunto $\overline{G}$. Denote por $\frac{g}{n}$ a classe de (g, n) e por G' o conjunto $\{\frac{g}{n}, g \in G, n > 0, n \in \mathbb{N}\}$. A operação

$$\frac{g}{n} + \frac{h}{m} = \frac{mg + nh}{nm},$$

para quaisquer $g/n, h/m$ em G' , está bem definida e dá à G' uma estrutura de grupo. A relação binária definida sobre G' por $h/m \preceq g/n$ se, e somente se, $nh \preceq mg$ em G é uma relação de ordem total que estende a ordem de G . Em outras palavras, $\varphi : G \rightarrow G'$ dada por $\varphi(g) = g/1$ é um homomorfismo de grupos, injetor e compatível com as ordens de G e de G' .

A *Propriedade Universal do Produto Tensorial* afirma que se M e N são A -módulos (onde A é um anel comutativo com unidade), então existe um par (T, h) , onde T é um A -módulo e $h : M \times N \rightarrow T$ é A -bilinear com a propriedade: Para qualquer A -módulo P e qualquer $f : M \times N \rightarrow P$ A -bilinear, existe uma única aplicação A -linear $f' : T \rightarrow P$ tal que $f = f' \circ h$. Em outras palavras, cada função A -linear definida sobre $M \times N$ se fatora através de T . Todo grupo H é um $\mathbb{Z}$ -módulo, e são estes módulos que vão nos interessar aqui.

Agora consideremos o grupo $G \otimes_{\mathbb{Z}} \mathbb{Q}$, onde G é um grupo totalmente ordenado. Todo elemento x de $G \otimes_{\mathbb{Z}} \mathbb{Q}$ é uma soma finita de elementos da forma $g \otimes a/b$ com $g \in G$ e $a/b \in \mathbb{Q}$, mas é possível escrevê-los na forma simples: $g \otimes a/b$. De fato, seja $x = \sum_{i=1}^n (g_i \otimes (a_i/b_i)) \in G \otimes_{\mathbb{Z}} \mathbb{Q}$ e denote por $c_i := a_i(\prod_{j \neq i} b_j)$ e por $b := \prod_{j=1}^n b_j$. Então $x = \sum_{i=1}^n g_i \otimes (c_i/b)$, e como $c_i \in \mathbb{Z}$ tem-se que $x = \sum_{i=1}^n (c_i g_i \otimes 1/b) = (\sum_{i=1}^n c_i g_i) \otimes 1/b = g \otimes 1/b$.

É simples a verificação de que a relação de $g \otimes \frac{1}{b} \preceq h \otimes \frac{1}{c}$ se $cg \preceq bh$ em G , com $g \otimes \frac{1}{b}, h \otimes \frac{1}{c} \in G \otimes_{\mathbb{Z}} \mathbb{Q}$ é uma relação de ordem total.

Um grupo Δ é chamado de *Divisible Hull* de G se Δ é isomorfo a $G \otimes_{\mathbb{Z}} \mathbb{Q}$. O Lema que segue mostra que G' pode ser tomado como o Divisible Hull de G .

Lema 6.1.1 *Seja G um grupo livre de torção e G' definido como antes. Então existe um*



isomorfismo $G \otimes_{\mathbb{Z}} \mathbb{Q} \simeq G'$.

Demonstração

Definimos $\varphi : G \times \mathbb{Q} \rightarrow G'$ por $\varphi(g, \frac{a}{b}) = \frac{ag}{b}$. Temos que φ é $\mathbb{Z}$ -bilinear pois: $\varphi(\alpha g, \frac{a}{b}) = \frac{a(\alpha g)}{b} = \frac{(\alpha a)g}{b} = \varphi(g, \frac{\alpha a}{b})$, e $\varphi(g_1 + g_2, \frac{a}{b}) = \frac{a(g_1 + g_2)}{b} = \frac{ag_1 + ag_2}{b} = \frac{ag_1}{b} + \frac{ag_2}{b} = \varphi(g_1, \frac{a}{b}) + \varphi(g_2, \frac{a}{b})$. Finalmente $\varphi(g, \frac{a}{b} + \frac{c}{d}) = \varphi(g, \frac{ad + bc}{bd}) = \frac{(ad + bc)g}{bd} = \frac{ad.g + cb.g}{bd} = \frac{ad.g}{bd} + \frac{cb.g}{bd} = \frac{a.g}{b} + \frac{c.g}{d} = \varphi(g, \frac{a}{b}) + \varphi(g, \frac{c}{d})$.

