ESTUDOS DE RELAÇÕES ENTRE UM CORPO FORMALMENTE REAL E SEU ANEL DE WITT

MÁRIO CONRADO CAVICHIA

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E CIÊNCIA COMPUTAÇÃO

CAMPINAS – SÃO PAULO
BRASIL

ESTUDOS DE RELAÇÕES ENTRE UM CORPO FORMALMENTE REAL E SEU ANEL DE WITT

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pelo Sr. Mario Conrado Cavichia e aprovada pela Comissão Julgadora.

Campinas, 9 de março de 1988

Prof. Dr. Antonio José Engler
Orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação - UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

Aos meus pais Mario e Irene,
e a minha tia Nelza (in memorian)

Agradeço ao Prof. Dr. Antonio José Engler pela orientação e estímulo recebido, aos meus pais por todo apoio dado nesses anos e ao CNPq pelo custeio parcial de meus estudos de Pós-Graduação e, a todos aqueles que colaboraram para a realização deste trabalho, em especial à Ires e Helena.

ÍNDICE

INTRODUÇÃO

O objetivo do trabalho é estudar alguns aspectos da chamado anel de Witt de um corpo de característica diferente de dois.

O Capítulo I foi incluído com o objetivo de atingir o leitor iniciante no assunto,, propiciando um primeiro contato com conceitos básicos da teoria das formas quadráticas e também visando a completude do trabalho. Nele além dos conceitos básicos, damos a construção do anel de Witt. Um leitor conhecedor do assunto poderá perfeitamente iniciar sua leitura pelo Capítulo II. Neste tratamos do anel de Witt de corpos formalmente reais e veremos também como caracterizar as ordens de um corpo via ideias primos do anel de Witt.

No Capítulo III veremos como certos corpos formalmente reais F podem ser caracterizados através de W(F) bem como certas propriedades de extensões podem ser estudadas ainda que em forma mais fraca.

No Capítulo IV estudamos W(Q) e percebemos quão complexa pode ser sua estrutura apesar da aparente simplicidade do corpo dos números racionais.

Em todo texto informações gerais serão apresentadas na forma de observações enumeradas em ordem crescente em cada capítulo

CAPÍTULO I

INFORMAÇÕES GERAIS SOBRE O ANEL DE WITT

Neste capítulo após a definição de formas quadráticas e sua caracterização através de matrizes, apresentamos a noção de espaços quadráticos e de isometria entre tais espaços. Visando a construção do anel de Witt, definimos uma operação induzida pela "soma ortogonal, que dá ao conjunto M(F), das classes de equivalência de espaços quadráticos, uma estrutura de semi-grupo comutativo com cancelamento e a partir daí, usando o processo universal de Groethendieck, construímos o grupo e o anel de Witt. Apresentamos também o anel de Witt, caracterizado através de relações, bem como os teoremas do Cancelamento, da Decomposição e o da Diagonalização, resultados tradicionais nesta teoria.

No texto, a menos que se diga o contrário, F denotará um corpo de característica diferente de dois (car F $\neq$ 2). Além disso, informações gerais serão apresentadas na forma de observações enumeradas em ordem crescente em cada capítulo.

Definição 1 - Uma forma quadrática de dimensão n sobre um corpo F é um polinômio homogêneo de grau dois, dado por

$$f(X_1, X_2, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \in F[X_1, X_2, \ldots, X_n]$$

Observação 1 - A forma quadrática $f(X) = \sum_{i,j=1}^{n} a_{ij}X_iX_j$ pode ser reescrita como $f(X) = \sum_{i,j=1}^{n} \frac{1}{2}(a_{ij} + a_{ji})\, X_iX_j$, donde se conclui que cada forma determina uma única matriz simétrica que será representada por M_f. Assim

$$f(X) = (X_1 \ldots X_n)(M_f)\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = X^t M_f X$$

Observação 2 - Podemos também apresentar uma forma quadrática como uma função de V em F, com V um F - espaço vetorial n - dimensional.

Para tanto seja $B: V \times V \longrightarrow F$ uma forma bilinear simétrica. A função $q = q_B : V \longrightarrow F$, com $q(x) = B(x, x)$, $x \in V$, é chamada função quadrática e temos:

i) $q(ax) = a^2 q(x)$

ii) $B(x,y) = \frac{1}{2}[\, q(x+y) - q(x) - q(y)\,]$.

Se em V for escolhida uma base $\{ e_1, e_2, \ldots, e_n \}$ então obte

mos a forma quadrática

$$f(X_1, X_2, \ldots, X_n) = \sum_{i,j} B(e_i, e_j)\, X_i X_j$$

onde $M_f = \left(B(e_i, e_j) \right)$ e temos assim uma correspondência bijetora entre formas e funções quadráticas e daqui para frente não faremos a distinção sem que haja perigo de confusão, pois a diferença far-se-á clara no contexto.

Definição 2 - Duas formas quadráticas f e g, de mesma dimensão n, são ditas equivalentes se existir uma matriz inversível C, n x n, com $f(X) = g(CX)$, com X dado por

$$X = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}$$

Notação: Se f é equivalente a g escreveremos $f \simeq g$

Observação 3 - Pela definição de equivalência de formas quadráticas, vemos que se $f \simeq g$ então

$$f(X) = g(X) = (CX)^t\, M_g\, (CX) = X^t\, (C^t M_g C)\, X$$

Como $f(X) = X^t M_f X$, vem que $M_f = C^t M_g C$.

Concluímos, portanto, que o estudo de equivalência de formas quadráticas se reduz ao estudo de semelhança de matrizes, e ainda mais, a relação definida acima é efetivamente uma relação de equivalência

Exemplo 1 - As formas $g(X) = X_1^2 + X_2^2$ e $f(X) = X_1^2 + 2X_1X_2 + 2X_2^2$ são equivalentes

Com efeito, temos

$$M_f = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \qquad M_g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e se tomarmos a matriz inversível

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

vemos que $M_f = C^t M_g C$

O exemplo a seguir aparece em muitos textos sobre formas quadráticas e, será apresentado aqui, pois será utilizado mais adiante.

Exemplo 2 - As formas $f(X) = X_1^2 - X_2^2$ e $g(X) = X_1X_2$ são equivalentes, pois

$$M_f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = C^t M_g C$$

Observação 4 - Qualquer espaço vetorial V, n - dimensional, pode ser identificado como o espaço das n - uplas F^n e considerando uma forma bilinear $B:V \times V \to F$, teremos uma forma quadrática dada por $q(x) = B(x, x)$. O par (V, B) será denominado espaço quadrático n - dimensional.

Usaremos, eventualmente, a notação (V, B, q) quando quizermos ressaltar a forma q.

Veremos, a seguir, a relação entre matrizes de formas quadráticas quando tomadas bases diferentes.

Sejam (V, B) um espaço quadrático n - dimensional e $\{e_1, e_2, \ldots, e_n\}$ uma base de V. Já observamos anteriormente que

$$f(X_1, X_2, \ldots, X_n) = \sum_{i,j=1}^{n} B(e_i, e_j)\, X_iX_j$$

é uma forma quadrática, onde $M_f = (B(e_i, e_j))$. Se escolhermos outra base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ obteremos uma forma quadrática g, tal que $g \tilde{} f$. Com efeito, se $\alpha_i = \sum_k C_{ki}\, e_k$, então

$$(M_g)_{ij} = B(\alpha_i, \alpha_j) = B\left(\sum_k c_{ki}\, e_k, \sum_\ell c_{\ell j}\, e_\ell\right) = \sum_{k,\ell} c_{ki}\, B(e_k, e_\ell)\, c_{\ell j} =$$

$$= (C^t M_f C)_{ij}$$

onde $C = (C_{k\ell})$ (simples verificação)

Concluímos então, que o espaço quadrático (V, B) determina uma classe de equivalência de formas quadráticas, aqui indicada por (f_B).

Definição 3: Diremos que dois espaços quadráticos, de mesma dimensão, (V_1, B_1) e (V_2, B_2) são isométricos, $(V_1, B_1) \simeq (V_2, B_2)$ ou $V_1 \simeq V_2$, se existir um isomorfismo linear $T : V_1 \longrightarrow V_2$ com $B_2\big(T(x), T(y)\big) = B_1(x, y)$, para quaisquer x, y em V_1.

Lema 1: $(V_1, B_1) \simeq (V_2, B_2)$ se e somente se $(f_{B_1}) = (f_{B_2})$

Demonstração: Supondo $(V_1, B_1) \simeq (V_2, B_2)$, vem que existe um isomorfismo $T : V_1 \longrightarrow V_2$ com $B_2\big(T(x), T(y)\big) = B_1(x, y)$ e como todo isomorfismo entre espaços vetoriais é dado por uma matriz inversível A, vem que

$$x^t\, (A^t M_{f_{B_2}}\, A)\, y = x^t\, M_{f_{B_1}}\, y$$

e assim

$$M_{f_{B_1}} = A^t M_{f_{B_2}} A$$

donde concluimos que $f_{B_1} \simeq f_{B_2}$

A igualdade $B(x, y) = x^t M_{f_B} y$, usada acima, é imediata, pois

$$B(x, y) = (x_1, x_2, \ldots x_n) \begin{pmatrix} B(e_1, e_1) \ldots B(e_1, e_n) \\ \\ B(e_n, e_1) \ldots B(e_n, e_n) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

com $B: V \times V \longrightarrow F$ e $\{ e_1, e_2, \ldots, e_n \}$ uma base do n - dimensional espaço V.

Vamos supor agora que $(f_{B_1}) = (f_{B_2})$. Temos então que $f_{B_1} \simeq f_{B_2}$, isto é, existe uma matriz inversível C, tal que

$$M_{f_{B_1}} = C^t M_{f_{B_2}} C$$

A matriz C dá origem a um isomorfismo $T: V_1 \longrightarrow V_2$, onde

$$B_2(T(x), T(y)) = x^t C^t M_{f_{B_2}} C y = x^t M_{f_{B_1}} y = B_1 (x, y) \blacksquare$$

Pelo lema anterior vemos que existe uma correspon-

dência biunívoca entre as classes de equivalência de forma quadráticas de dimensão n e as classes de equivalência dos espaços quadráticos n - dimensionais. Sob esse aspecto identificaremos espaços quadráticos e formas quadráticas.

Definição 4 - Seja (V, B) um espaço quadrático, diremos que dois vetores x e y de V são ortogonais se $B(x, y) = 0$. Além disso, diremos que dois subconjuntos M e N de V são ortogonais se $B(x, y) = 0$ para todo x de M e todo y de N.

Notação - Se M é ortogonal a N, escreveremos $M \perp N$.

Definição 5 - Seja U um subespaço de V. Então o subconjunto

$$U^{\perp} = \{ x \in V \ / \ \{x\} \perp U \}$$

será denominado complemento ortogonal de U.

Observação 5 - $U^{\perp}$ é um subespaço vetorial de V.

Demonstração: Óbvia. Ver [S].

Definição 6 - O subespaço $V^{\perp}$ será chamado radical de V, indicado por rad V e diremos que (V, B) é regular se $rad\ (V) = V^{\perp} = \{ 0 \}$.

Definição 7 - Tomaremos como o **espaço zero** o 0 - dimensional espaço vetorial consistindo apenas do vetor zero e com $q(0) = 0$. Tal espaço será indicado por $(0, 0)$.

Observação 6 - No contexto é conveniente incluirmos o espaço zero, acima definido, tomando-o como regular.

Definição 8 - Sejam q uma forma quadrática sobre F e $d \in F$. Diremos que f representa **d** se existir $v \in F^n$ com $q(v) = d$ e colocamos $D(q) = \{ d \in F \ / \ \text{existe } v \in V \text{ com } q(v) = d \}$, que poderá ser denotado por $D(V)$.

Definição 9 - Um espaço quadrático (V, B, q) é dito universal se q representa todo elemento não nulo de F.

Observação 7 - Notemos ainda que se (V, B) é regular então $B(x, y) = 0$ para todo y em V implicará em $x = 0$.

Definição 10 - Seja v um vetor não nulo de um espaço quadrático (V, B). Então

1 - Diremos que v é um vetor isotrópico se $B(v, v) = 0$.

2 - Se $B(v, v) \neq 0$, então v é chamado anisotrópico.

Se existir um vetor isotrópico, diremos que (V, B)

é um espaço isotrópico, caso contrário, (V, B) será anisotrópico.

Definição 11 - Um espaço (V, B) é dito totalmente isotrópico ou trivial se $B(v, v) = 0$ para todo $v \in V$.

Devido a **definição 10**, podemos dizer que um espaço (V, B, q) é isotrópico se zero não é representado trivialmente, isto é, existe $0 \neq v \in V$ com $q(v) = 0$.

Pensando na construção de um anel comutativo onde deverá valer a lei do cancelamento, definiremos a primeira operação, chamada soma direta ou soma ortogonal.

Observação 8 - Sejam os espaços quadráticos regulares (V_1, B_1, q_1) e (V_2, B_2, q_2) e definamos outro espaço (V, B, q), onde

$$V = V_1 \oplus V_2 \quad e \quad q = q_1 \perp q_2 : V_1 \oplus V_2 \longrightarrow F$$

com

$$q(v_1 \oplus v_2) = q_1(v_1) + q_2(v_2)$$

para

$$v_1 \in V_1 \text{ e } v_2 \in V_2$$

Observemos que $q/_{V_1} = q_1$, $q/_{V_2} = q_2$ e que $V_1 \perp V_2$ em (V, B), pois

$$B(v_1, v_2) = \frac{1}{2}[q(v_1 \oplus v_2) - q(v_1) - q(v_2)] = \frac{1}{2}[q_1(v_1) + q_2(v_2) -$$

$$- q_1(v_1) - q_2(v_2)] = 0$$

para todo $v_1 \in V_1$ e $v_2 \in V_2$.

Usaremos também a notação $V_1 \perp V_2$ para indicarmos a soma direta $V_1 \oplus V_2$ e a operação $\perp$ passa a ser chamada soma ortogonal.

Exemplo 3 - Se $f(X_1, X_2) = X_1^2 - X_2^2$ e $g(X_1, X_2) = X_1X_2$

então

$$(f \perp g)(X_1, X_2, X_3, X_4) = X_1^2 - X_2^2 + X_3X_4$$

Teorema 1: (Critério de Representação) Seja (V, B, q) um espaço quadrático qualquer e $d \in \dot{F}$. Então $d \in D(q)$ se e somente se existe outro espaço quadrático (V', B') tal que $V \simeq \langle d \rangle \perp V'$

($\Longleftarrow$) Se $V \simeq \langle d \rangle \perp V'$ então de $D(\langle d \rangle \perp V') = D(q)$, logo d $D(q)$.

($\Longrightarrow$) Vamos tomar $v \in V$ tal que $q(v) = d$

Primeiramente veremos que V pode ser assumido como regular.

Seja W um subespaço vetorial de V tal que

$$V = (\text{rad } V) \oplus W = (\text{rad } V) \perp W$$

Pela observação 8, vem que $D(V) = D(W)$, e tem-se que ainda que W é regular.

Portanto V pode ser tomado como regular.

Consideremos o subespaço $F.v$. Tal subespaço é isométrico a $\langle d \rangle$ e $(F \,.\, v) \cap (F \,.\, v)^{\perp} = 0$. Como

$$\dim (F.v) + \dim (F.v)^{\perp} = \dim V$$

vem que

$$V \simeq \langle d \rangle \perp (F \,.\, v)^{\perp} \blacksquare$$

Teorema 2 (Teorema da Diagonalização): Toda forma quadrática é equivalente a uma soma ortogonal de formas uni-dimensionais.

Demonstração: Vamos seguir a demonstração feita em [L].

É imediato que se S é um subespaço regular de um espaço quadrático (V, B) então

$$V = S \perp S^{\perp}$$

Se V = 0, a diagonalização é óbvia. Tomemos então $q \neq 0$. Podemos escolher e_1 em V tal que $q(e_1) \neq 0$ e considerarmos o espaço uni-dimensional $W = F.e_1$. Tal espaço é regular e assim

$$(V, B) \simeq (W, B/_W) \perp (W^{\perp}, B/_W)$$

Se a dimensão de $W^{\perp}$ for diferente de um, o processo se repete e a demonstração segue por indução sobre a dimensão de V.■

Usaremos

$$< a_1, \ldots a_n >$$

para representar

$$< a_1 > \perp < a_2 > \perp \ldots < a_n >$$

onde

$$< a_i > = a_i X_i^2$$

Podemos dizer então que todo espaço quadrático é gerado pelas classes de espaços uni-dimensionais.

Definição 12 - O determinante de uma forma quadrática regular f, também chamado discriminante de f, é definido como

$$\text{disc}\ (f) = \det\ (M_f).\dot{F}^2$$

Podemos observar que a definição dada é precisa, pois sabemos que a matriz associada a um espaço quadrático está bem definida a menos de uma semelhança, isto é, se $f \simeq g$ então

$$\text{disc}\ (f) = \det\ (M_f)\ \dot{F}^2 = \det\ (M_g)(\det\ C)^2\ \dot{F}^2 = \text{disc}\ (g)$$

pois

$$M_f = C^t\ M_g\ C$$

onde C é inversível

Vale ressaltar ainda que uma forma quadrática é regular se e somente se disc $(f) \neq 0$

Consideremos agora as matrizes M_1 e M_2 dos espaços quadráticos (V_1, B_1) e (V_2, B_2) em relação às bases $\{e_1, e_2, \ldots, e_n\}$ e $\{f_1, f_2, \ldots, f_m\}$ dos espaços V_1, V_2 respectivamente.