Pela Propriedade Universal do produto tensorial φ induz $f : G \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow G'$ definida por $f(g \otimes \frac{a}{b}) = \frac{ag}{b}$ que é evidentemente sobrejetora. Como todo elemento de $G \otimes_{\mathbb{Z}} \mathbb{Q}$ é do tipo $x = g \otimes \frac{a}{b}$, se $x \in \text{Ker}(f)$ então em G' , $\frac{a.g}{b} = 0 = \frac{0}{m}$, $m > 0$. Assim $m(ag) = ma.g = 0$ em G . Como G é livre de torção temos que $ma = 0$ em $\mathbb{Z}$ e como $m > 0$ vem que $a = 0$. Logo $x = 0$ e f é um isomorfismo. ■

Note que se G é totalmente ordenado então o Lema anterior é válido e o isomorfismo $G \otimes_{\mathbb{Z}} \mathbb{Q} \simeq G'$ é compatível com as ordens dos grupos $G \otimes_{\mathbb{Z}} \mathbb{Q}$ e G' .

Definição 6.1.2 (A) Um subanel A de um anel de divisão (= corpo não comutativo) D é dito *anel de valorização* se para todo $x \in D$, $x \in A$ ou $x^{-1} \in A$.

(B) Uma *valorização de Krull* de D é a função $w : \dot{D} \rightarrow G$, onde G é um grupo totalmente ordenado, e para quaisquer $a, b \in \dot{D}$ tem-se:

$$(i) \quad w(ab) = w(a) + w(b)$$

$$(ii) \quad w(a + b) \geq \min \{w(a), w(b)\} \text{ se } b \neq -a, \forall a, b \in \dot{D}.$$

Vamos definir também $w(0) = \infty$, e estender a adição de D para $D \cup \{\infty\}$ por $\alpha + \infty = \infty + \alpha = \infty + \infty = \infty$, para todo $\alpha \in G$.

Adotaremos a notação aditiva para G mesmo se G não for abeliano.



Seja D uma álgebra sobre F , e w uma valorização de D . Se E é um subanel de D dizemos que (D, w) é uma *extensão* de $(E, w|_E)$, onde $w|_E$ é a restrição de w à E .

Se $A \subseteq B$ são anéis, diz-se que um elemento $b \in B$ é *inteiro* sobre A se b é raiz de um polinômio mônico com coeficientes em A . O conjunto A' definido por $A' := \{x \in B \mid x \text{ é inteiro sobre } A\}$ é um sub-anel de B que contém A , chamado de *fecho inteiro* de A em B . Se $A' = B$ dizemos que B é *inteiro sobre* A . Se B é o corpo de frações de A e $A' = A$ dizemos que A é *integralmente fechado*. Estes resultados e os Lemas que seguem também são bastante conhecidos na teoria de valorizações.

Lema 6.1.3 *Seja A um anel de valorização de F . Então*

1. *A é um anel local (isto é: possui um único ideal maximal).*
2. *A é integralmente fechado.*

Demonstração:

Ver [AM, Prop. 5.18] ■

Lema 6.1.4 *Sejam F um corpo, v uma valorização de F e K uma extensão algébrica de F . Seja A' o fecho inteiro de A em K . Se W é o conjunto de todas as valorizações w de K que estendem v e M' o conjunto dos ideais maximais de A' , então existe uma correspondência bijetora entre os elementos de W e M' .*

Demonstração:

Ver [B, Chapitre 6: Valuations §8, n°6, Prop.6] ■



Teorema 6.1.5

Seja $D = (\frac{a}{F}, b)$ uma álgebra de quatérnios com divisão e v uma valorização de Krull de F . Então v se estende a uma valorização w em D se, e somente se v tem uma única extensão à cada corpo K , com $F \subseteq K \subseteq D$.

Demonstração:

($\Leftarrow$) Sejam $\Gamma_F := v(\dot{F}R)$ o grupo de valores de v e Δ o Divisible Hull de Γ_F . Portanto Γ_F é um grupo abeliano livre de torção e $\Delta \simeq \Gamma_F \otimes_{\mathbb{Z}} \mathbb{Q}$. Pelo Lema 6.1.1 e os cálculos que o antecede a ordem total de Γ_F se estende de modo único à uma ordem total de Δ . Para cada extensão algébrica L de F e cada extensão w de v para L podemos ver $w(L^*)$ como um subgrupo de Δ .

De fato, para qualquer $x \in L$ seja $a_0X^n + a_1X^{n-1} + \dots + a_n$ um polinômio sobre F que anula x . Então $a_0x^n + a_1x^{n-1} + \dots + a_n = 0$ e $w(a_0x^n + a_1x^{n-1} + \dots + a_n) = \infty$. Como $v(x + y) \geq \min\{v(x), v(y)\}$ segue-se que $v(x + y) = \min\{v(x), v(y)\}$ quando $v(x) \neq v(y)$. Assim existe $i \neq j$ tal que $w(a_ix^i) = w(a_jx^j)$, ou seja, $w(a_i) + iw(x) = w(a_j) + jw(x)$. Segue-se que $w(x) = \frac{w(a_j) - w(a_i)}{i - j} \in \Delta \simeq \Gamma_F \otimes_{\mathbb{Z}} \mathbb{Q}$.

Agora suponhamos que v admite uma única extensão à cada corpo K , com $F \subseteq K \subseteq D$, e definimos a função

$$w : \dot{D} \longrightarrow \Delta \text{ por } w(a) = \frac{1}{2}v(N(a)), \quad (*)$$

onde $N(a) = a\bar{a} \in F$, (veja Definição 3.1.6). Se vê claramente que a restrição de w à F coincide com v .

Desejamos demonstrar que w é uma valorização de D . Primeiro vamos verificar que para todo subcorpo K de D , $w|_K$ é a valorização de K estendendo v . De fato, como K é uma extensão quadrática de F seja $\sigma(x) = \bar{x}$ a conjugação em K e $u : K \rightarrow \Delta$ a única valorização de K que estende v . Desde que $u \circ \sigma$ também é uma valorização de K que estende v , por



hipótese elas devem coincidir. Portanto para todo $b \in K$ tem-se que $u(\bar{b}) = u(\sigma(b)) = u(b)$.
Consequentemente

$$w(b) = \frac{1}{2}v(N(b)) = \frac{1}{2}v(\bar{b}.b) = \frac{1}{2}u(\bar{b}.b) = \frac{1}{2}(u(\sigma(b)) + u(b)) = u(b).$$

Portanto $w|_K = u|_K$, e $w|_K$ é a única valorização de K que estende v .

Para demonstrarmos que w é uma valorização de D , tomamos $a, b \in \dot{D}$, a, b quaisquer. Como N é multiplicativa temos que $w(ab) = w(a) + w(b)$. Agora assumimos $b \neq -a$, e seja K qualquer subcorpo de D contendo $a^{-1}b$. Desde que $w|_K$ é uma valorização de K , $w(1 + a^{-1}b) \geq \min\{w(1), w(a^{-1}b)\}$. Consequentemente $w(a + b) = w(a(1 + a^{-1}b)) = w(a) + w(1 + a^{-1}b) \geq w(a) + \min\{w(1), w(a^{-1}b)\} = \min\{w(a) + w(1), w(a) + w(a^{-1}b)\} = \min\{w(a), w(b)\}$. Isto conclui uma parte da demonstração.

($\Rightarrow$) Suponhamos que v se estende à uma valorização w de D , e demonstraremos primeiro que o grupo de valores totalmente ordenado Γ_D é abeliano. Para isto, provemos por indução em k que se existem $\alpha, \beta \in \Gamma_D$ tais que $\alpha + \beta + (-\alpha) < \beta$ em Γ_D , então $\alpha + k\beta + (-\alpha) < k\beta, \forall k \in \mathbb{N} - \{0\}$. Se $\alpha + \beta < \beta + \alpha$ então $\alpha + 2\beta = (\alpha + \beta) + \beta < (\beta + \alpha) + \beta = \beta + (\alpha + \beta) < \beta + (\beta + \alpha) = 2\beta + \alpha$.

Agora se $\alpha + k\beta < k\beta + \alpha$ então $\alpha + (k+1)\beta = \alpha + (k\beta + \beta) = (\alpha + k\beta) + \beta < (k\beta + \alpha) + \beta = k\beta + (\alpha + \beta) < k\beta + (\beta + \alpha) = (k+1)\beta + \alpha$. Desde que $\Delta \simeq G'$ (Lema 6.1.1), vem que $k\beta \in \Gamma_F$ para algum $k \in \mathbb{N} - \{0\}$. Como os elementos de Γ_F comutam com todos os elementos de Γ_D segue-se que $\alpha + k\beta + (-\alpha) = k\beta$. Logo $\alpha + \beta + (-\alpha) = \beta$, para todos $\alpha, \beta \in \Gamma_G$. Isto demonstra que Γ_D é abeliano e temos $w(aba^{-1}) = w(b), \forall a, b \in \dot{D}$.