Se considerarmos os vetores $e_i + 0$ e $0 + f_i$ como elementos de $V = V_1 \perp V_2$, então $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ será uma base de (V, B) e sua matriz M será

$$M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$$

e temos então que

$$\text{disc}(V, q) = \text{disc}(q) = \text{disc}(V_1, B_1)\,\text{disc}(V_2, B_2) = \text{disc}(q_1)\,\text{disc}(q_2)$$

em $\dot{F}/\dot{F}^2$

Veremos, a seguir, um espaço quadrático que desempenha um papel relevante nesse trabalho.

Teorema 3 - Seja (V, B) um espaço quadrático 2 - dimensional. As seguintes afirmações são equivalentes.

i) V é regular e isotrópico

ii) V é regular e disc (V) = $-1\ \dot{F}^2$

iii) V é isométrico a < 1, -1 >

iv) V corresponde à classe de equivalência da forma quadrática $X_1\ X_2$.

Demonstração: iii) $\Longleftrightarrow$ iv) (ver exemplo 2)

i) $\Longrightarrow$ ii) Seja x um vetor isotrópico de V e $\{x, y\}$ uma base de V. Então $B(x, y) = a \neq 0$, pois caso contrário a matriz de B seria

$$\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}$$

que teria determinante nulo (absurdo, pois V é regular).

Trocando y por $a^{-1}y$, podemos assumir que $B(x, y) = 1$ e a matriz de B, na base $\{x, y\}$, fica

$$\begin{pmatrix} 0 & 1 \\ 1 & c \end{pmatrix}$$

Tomando a base $\{ x, -\frac{x}{2} + y \}$, temos $B(x, x) = 0$

$$B(-\frac{cx}{2}+y, -\frac{cx}{2}+y) = \frac{c}{4} B(x, x) - \frac{c}{2} B(x,y) - \frac{c}{2} B(x,y) + B(y,y) = 0 \quad e$$

$$B(x, -\frac{cx}{2} + y) = -\frac{c}{2} B(x, x) + B(x, y) = 1$$

Portanto, nessa base, a matriz de B é

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ e assim } \operatorname{disc}(V) = -1.\dot{F}^2$$

ii) $\Longrightarrow$ iii)

Sendo B a forma bilinear associada a V, sabemos que sua matriz para alguma base ortogonal $\{e_1, e_2\}$ é

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

Como discV = -1, vem que b = -a. Assim $V \simeq \langle a, -a \rangle$. Como $X^2-Y^2 \simeq XY$ e $aX^2 - aY^2$ representam um mesmo elemento, vem que $\langle a, -a \rangle \simeq \langle 1,-1 \rangle$.

Logo V é isométrico a $\langle 1, -1 \rangle$.

iii) $\Longrightarrow$ i) Se $V \simeq \langle 1, -1 \rangle$ então disc (V) $\neq 0$, V é regular e ainda 0 é representado por $q(X) = X_1^2 - X_2^2$ não trivialmente, isto é, V é isotrópico.

Observação 9 - Vemos então que existe uma única classe de isometria de espaços quadráticos isotrópicos de dimensão dois. Tal classe é denominada plano hiperbólico e indicado por H.

A soma ortogonal de planos hiperbólicos será chamado espaço hiperbólico e a este corresponderá a forma quadrática

$$X_1^2 - X_2^2 + \ldots + X_{2m-1}^2 - X_{2m}^2$$

Teorema 4 - Seja (V, B) um espaço quadrático regular, então:

i) Todo subespaço trivial, $U \subset V$, de dimensão não - nula r, está contido em um subespaço hiperbólico $T \subset V$ de dimensão 2r.

ii) V é isotrópico se e somente se contém um plano hiperbólico.

iii) Se V é isotrópico então V é universal.

Demonstração - Provaremos i) e depois que i) $\Rightarrow$ ii) $\Rightarrow$ iii). Vamos provar i) por indução sobre r.

Para r = 1 tomemos x isotrópico, U unidimensional com U = F.x.

Temos que dim V $\geq$ dim V - 1 = dim $U^{\perp}$. Sabemos que existe $y \in V - U^{\perp}$ e assim $y \in V$ e $B(y, x) \neq 0$.

Logo a matriz de B é

$$\begin{pmatrix} 0 & B(x, y) \\ B(x, y) & B(y, y) \end{pmatrix}$$

cujo determinante é $-1.F^2$.

Temos então que

$$F.x + F.y \simeq H$$

Agora tomando uma base $\{ x_1, x_2, \ldots, x_r \}$ em U, seja S o conjunto gerado por $x_2, \ldots, x_r$. Temos que $U^{\perp} \subseteq S^{\perp}$ e desde que V é regular segue-se que

$$\dim S^{\perp} = \dim V - \dim S > \dim V - \dim U = \dim U^{\perp}$$

Portanto, existe um vetor y_1 ortogonal a $x_2, \ldots, x_r$ mas não é ortogonal a x_1. Podemos ver que x_1, y_1 são linearmente independentes, pois x_1 é isotrópico. O subespaço $H_1 = F.x_1 + F.y_1$ tem determinante

$$\operatorname{disc}(H_1) = \begin{vmatrix} 0 & B(x_2, y_1) \\ B(x_2, y_1) & B(y_1, y_1) \end{vmatrix} . \dot{F}^2 = -1.\dot{F}^2$$

Assim $H_1 \simeq H$

Podemos escrever então $V = H_1 + V'$, onde $V' = H_1^{\perp}$ contêm $x_2, \ldots, x_r$. Desde que V é regular, a prova segue por indução.

i) $\Rightarrow$ (ii). Basta tomar $r = 1$ em (i)

ii) $\Rightarrow$ (iii). Óbvio, pois a forma quadrática correspondente a H é claramente universal.

Corolário 1 - (Primeiro Teorema da Representação). Seja q uma forma quadrática regular e $d \in \dot{F}$, então $d \in D(q)$ se e somente se $q \perp < -d >$ é isotrópica.

Demonstração

($\Rightarrow$) Seja $q(X) = a_1 X_1^2 + a_2 X_2^2 + \ldots + a_n X_n^2$ e $d \in D(q)$

então existe $(x_1, x_2, \ldots x_n) \in F^n$, não - nulo, com $a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2 = d$

Assim $a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2 + (-d)1^2 = 0$, isto é, $q \perp < -d >$ é isotrópica.

($\Leftarrow$) Vamos supor que $(x_1, x_2, \ldots, x_n, x_{n+1})$ seja um vetor isotrópico para $q \perp < -d >$, então

$$a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2 - dx_{n+1}^2 = 0$$

Se $x_{n+1} \neq 0$, vem que

$$d = a_1\left(\frac{x_1}{x_{n+1}}\right)^2 + a_2\left(\frac{x_2}{x_{n+1}}\right)^2 + \ldots a_n\left(\frac{x_n}{x_{n+1}}\right)^2 \in D(q)$$

Agora se $x_{n+1} = 0$, então $(x_1, x_2, \ldots, x_n) \neq 0$ já é um vetor isotrópico para q. Assim q é universal (Teorema 4) e $D(q) = \dot{F}$, donde, claramente, $d \in D(q)$. ■

Teorema 5 - Sejam $q = \langle a, b \rangle$ e $q' = \langle c, d \rangle$ formas binárias regulares. Então $q \simeq q'$ se e somente se $disc(q) = disc(q')$ e q e q' representam um elemento em comum $e \in F$.

Demonstração

($\Longrightarrow$) Evidente (observar comentário feito após a definição 12).

($\Longleftarrow$) Supondo que $disc(q) = disc(q')$ e $e \in D(q)$ tiramos pelo Teorema 1, que $q \simeq \langle e, e' \rangle$ para algum $e' \in \dot{F}$. Temos agora que $ab\dot{F}^2 = ee'\dot{F}^2$ e assim $q \simeq \langle e, abe \rangle$.

Do mesmo modo $q' \simeq \langle e, cde \rangle$. Mas como $ab\dot{F}^2 = cd\dot{F}^2$ concluimos que $q \simeq q'$. ■

Voltemos nossa atenção para a operação soma ortogonal anteriormente definida.