Agora vamos demonstrar que o anel de valorização de w , $A_w := \{a \in \dot{D} \text{ tal que } w(a) \geq 0\} \cup \{0\}$ é inteiro sobre A_v : o anel de valorização v . Como o polinômio minimal de cada elemento $a \in A_w$ é $f(X) = X^2 + T(a)X + N(a) = (X - a)(X - \bar{a})$, basta demonstrarmos que $T(a)$ e $N(a) \in A_v$. Pelo item anterior, basta demonstrarmos que $\bar{a} = b^{-1}ab$, para algum $b \in D$, pois daí $w(\bar{a}) = w(a) \geq 0$. Ocorre que se b é um quaternio puro $\bar{a} = b^{-1}ab$ é equivalente a $b\bar{a} + a\bar{b} = 0$, ou seja: $b_N(a, b) = 0$, onde b_N é a forma bilinear

associada a forma quadrática N (ver Definição 3.1.7). Em outras palavras, b é um quatérnio puro ortogonal a a . Como a dimensão do F -subespaço de D constituído pelos quatérnios puros $D_0 := \{x \in D \mid T(x) = 0\}$ tem dimensão 3, segue-se que a equação $b_N(a, b) = 0$, é solúvel em D_0 para $a \in D$ fixado. Assim $f(X) \in A_v[X]$ e portanto a é inteiro sobre A_v . Logo A_w é inteiro sobre A_v .

Agora seja K um corpo intermediário, $F \subseteq K \subseteq D$. Então $A_0 := A_w \cap K$ é um anel de valorização de K , e por isso integralmente fechado. Desde que $A_0 \subset A_w$ segue-se que A_0 é inteiro sobre A_v . Pelo Lema 6.1.3 temos que A_0 é um anel local, e pelo Lema 6.1.4 a valorização correspondente a A_0 (isto é: $w|_K$) é a única extensão de v para K . Isto conclui o Teorema. ■

Corolário 6.1.6 *Sejam D , F e v como no teorema anterior, e suponha que v estende à uma valorização w em D . Então:*

1. *w é a única extensão de v à D ; de fato, w é determinado a partir de v pela fórmula (*) do teorema 1.5 .*
2. *O anel de valorização de w , A_w é igual a $\{a \in D \mid a \text{ é inteiro sobre } A_v\}$, que coincide com $\{a \in D \mid N(a) \in A_v\}$.*

Agora vamos usar o Teorema anterior e demonstrar que qualquer valorização $R_1(F)$ -compatível sobre um corpo Hilbertiano com $u(F)$ finito (equivalentemente, F não ordenado) se estende a única álgebra de quatérnios com divisão (a menos de isomorfismo) sobre F . Como estes corpos tem u -invariante maior ou igual a 4 (pois existe uma 2-forma de Pfister anisotrópica), o Teorema 5.1.19 garante que existe uma valorização de F , $R_1 F$ -compatível.

Pelo Teorema anterior precisamos demonstrar que v se estende de modo único a cada extensão quadrática K com $F \subseteq K \subseteq D$, onde D é a única álgebra de quatérnios com divisão. Começemos com a

Proposição 6.1.7 *Seja v uma valorização não-diádica de F tal que $\Gamma_v \neq 2\Gamma_v$. Se v é $R_1(F)$ -compatível então para cada $a \in F \setminus R_1(F)$, existe uma única extensão de v em $K = F(\sqrt{a})$.*

Demonstração

Seja $K = F(\sqrt{a})$. Como $K = F(\sqrt{a^{-1}})$, podemos considerar $a \in A_v$: o anel de valorizações de v . Da teoria de valorizações sobre corpos, temos que v se estende a K . Se existirem duas valorizações distintas w_1 e w_2 de K que estendem v então

$$2 = \sum_{i=1}^2 (\overline{K_i} : \overline{F})(\Gamma_i : \Gamma),$$

onde $\Gamma_i := w_i(K)$, $\Gamma := v(F)$ e $\overline{K_i} = \frac{A_{w_i}}{M_{w_i}}$. Assim $\Gamma_i = \Gamma$ e $\overline{K_i} = \overline{F}$. Isto implica que existe $s \in \dot{F}$ tal que $w_i(\sqrt{a}) = v(s)$ e portanto $v(a) = w_i(a) = w_i(\sqrt{a}^2) = 2w_i(\sqrt{a}) = 2v(s)$. Logo $v(a) = v(s^2)$. Então existe $u \in U_i$ tal que $a = us^2$ e daí $\sqrt{a} = \sqrt{u}s$. Concluimos que podemos supor que $a \in U_i$. Consequentemente $\sqrt{a} \in \overline{K_i} = \overline{F}$. Logo existe $\bar{b} \in \overline{F}$ tal que $\sqrt{a} = \bar{b}$, ou $\bar{a} = \bar{b}^2 \in \overline{F}$. Assim $a \equiv b^2 \pmod{M_v}$, ou $a = b^2 + m = (1 + \frac{m}{b^2})b^2$. Como $b^2 \in \dot{F}^2 \subseteq R_1(F)$ segue-se que $a \in R_1(F)$, absurdo. Portanto v possui uma única extensão w a K . ■