Lema 2 - A operação soma ortogonal é compatível com a relação de equivalência "ser isométrico a", isto é,

$$\text{se } \alpha_1 : (V_1, B_1, q_1) \longrightarrow (V_1', B_1', q_1')$$

$$e\ \alpha_2 : (V_2, B_2, q_2) \longrightarrow (V_2', B_2', q_2')$$

são isometrias, então

$$\alpha_1 \oplus \alpha_2\ (x_1 \oplus x_2) = \alpha_1\ (x_2) \oplus \alpha_2\ (x_2)$$

é uma isometria de $(V_1 \perp V_2, q_1 \perp q_2)$ em $(V_1' \perp V_2', q_1' \perp q_2')$

Demonstração: $(q_1' \perp q_2')[(\alpha_1 \oplus \alpha_2)(x_1 \oplus x_2)] =$

$$(q_1' \perp q_2')\ [\ \alpha_1\ (x_1) \oplus \alpha_2\ (x_2)] \ =$$

$$q_1'(\alpha_1(x_1)) + q_2'(\alpha_2(x_2)) = q_1(x_1) + q_2(x_2) = q_1 \perp q_2(x_1 \oplus x_2)\ \blacksquare$$

Lema 3 - A operação $\perp$ é comutativa e associativa, isto é,

$$q_1 \perp q_2 \simeq q_2 \perp q_1 \ \text{ e } \ (q_1 \perp q_2) \perp q_3 \simeq q_1 \perp (q_2 \perp q_3)$$

Para a verificação basta observarmos que as seguintes são isometrias.

$$\alpha : V_1 \perp V_2 \longrightarrow V_2 \perp V_1, \text{ com } \alpha(x_1 \oplus x_2) = x_2 \oplus x_1 \ \text{ e}$$

$$\beta : (V_1 \perp V_2) \perp V_3 \longrightarrow V_1 \perp (V_2 \perp V_3), \text{ com}$$

$$\beta[(x_1 \oplus x_2) \oplus x_3] = x_1 \oplus (x_2 \oplus x_3)$$

Pelos resultados anteriores, concluímos que o conjunto M(F) das classes de equivalência de espaços quadráticos regulares, junto com a operação induzida pela soma ortogonal, é um semi-grupo comutativo, onde como veremos mais ainda, vale a lei do cancelamento. O espaço (0, 0) é o elemento neutro de tal semi-grupo.

Apresentaremos a seguir os teoremas do Cancelamento e da Decomposição, que juntamente com o teorema da Diagonalização, desempenham importante papel em toda essa teoria. A demonstração, essencialmente técnica de cada um desses resultados, pode ser encontrada, de forma detalhada em [L].

Teorema 6 - (Do Cancelamento) Sejam q, q_1 e q_2 formas quadráticas quaisquer. Se $q \perp q_1 \simeq q \perp q_2$ então $q_1 \simeq q_2$.

Teorema 7 - (Da Decomposição). Qualquer espaço quadrático (V, B, q) pode ser decomposto numa soma ortogonal $(V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$, onde V_t é totalmente isotrópico, V_h é um subespaço hiperbólico e V_a é um subespaço anisotrópico. Tal decomposição é única a menos de uma isometria.

Voltando ao conjunto M(F) das classes de equivalência de formas quadráticas sobre um corpo F, definiremos sobre M(F) x M(F) uma operação (+), onde para quaisquer (f, g) e (f_1, g_1) de M x M, teremos $(f, g) + (f_1, g_1) = (f \perp f_1, g \perp g_1)$. Observemos

bem que aqui ($\perp$) denota a operação induzida pela soma ortogonal sobre as classes de equivalências de formas quadráticas.

Atentemos para o fato que $(M \times M, +)$ é um semi-grupo comutativo com cancelamento, onde $(0, 0)$ é o elemento neutro.

Dando continuidade, sobre $M \times M$ definimos a relação de equivalência $(f, g) \sim (f_1, g_1)$ se e só se $f \perp g_1 = g \perp f_1$.

Observação 10 - A operação acima definida é compatível com tal relação, isto é, se

$(f, g) \sim (f', g')$ e $(f_1, g_1) \sim (f_1', g_1')$ então

$(f, g) + (f_1, g_1) \sim (f', g') + (f_1', g_1')$

Isto decorre imediatamente, pois temos

$f \perp g' = g \perp f'$ e $f_1 \perp g_1' = g_1 \perp f_1'$ e assim

$f \perp g' \perp f_1 \perp g_1' = g \perp f' \perp g_1 \perp f_1'$

Agora, sobre $G(F) = M \times M/\sim$ definimos uma outra operação $\oplus$, com

$\alpha \oplus \alpha_1 = \overline{(f \perp f_1, g \perp g_1)}$, onde $(f, g) \in \alpha$ e $(f_1, g_1) \in \alpha_1$

Esta operação dá a $G(F)$ uma estrutura de grupo

comutativo, chamado grupo de Witt - Groethendieck, onde:

i) o elemento neutro é dado por $\alpha_0 = \overline{(q, q)}$, pois se $\alpha = \overline{(q_2, q_3)}$ é um elemento qualquer de G(F) então

$$\alpha \oplus \alpha_0 = \overline{(q_2, q_3)} \oplus \overline{(q, q)} = \overline{(q_2 \perp q, q_3 \perp q)} = \overline{(q_2, q_3)}$$

pelo simples fato de $(q_2 \perp q, q_3 \perp q) \sim (q_2, q_3)$

Colocaremos $\overline{(q, q)} = 0$

ii) para qualquer $\alpha \in G(F)$, $\alpha = \overline{(q_1, q_2)}$, a classe $\alpha' = \overline{(q_2, q_1)}$ é sua inversa. De fato,

$$\overline{(q_1, q_2)} \oplus \overline{(q_2, q_1)} = \overline{(q_1 \perp q_2, q_2 \perp q_1)} = \overline{(q, q)} = 0$$

iii) a operação é evidentemente comutativa e associativa.

Podemos observar ainda que a aplicação $i : M \to G(F)$ dada por $i(q) = \overline{(q, 0)}$ é um homomorfismo de semi-grupo, injetor, pois

i) $i(q \perp q_1) = \overline{(q \perp q_1, 0)} = \overline{(q, 0)} + \overline{(q_1, 0)} = i(q) \oplus i(q_1)$ e

ii) $\overline{(q, 0)} = \overline{(q_1, 0)}$ se e só se $q = q_1$

Sob esse aspecto, vemos que M(F) pode ser encarado como um subconjunto de G(F).

Podemos notar ainda que

$$\overline{(q, q_1)} = \overline{(q, 0)} \oplus \overline{(0, q_1)} = \overline{(q, 0)} - \overline{(q_1, 0)} = i(q) - i(q_1) = q - q_1$$

e assim dizemos que G(F) é gerado aditivamente por M(F).

A partir daqui trabalharemos com o intuito de dar a G(F) uma estrutura de anel comutativo.

Para tanto definiremos, primeiramente, o chamado produto de Kronecker de espaços quadráticos.

Definição 13 - Sejam (V_1, B_1) e (V_2, B_2) espaços quadráticos. Se fizermos

$$V = V_1 \otimes_F V_2 \quad e \quad B : V \times V \to F$$

dada por

$$B(u_1 \otimes u_2, v_1 \otimes v_2) = B_1(u_1, v_1) . B_2(u_2, v_2)$$

e estendermos por linearidade a $V_1 \otimes V_2$, pois qualquer

$$v \in V_1 \otimes V_2, \; v = \sum_{i=1}^{n} a_i \otimes b_i$$

com $a_i \in V_1$ e $b_i \in V_2$, então (V, B) ainda será um espaço quadrático.

A forma quadrática $q : V \to F$ associada, satisfaz $q(v_1 \otimes v_2) = q_1(v_1).q_2(v_2)$, onde q_1 e q_2 são as formas associadas

a B_1 e B_2 respectivamente. Denotaremos a por $q_1 \otimes q_2$.

A operação $\otimes$ é compatível com a relação de equivalência "ser isométrico a", isto é, se $q_1 \simeq q_1'$ e $q_2 \simeq q_2'$, então

$$q_1 \otimes q_2 \simeq q_1' \otimes q_2'$$

Demonstração: Simples verificação.

Em M(F), o produto de Kronecker induz uma operação associativa, comutativa e distributiva em relação à soma ortogonal. A prova desses fatos é imediata, uma vez que o produto tensorial goza dessas propriedades.

Observemos que se

$$q = \langle a_1, a_2, \ldots, a_n \rangle \quad e$$

$$q_1 = \langle b_1, b_2, \ldots, b_n \rangle$$

são duas formas diagonalizadas, então

$$q \otimes q_1 = \langle a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_n \rangle$$

Lema 4 - Se q é uma forma quadrática regular então $q \otimes H = \dim q.H$

Demonstração: Suponhamos que $q \simeq \langle a \rangle$, $a \neq 0$. Então

$$\langle a \rangle \otimes H = \langle a \rangle \otimes \langle 1, -1 \rangle \simeq \langle a, -a \rangle \simeq H$$

pelo teor 3.

Agora a prova segue por indução sobre a dimensão de q (dim q).

Até aqui mostramos que (M, +, ⊗) é um semi-anel comutativo com elemento neutro e com identidade < 1 >.

Finalmente, sobre M(F) x M(F)/~ definimos a operação (·), onde

$$\overline{(q, q_1)} \cdot \overline{(q', q_1')} = \overline{(q \otimes q' + q_1 \otimes q_1', q \otimes q_1' + q_1 \otimes q')}$$

e assim (G(F), +, ·) é o anel denominado anel de Witt - Groethendieck, denotado por $\hat{W}$ (F).

Em $\hat{W}(F)$ podemos observar que

i) todo elemento tem a forma $q_1 - q_2$, onde q_1 e q_2 são classes de isometrias das formas q_1 e q_2 e, como já foi observado, $M(F) \subset \hat{W}(F)$, assim $(q_1) = (q_2)$ em $\hat{W}(F)$ se e somente se $q_1 \simeq q_2$.

ii) $\hat{W}(F)$ goza da chamada "propriedade universal", isto é, qualquer homomorfismo de semi-grupo f, de M(F) em um grupo abeliano A, estende-se a um único homomorfismo de grupo $g : \hat{W}(F) \to A$, pela regra $g(q_1 - q_2) = f(q_1) - f(q_2)$. Isso pode ser visualizado mais facilmente com a ajuda do diagrama abaixo.

$$\begin{array}{ccc} M(F) & \xrightarrow{\ i\ } & G(F) = \hat{W}(F) \\ & \searrow^{f} & \downarrow g \\ & & A \end{array}$$

onde i é a inclusão $M(F) \subset G(F)$

Daremos, a seguir, o anel que será alvo de todo nosso trabalho.

Como foi visto no Lema 4, ZH é um ideal de $\widehat{W}(F)$ e assim

$$W(F) = \widehat{W}(F)/ZH$$

é o denominado **Anel de Witt do Corpo F.**

Proposição 1 - Os elementos de W(F) estão em correspondência biunívoca com as classes de isometrias de todas as formas anisotrópicas sobre F.

Demonstração: Vimos que se $< \overline{q, q_1} > \in G(F)$ então $\overline{(q, q_1)} = q - q_1$, isto é, G(F) é gerado aditivamente por M(F).

Sabemos $< a > + < -a >$ representa o zero em W(F), assim $-(< a >) = (< -a >)$ em W(F), para todo $a \in F$. E em particular podemos dizer que todo elemento de W(F) é representado por uma forma q.

Usando o teorema da Decomposição de Witt, podemos escrever $q = q_h + q_a$ e como $q_h = 0$ em W(F), q e q_a representam o mesmo elemento em W(F).

Vejamos agora a unicidade.

Se q e q' são formas anisotrópicas, então (q) = (q') em W(F), implica $q \simeq q'$, pois se (q) = (q'), vem que $q = q' + m\,H$ em $\widehat{W}(F)$, para algum inteiro m, que podemos supor positivo ou nulo.

Logo $q \simeq q' \perp m\,H$, o que nos leva a concluir que $m' = 0$, pois q é anisotrópico. Assim $q \simeq q'$.■

A proposição acima ocupa um lugar de fundamental importância, pois a partir dela, poderemos encarar $W(F)$ como formado por classes de equivalência de formas anisotrópicas.

Observação 11 - Ouando não houver perigo de confusão, representaremos a classe de q, que de fato pertence a $W(F)$, simplesmente por q.

Antes de prosseguirmos, faremos mais alguns comentários sobre $\widehat{W}(F)$ e $W(F)$.

Observação 12 - Consideremos a função "dimensão", $\dim M(F) \longrightarrow Z$, que é um homomorfismo de semi-grupo. Pela propriedade universal de $\widehat{W}(F)$, tal homomorfismo se estende a um único homomorfismo de grupo $\dim \widehat{W}(F) \longrightarrow Z$, com $\dim (q_1 - q_2) = \dim (q_1) - \dim (q_2)$, que também é um homomorfismo de anel.

O núcleo $\widehat{IF}$ de tal homomorfismo é um ideal de $\widehat{W}(F)$, consistindo das formas $q_1 - q_2$, onde $\dim q_1 = \dim q_2$ e ainda $\widehat{W}(F)/\widehat{IF} \simeq Z$, pois dim é sobrejetor.

Observação 13 - Tomemos o homomorfismo canônico $\phi : \widehat{W}(F) \longrightarrow W(F)$. O ideal $IF = \phi(\widehat{IF})$, de $W(F)$, é tal que $\widehat{IF} \simeq IF$ e uma forma q representa um elemento em IF se e somente se dim q for par.

Demonstração: Mostremos que $\widehat{IF} \simeq IF$

Temos que

$$\widehat{IF} = \{ q_1 - q_2, \text{ com } \dim q_1 = \dim q_2 \}$$

$$ZH = \{ nH, \ n \in Z \}$$

Podemos ver que $\widehat{IF} \cap ZH = \{0\}$, pois se $q_1 - q_2 \in nH$, vem que

$$q_1 - q_2 = \begin{cases} nH - 0, \text{ se } n \geq 0 \\ 0 - (-nH), \text{ se } n < 0 \end{cases}$$

Assim, teremos

$$q_1 \perp 0 = nH \perp q_2 \quad \text{ou} \quad q_1 \perp (-nH) = 0 \perp q_2$$

Aplicando a função dim, tem-se

$$\dim q_1 = 2n + \dim q_2 \quad \text{ou} \quad \dim q_1 - 2n = \dim q_2$$

Como $\dim q_1 = \dim q_2$, obtemos em qualquer caso, $n = 0$.
Agora $IF = \phi(\widehat{IF}) = \widehat{IF}$, pois

$$\phi(\widehat{IF}) = \frac{ZH + \widehat{IF}}{ZH} = \frac{\widehat{IF}}{ZH \cap \widehat{IF}} = \frac{\widehat{IF}}{\{0\}} = \widehat{IF}$$

Para tanto basta definirmos o homomorfismo sobrejetor

$$\theta : \widehat{IF} + ZH \longrightarrow \frac{\widehat{IF}}{ZH \cap \widehat{IF}},$$

onde $\theta(a + ZH) = a + (ZH \cap \widehat{IF})$ e notarmos que $\ker \theta = ZH$.

Veremos agora a segunda afirmação.

($\Longrightarrow$) Tomemos $\overline{q_1 - q_2} = \bar{q}$, q anisotrópica e $q_1 - q_2 \in \widehat{IF}$

Temos que

$$q_1 = rH \perp < a_1, a_2, \ldots, a_n >$$

$$q_2 = sH \perp < b_1, b_2, \ldots, b_n >$$

com

$$n + 2r = m + 2s$$

Assim

$$\overline{q_1 - q_2} = \bar{q}_1 - \bar{q}_2 = < \overline{a_1, a_2, \ldots, a_n} > - < \overline{b_1, b_2, \ldots, b_n} > =$$

$$= < \overline{a_1, a_2, \ldots, a_n, b_1, \ldots, b_m} > = \overline{\ell H + < c_1, c_2, \ldots, c_t >} =$$

$$= < \overline{c_1, c_2, \ldots, c_t} >$$

Como $n + m = 2m + 2s - 2r$, vem que $n + m$ é par, e desde que $2\ell + t = n + m$, vem que t é par.

Concluímos assim que uma forma q representa um elemento de IF somente se dim q é par.

($\Leftarrow$) Supondo que dim q é par, podemos assumir que q é binária, $q = \langle a, b \rangle$. Observamos então que q é a imagem de $\langle a \rangle \perp \langle b \rangle$ pela projeção natural $\phi: \hat{W}(F) \longrightarrow W(F)$. Logo $q \in IF$. ■

Atentemos também para o fato do epimorfismo

$$\dim : \hat{W}(F) \longrightarrow Z$$

induzir outro epimorfismo, bem definido

$$\dim_0 : W(F) \longrightarrow Z/2Z$$

onde

$$\dim_0 (\overline{q_1 - q_2}) = \dim (q_1 - q_2) + 2Z = (\dim q_1 - \dim q_2) + 2Z$$

Para verificarmos a boa definição basta notarmos que se

$$\overline{q_1 - q_2} = \overline{q_3 - q_4}$$

então

$$q_1 - q_2 = (q_3 - q_4) + nH$$

onde nH é tomado como nH - 0 quando $n > 0$ e como 0 - (-nH), caso contrário.