Observação 6.1.8 *Se demonstrarmos que toda extensão quadrática de F contida em uma álgebra de quatérnios com divisão D sobre F são do tipo $F(\sqrt{a})$, $a \in \dot{F} \setminus R_1(F)$, então pela Proposição 6.1.7 e Teorema 6.1.5 segue-se que toda valorização v de F $R_1(F)$ -compatível se estende a álgebra de quatérnios D , desde que F seja Hilbertiano.*

Temos:

Proposição 6.1.9 *Seja F um corpo Hilbertiano não ordenado, e $D = (\frac{\alpha, \beta}{F})$ a única álgebra de quatérnios com divisão sobre F , a menos de isomorfismo. Então toda extensão quadrática $F(\sqrt{a})$ de F contida em D é não radical (isto é: $a \notin R_1(F)$).*

Demonstração

Cada $x \in D$ satisfaz uma equação do tipo $X^2 - T(x)X + N(x) = 0$. Seja $D_0 = \{x \in D : T(x) = 0\} = \{x \in D \setminus F : x^2 \in F\}$. Para $d \in D_0$, $F(d)$ é uma extensão quadrática de F , pois $d^2 = -N(d) \in F$. Assim, qualquer extensão quadrática $K = F(\sqrt{a})$ de F está contida em D se, e somente se, $a \in -D < -\alpha, -\beta, \alpha\beta >$. Do Lema 5.1.22, segue-se a conclusão. ■

Exemplo 6.1.10 Os Corpos $K((X))$, com K finito; os corpos p -ádicos $\mathbb{Q}_p$, $p \neq 2$ e todos os corpos $F \subset \mathbb{Q}_p$ construídos em Lema 4.1.11 e Teorema 4.1.13 são corpos Hilbertianos que admitem valorizações $R_1(F)$ -compatível, a saber, as valorizações dadas por $v(X) = 1$ e as valorizações p -Ádicas respectivamente. Logo estas valorizações são estendíveis a única álgebra de quatérnios com divisão (a menos de isomorfismo) sobre o corpo em questão.

Para finalizar P. M. Cohn em [C, p.67] demonstra que a álgebra de quatérnios $D = (\frac{-1, -3}{\mathbb{Q}})$ não admite extensão da valorização 2-ádica de $\mathbb{Q}$. Cohn demonstra ainda no artigo supracitado, que de um modo geral qualquer valorização p -ádica ($p \neq 2$) não se estende à uma valorização w sobre uma álgebra de quatérnios com divisão sobre $\mathbb{Q}$, (veja [C]). Por outro lado, o corpo $\mathbb{Q}$ não é Hilbertiano.

Bibliografia

- [AEJ] ARASON, J. K., ELMAN, R. and JACOB, B. Rigid Elements, Valuations, and Realization of Witt Rings. J. of Algebra, **1987**, *110*, 449-467.
- [AM] ATIYAH, M.F. e MACDONALD, I.G.: *Introduccìon Al Álgebra Conmutativa*, Addison-Wesley Publishing Company, Inc., Massachusetts, 1969.
- [B] BOURBAKI, N.: *Algèbre Commutative, Chapitre 6: Valuations*; Hermann, Paris, 1964.
- [C] COHN. P.M. On Extending Valuations in Division Algebras. Studia Sci. Math. Hungar., **1981**, *16*, 65-70.
- [De] DELANG, L. A Family of Fields With Finite Square Class Number. Scientia Sinica, **1980**, Vol. XXIII(10), 1226-1236.
- [K] KAPLANSKY, I. Fröhlich's Local Quadratic Forms. J. Reine Angew. Math., **1969**, *239/240*, 74-77.
- [L] LAM, T. Y.: *The Algebraic Theory of Quadratic Forms*; Mathematics Lectures Note Series; Reading, W. A. Benjamin, New York, 1980.
- [S] SANTOS, C.M. On Witt Rings Of Quaternion Algebra Over 1-Hilbert Fields. Communications in Algebra, To appear in 2002.
- [Sz] SZYMICZEK, K. Quadratic Forms Over Fields. Dissert. Math. Rozprawy Math., **1977**, *52*.