Para $n > 0$, vem que $q_1 \perp q_4 \simeq q_2 \perp q_3 + nH$ e assim

$$\dim q_1 + \dim q_4 = \dim q_2 + \dim q_3 + 2n$$

Logo

$$\dim q_1 - \dim q_2 = (\dim q_3 - \dim q_4) + 2n$$

ou ainda,

$$(\dim q_1 - \dim q_2) + 2Z = (\dim q_3 - \dim q_4) + 2Z$$

Tem-se ainda que $\ker \dim_0 = IF$ e logo

$$\frac{W(F)}{IF} \simeq \frac{Z}{2Z}$$

Salientamos, desde já a importância do ideal IF.

Passamos a caracterizar W(F) através de certas relações entre seus geradores e veremos que tais relações realmente determinam o anel de Witt.

Consideremos a função

$$< > : F \to W(F)$$
$$a \mapsto (< a >)$$

Teorema 8: A função definida acima satisfaz

i) $\langle 0 \rangle = 0$ (elemento neutro)

ii) $\langle 1 \rangle = 1$ (elemento identidade)

iii) $\langle a \rangle . \langle b \rangle = \langle ab \rangle$

iv) $\langle a \rangle + \langle b \rangle = \langle a + b \rangle (1 + \langle ab \rangle)$

e além disso verificamos que estas relações determinam o anel de Witt, ou seja, se R é um anel comutativo qualquer e $t: F \to R$ é uma função satisfazendo os ítens i - iv acima, então existe um único homomorfismo de anel $\theta : W(F) \to R$ tal que $\theta (\langle a \rangle) = t(a)$.

Demonstração: Usando a definição de soma e produto no anel de Witt e o fato de $\langle 0 \rangle$ ser a forma quadrática de zero variáveis, vemos que i) e ii) são imediatas.

iii) também é imediata, visto que como

$$\langle a \rangle = a X_1^2 \quad e \quad \langle b \rangle = b X_1^2 \quad \text{então}$$

$$\langle a \rangle . \langle b \rangle = ab X_1^2 = \langle ab \rangle$$

Mostremos o ítem iv) separando em partes.

1 - Consideremos a = 0 (ou b = 0). Então

$$< a > + < b > = < b >(1 + < 0 >)$$

2 - Tomemos a + b = 0

Já vimos que $- < 1 > = < -1 >$ em W(F) e como a = -b, teremos

$$< a > + < b > = < a > + < -a > = 0$$

$$< a + b > (1 + < ab >)$$

3 - Sejam $a + b \neq 0$, $f(X) = aX_1^2 + bX_2^2$ e

$$g(X) = (a + b)\, X_1^2 + (a^2b + ab^2)X_2^2$$

Observamos que a matriz

$$\begin{pmatrix} 1 & b \\ 1 & -a \end{pmatrix}$$

é inversível e que para todo x_1, x_2 em F, temos

$$f(x_1 + bx_2,\ x_1 - ax_2) = a(x_1 + bx_2)^2 + b(x_1 - ax_2)^2$$

$$= ax_1^2 + 2abx_1x_2 + ab^2x_2^2 + bx_1^2 - 2abx_1x_2 + a^2bx_2^2$$

$$= (a + b)\, x_1^2 + (a^2b + ab^2)\, x_2^2$$

Logo $f = g$ e podemos concluir que

$$< a > + < b > = < a + b > + < a^2b + ab^2 >$$

$$= < a + b > + < a + b > < ab >$$

$$= < a + b > (1 + < ab >)$$

Assim, por 1-, 2-, 3-, vemos que iv) se verifica

Passamos a demonstrar a parte final do teorema.

Para tanto sejam R um anel comutativo, e $t : F \to R$ uma função satisfazendo as relações i - iv.

Mostremos que existe um homomorfismo de anel $\theta : W(F) \to R$ com $\theta(< a >) = t(a)$, para todo $a \in F$.

Temos que $t(-1) + t(1) = t(0)[1 + t(-1)] = 0$ e assim $t(-1) = -t(1) = -1$.

Supondo $a \neq 0$, vemos que

$$t(a)[t(1+1)(1+t(1)] = t(a)[t(1) + t(1)] = t(a) + t(a)$$

$$= t(a+a)(1+t(a^2) = t(2a)(1+t(a^2) = t(a)\,t(2)(1+t(a^2))$$

Assim

$$t(a).t(2)(1+1) = t(a).t(2)(1+t(a^2)),$$

donde

$$t(a).t(2) + t(a).t(2) = t(a).t(2) + t(a).t(2).t(a^2)$$

e portanto

$$t(a).t(2) = t(a).t(2).t(a^2)$$

Multiplicando ambos os lados da última igualdade por $t(a^{-1}).t(2^{-1})$, concluímos que

$$1 = t(a^2) = t(a).t(a) = t(a)^2 \qquad (I)$$

Vejamos agora que se a_1, a_2, b_1, b_2 são elementos não nulos de F e que se $f(x) = a_1X_1^2 + a_2X_2^2$ é equivalente a

$$g(X) = b_1X_1^2 + b_2X_2^2$$

então

$$t(a_1) + t(a_2) = t(b_1) + t(b_2) \qquad (II)$$

De fato:

Se f ≈ g então deve existir uma matriz inversível $[(c_{ij})]$ com $f(c_{11}\,x_1 + c_{12}\,x_2,\ c_{21}\,x_1 + c_{22}\,x_2) = g\,(x_1, x_2)$, pa

ra todo x_1, x_2 em F. Daqui vem que

$$\begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix} = [(c_{ij})]^t \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} [(c_{ij})] \qquad (1)$$

Se fizermos $\det([(c_{ij})]) = k$, vem

$$b_1 b_2 = k a_1 a_2 k$$

Tomando $x_1 = 1$ e $x_2 = 0$, obtemos

$$f(c_{11}, c_{21}) = g(1, 0)$$

ou seja

$$a_1 c_{11}^2 + a_2 c_{21}^2 = b_1 \qquad (2)$$

Observando que se tomarmos $c_{11} = 0$, teremos $c_{21} \neq 0$, com $a_2 c_{21}^2 = b_1$ o que nos leva a $t(a_2 c_{21}^2) = t(b_1)$. Mas

$$t(a_2 c_{21}^2) = t(a_2)\, t(c_{21})^2 = t(a_2)$$

Assim $t(a_2) = t(b_1)$.

Vemos ainda que

$$t(b_2) = t(b_2\, b_1^2) = t(b_2 b_1 b_1) = t(b_2 b_1)\ t(b_1)$$

$$= t(k a_1 a_2 k)\ t(b_1) = t(k)^2 t(a_1)\ t(a_2)\ t(b_1) = t(a_1)$$

pois como foi visto $b_1 b_2 = k a_1 a_2 k$, $t(k)^2 = 1$ e $t(b_1) = t(a_2)$

Concluimos então que $t(b_1) + t(b_2) = t(a_1) + t(a_2)$

De maneira análoga, se $c_{21} = 0$ então $c_{11} \neq 0$ e teremos $t(a_1) + t(a_2) = t(b_1) + t(b_2)$.

Tomando $c_{11} \neq 0$ e $c_{21} \neq 0$, vem

$$t(a_1) + t(a_2) = t(a_1 c_{11}^2) + t(a_2 c_{21}^2) - t(b_2) + t(b_2)$$

$$= t(a_1 c_{11}^2 + a_2 c_{21}^2)\,[1 + t(a_1 a_2 c_{11}^2 c_{21}^2)] - t(b_2 b_1^2) + t(b_2)$$

$$= t(b_1)[1 + t(a_1 a_2)] - t(b_1 a_1 a_2 k^2) + t(b_2)$$

$$= t(b_1) + t(b_1 a_1 a_2) - t(b_1 a_1 a_2) + t(b_2) = t(b_1) + t(b_2)$$

por (1) e (2).

Concluimos assim a demonstração de (II).

Para chegarmos "a boa definição" de homomorfismo $\theta : W(F) \longrightarrow R$, usaremos um lema técnico sem demonstrá-lo, mas o

leitor pode encontrar sua prova detalhada em [L].

Lema 5: "Sejam f e g formas quadráticas regulares dadas por matrizes em formas diagonais e supunhamos que f ≃ g. Então existe uma sequência $h_1, h_2, \ldots, h_m$ de formas quadráticas regulares, cujas matrizes também estão em formas diagonais, tais que $f = h_1$, $g = h_m$ e com h_i diferindo de h_{i+1} no máximo em dois coeficientes e ainda com $h_i \simeq h_i + 1$, para todo i".

Consideremos uma classe $\alpha \in W(F)$. Pelo teorema da diagonalização, existe uma forma quadrática

$$f(X) = a_1X_1^2 + a_2X_2^2 + \ldots + a_nX_n^2$$

com $f \in \alpha$, onde $0 \neq a_i \in F$, para todo i, pois f é anisotrópica.

Colocamos então

$$\theta(\alpha) = t(a_1) + t(a_2) + \ldots + t(a_n)$$

Mostremos que θ independe da escolha do representante em α.

Seja $g \in \alpha$. Então $g \simeq f$ e pelo lema acima existe uma sequência de formas quadráticas $h_1, h_2, \ldots, h_m$, com as propriedades citadas e que nos permite escrever $h_i \simeq r + h$, $h_{i+1} \simeq s + h$ com r e s formas binárias. Pelo teorema de cancelamento temos $r \simeq s$. Como h tem os mesmos coeficientes de f e pelo provado em (II), vem

$$\theta_f(\alpha) = \theta_{h_1}(\alpha) = \ldots = \theta_{hm}(\alpha) = \theta_g(\alpha)$$

donde concluimos a independência.

Conseguimos então uma função $\theta: W(F) \rightarrow R$ dada por $\theta(< a >) = t(a)$ para todo a em F, $a \neq 0$.

Se $a \neq 0$ e $b \neq 0$ estão em F, então

$$\theta(<a>), \theta(<b>) = t(a)\ t(b) = t(ab) = \theta(<ab>) = \theta(<a>\ <b>)$$

Todo elemento em W(F) pode ser escrito na forma

$$<a_1> + <a_2> + \ldots <a_n> \qquad \text{com } a_i \neq 0$$

Assim

$$\theta(<a_1> + \ldots + <a_n>) = t(a_1) + \ldots + t(a_n) = \theta(<a_1>) + \theta(<a_2>) + \ldots + \theta(<a_n>)$$

Pelo exposto acima, chegamos que θ é um homomorfismo de anel.

Veremos, a seguir, que tal homomorfismo é único.

Com esse fim, suponhamos que exista $\phi: W(F) \rightarrow R$ com $\phi(< a >) = t(a)$.

W(F) é gerado por elementos da forma $< a >$ e como $\phi(< a >) = t(a) = \theta(< a >)$, podemos dizer que $\phi = \theta$. Terminamos aqui a demonstração do teorema.

Observação 14 - Um resultado análogo ao teorema - 8 pode ser dado considerando-se a estrutura de grupos e as relações

i) $< 0 > = 0$

ii) $< a > + < b > = < a + b > (1 + < ab >)$

iii) $< a > + < -a > = 0$

Saliente-se que iii) é consequência direta de i) e ii) e que tal caracterização será usada mais adiante.

CAPÍTULO II

CORPOS FORMALMENTE REAIS

Parte 1

Estudaremos a seguir um dos aspectos mais interessantes do Anel de Witt, a estreita relação entre os ideais primos não-maximais e as ordens de F. Na verdade existe uma correspondência biunívoca entre eles. Este fato é de grande utilidade, pois conhecendo-se a estrutura de ordem de um corpo F, podemos tirar conclusões sobre os ideais de W(F) e do próprio W(F).

O cálculo do Anel de Witt de um corpo nem sempre é fácil, mas conhecendo-se suas ordens, sempre podemos obter algumas informações.

Relembremos alguns fatos sobre ordem em um corpo.

Seja P um subconjunto de um corpo F, gozando das seguintes propriedades:

O - 1: Dado x em F, temos que ou $x \in P$, ou $x = 0$, ou $-x \in P$, isto é, F é a união disjunta de P, $\{0\}$ e $-P$

O - 2: Se x e y estão em P então $x + y \in P$ e $xy \in P$.

O subconjunto P é denominado cone positivo de F.

Podemos definir, sobre F, uma ordem colocando:

$$\forall x, \forall y,\ x, y \in F,\ x < y$$

se e somente se $y - x \in P$. Afirmamos que, para todo x, y e z em F, as seguintes propriedades são de verificação imediata.

1 - se $x < y$ e $y < z$ então $x < z$

2 - Tricotomia. Apenas uma das afirmações a seguir é verdadeira: $x < y$, $x = y$ ou $y < x$.

3 - se $x < y$ e $0 < z$, então $xz < yz$

4 - se $x < y$, então $x + z < y + z$

Vemos então que $<$ é uma relação de ordem e diremos que F é ordenável por P.

Se $x \notin P$, então $x \in -P$ e $x < 0$. Diremos que x é negativo e -P passa a ser denominado o conjunto dos números negativos em F. Usaremos também $x > y$ quando $x - y \in P$.

Podemos observar que se F é ordenado por $<$, então, em F, o conjunto $P = \{ x \in F,\ x > 0 \}$ tem as propriedades exigidas para um cone positivo. Assim existe uma bijeção entre ordens de F e os cones positivos de F.

Mais adiante veremos que se -1 não for soma de quadrados em F (F formalmente real) então este será ordenável.

Observação 1: Se assumirmos F ordenável por P, então com $1 \neq 0$, teremos $1 \in P$, pois caso contrário $-1 \in P$ e $1 = (-1)(-1) \in P$, absurdo. Por 0 - 2 vem que $1 + 1 + \ldots + 1 \in P$ e assim F terá característica zero (car F = 0).

Voltando a W(F), veremos alguns resultados que nos auxiliarão na classificação dos ideais primos de W(F).

Definição 1: O conjunto dos ideais primos de W(F) é chamado espectro e indicado por Espec (W(F))

Observemos primeiramente que se $Y \in$ Espec (W(F)) então, para todo $0 \neq a \in F$, vem que $< a > \in \pm 1 + Y$, pois sabendo que $(<a>)^2 = 1$, teremos $(< a > - 1)(< a > + 1) = 0 \in Y$. Logo, como Y é primo, $< a > + 1 \in Y$ ou $< a > - 1 \in Y$.

Proposição 1: Se $Y \in$ Espec (W(F)) então $W(F)/Y \simeq Z$ ou $W(F)/Y \simeq F_p$

Demonstração: Seja q em W(F), $q \simeq <a_1, a_2, \ldots, a_n> = <a_1> + <a_2> + \ldots + <a_n>$

Para cada i, $<a_i> \in (-1)^{\varepsilon i} + Y$, onde ε_i é 0 ou 1. Assim

$$q + Y = \sum_{i=1}^{n} ((-1)^{\varepsilon i} + Y) = m < 1 > + Y, \text{ m inteiro.}$$

Vemos então que W(F)/Y é cíclico gerado por $< 1 > + Y$ e portanto $W(F)/Y \simeq Z$ ou $W(F)/Y \simeq Z/nZ$. Como Y é primo, W(F)/Y é um anel de integridade. Logo n = p e temos $W(F)/Y \simeq Z$ ou $W(F)/Y \simeq F_p$.

Até o presente momento, o único ideal do espectro de W(F) conhecido é IF, o ideal das formas pares, apresentado na página 31, observação 13.

Agora daremos outra caracterização do ideal IF.

Teorema 1

i) IF é o único ideal máximal de W(F) contendo $2 = \langle 1 \rangle + \langle 1 \rangle$

ii) se Y é ideal primo não - maximal de W(F) então $Y \subset IF$

Demonstração:

i) Vamos supor que M_0 é outro ideal com $2 \in M_0$.

Então $K = W(F)/M_0$ é um corpo, com car(K) = 2, pois 2 = 0 em K. Assim

$$\frac{W(F)}{M_0} \simeq \frac{Z}{2Z} = F_2$$

Para qualquer $u = \langle a_1 \rangle + \langle a_2 \rangle + \ldots + \langle a_n \rangle$ em W(F), com $a_i \neq 0$, para todo i, temos

$\theta(\langle a_i \rangle)^2 = 1 = 1^2$, θ é o isomorfismo acima.

Logo

$$[\theta(< a_i >) - 1]^2 = 0$$

e portanto $\theta(< a_i >) = 1 \in F_2$

Vemos então que

$$\theta(u) = \begin{cases} 0, \text{ se } n \text{ é par} \\ 1, \text{ se } n \text{ é impar} \end{cases}$$

e teremos $u \in M_0 = \theta^{-1}(0)$ se e somente se n é par, isto é, $M_0 = IF$.

Para verificarmos ii), tomemos um ideal primo não-maximal Y, de W(F).

Temos então que $W(F)/Y \simeq Z$. De um modo geral, ao tomarmos o ideal pZ de Z, teremos que $\theta^{-1}(pZ)$ é um ideal maximal de W(F) contendo Y, onde θ é a projeção $\theta : W(F) \longrightarrow W(F)/Y \simeq Z$. Ao considerarmos o ideal 2Z de Z, teremos $\theta^{-1}(2Z)$ maximal em W(F) contendo 2, isto é, $\theta^{-1}(2Z) = IF$ e assim ii) segue.

Tendo em mente estudos de resultados que nos permitam ter uma visão mais abrangente do Anel de Witt de um corpo, através da intrínseca relação entre os homomorfismos de anel de W(F) em Z, os ideais primos de W(F) e as ordens de F, formalizaremos o conceito de "função assinatura", que já apareceu no teorema 8, capítulo I.

Definição 2: Sejam F um corpo e R um anel comutativo. Uma função $s : F \to R$ satisfazendo as condições abaixo é chamada assinatura.

i) $s(0) = 0$

ii) $s(1) = 1$

iii) $s(ab) = s(a)\, s(b)$

iv) $s(a) + s(b) = s(a + b)(1 + s(ab))$

Teorema 2 - Seja $I \subsetneq W(F)$ um ideal. As seguintes afirmações são equivalentes.

(1) I é um ideal primo não-maximal de W(F)

(2) Existe um único cone positivo P de F tal que $a \in P$ se e só se $< a > -1 \in I$.

(3) Existe uma única função assinatura $t : F \to Z$ tal que $t(a) = 1$ se e só se $< a > - 1 \in I$.

(4) Existe um único homomorfismo $\theta : W(F) \to Z$ com $\ker(\theta) = I$

Em particular a cada cone positivo de F corresponde um unico ideal I primo não - maximal de W(F).

Demonstração: (1) $\Rightarrow$ (2)

Definamos $a <_I b \iff < b - a > - 1 \in I$ e verifiquemos

que $<_I$ é uma relação de ordem.

i) se $a <_I b$ e $b <_I c$ então $\langle b-a\rangle - 1 \in I$ e $\langle c-b\rangle - 1 \in I$

Assim

$$(\langle b-a\rangle-1)(\langle c-b\rangle-1)=\langle b-a\rangle\langle c-b\rangle-\langle b-a\rangle-\langle c-b\rangle+1=\langle b-a\rangle\langle c-b\rangle-\langle b-a\rangle-\langle c-b\rangle+2-1$$

$$= (\langle b-a\rangle\langle c-b\rangle-1)-\langle b-a\rangle+1-\langle c-b\rangle+1 \in I$$

Como $-\langle b-a\rangle+1$ e $-\langle c-b\rangle+1$ pertencem a I, temos que

$$\langle b-a\rangle\langle c-b\rangle - 1 \in I \qquad (A)$$

Queremos mostrar que

$$\langle c-a\rangle - 1 \in I$$

Temos que

$$\langle b-a\rangle - 1 + \langle c-b\rangle - 1 \in I$$

Daqui

$$\langle b-a\rangle-1+\langle c-b\rangle-1=\langle b-a+c-b\rangle(1+\langle b-a\rangle\langle c-b\rangle)-1-1=\langle c-a\rangle-1+\langle c-a\rangle\langle b-a\rangle\langle c-b\rangle - 1$$

$= \langle c-a\rangle -1+\langle c-a\rangle\langle b-a\rangle\langle c-b\rangle+\langle c-a\rangle-\langle c-a\rangle -1$

$= \langle c-a\rangle -1+\langle c-a\rangle(\langle b-a\rangle\langle c-b\rangle -1)+\langle c-a\rangle -1$

$= 2(\langle c-a\rangle -1)+\langle c-a\rangle(\langle b-a\rangle\langle c-b\rangle -1) \in I$

Por (A), vem que $2(\langle c-a\rangle -1) \in I$ e desde que $2 \notin I$, pela proposição - 1, temos que $\langle c-a\rangle -1 \in I$, isto é, $a <_I c$.

ii) tricotomia

Já vimos que se $b - a \neq 0$ então $\langle b-a\rangle \in \pm 1 + I$

Então:

se $\langle b-a\rangle \in 1 + I$, vem que $\langle b-a\rangle - 1 \in I$, ou seja, $a < b$

se $\langle b-a\rangle \in -1 + I$, vem que $\langle b-a\rangle + 1 \in I$

ou - $\langle b-a\rangle -1 \in I$, ou ainda, $\langle a-b\rangle -1 \in I$ e assim $b < a$

se $b-a = 0$, trivialmente tem-se $a=b$

iii) se $a <_I b$ e $0 <_I c$ então $\langle b-a\rangle - 1 \in I$, $\langle c\rangle - 1 \in I$ e

$\langle bc-ac\rangle - 1 = \langle c\rangle\langle b-a\rangle - 1 + \langle c\rangle - \langle c\rangle$

$= \langle c\rangle (\langle b-a\rangle - 1) + \langle c\rangle - 1 \in I$ e portanto $ac < bc$

iiii) se $a <_I b$ então $\langle b-a\rangle - 1 \in I$ e de

$$\langle b-a\rangle - 1 = \langle b+c-a-c\rangle - 1 = \langle b+c-(a+c)\rangle - 1,$$

vem que $a + c < b + c$.

(2) $\Rightarrow$ (3). Definamos $t : F \to Z$ colocando

$$t(a) = \begin{cases} 0, \text{ se } a = 0 \\ 1, \text{ se } a \in P \\ -1, \text{ se } a \notin P \end{cases}$$

Verifiquemos que t satisfaz as exigências da função assinatura.

i) segue pela definição de t

ii) $t(1) = 1$, pois $1 \in P$

iii) - se $a = 0$ ou $b = 0$ então $t(ab) = t(a)\ t(b)$
- se $a \in P$ e $b \in P$ então $ab \in P$ e $t(ab) = 1 = t(a)t(b)$
- se $a \notin P$ e $b \notin P$ então $ab \in P$ e $t(ab) = 1 = -1.-1 = t(a)t(b)$
- se $a \notin P$ e $b \in P$ então $ab \notin P$ e $t(ab) = -1 = -1.1 = t(a)t(b)$

iv) - se $a = 0$ ou $b = 0$ então $t(a) + t(b) = t(a+b)(1 + t(ab))$

- se $a \in P$ e $b \in P$ então $t(a) = 1$, $t(b) = 1$, $t(a+b) = 1$, $t(ab)=1$ e $2 = t(a) + t(b) = 1(1 + 1) = t(a+b)(1+t(ab))$

- se $a \notin P$ e $b \notin P$ então $t(a)=-1$, $t(b)=-1$, $t(a+b)=-1$, $t(ab)=1$ e $-2 = t(a) + t(b) = -1(1 + 1) = t(a+b)(1 + t(ab))$

- se $a \notin P$ e $b \in P$ então $t(a)=-1$, $t(b)=1$, $t(ab)=-1$ e $t(a) + t(b) = 0 = t(a+b)(1+-1) = t(a+b)(1+t(ab))$

(3) $\Rightarrow$ (4)

Pelo teorema 8, capítulo I, existe um único homomorfismo $\theta : W(F) \to Z$ com $\theta(\langle a \rangle) = t(a)$ para todo $a \in F$.

De $\theta(1) = 1$, vem que θ é sobrejetor e o núcleo N, de θ, é um ideal primo não-maximal de W(F).

Como (1) $\Rightarrow$ (2) $\Rightarrow$ (3), existe única $t' : F \to Z$ tal que

$$t'(a) = 1 \iff \langle a \rangle - 1 \in N$$

Temos então que

$$t'(a) = 1 \iff \theta(\langle a \rangle) = 1 \iff t(a) = 1$$

e portanto

$$t' = t \quad e \quad \langle a \rangle - 1 \in N \iff \langle a \rangle - 1 \in I$$

Agora como $t(a^2) = 1$, vem que $t(a) = \pm 1$ e assim se $t(a) = 1$ temos $\langle a \rangle - 1 \in I \Longleftrightarrow \langle a \rangle - 1 \in N$ e se $t(a) = -1$ então $(-1)\, t(a) = 1$ ou $t(-a) = 1$. Logo $\langle -a \rangle - 1 \in I$ e portanto $\langle a \rangle + 1 \in I$. Concluímos então que $\langle a \rangle + 1 \in N \Longleftrightarrow \langle a \rangle + 1 \in I$.

Mostremos que $N \subset I$.

Seja $q = \langle a_1, a_2, \ldots, a_n \rangle \in N$, com $a_i \neq 0, \forall i$.

Observemos que a dimensão de q é par, pois $N \subset IF$.

Colocando

$$a_i = \begin{cases} b_i \text{ se } \langle a_i \rangle - 1 \in N \\ \\ c_i \text{ se } \langle a_i \rangle + 1 \in N \end{cases}$$

e reagrupando, podemos escrever

$$\langle a_1, a_2, \ldots, a_n \rangle = \langle b_1, b_2, \ldots, b_{n/2} \rangle + \langle c_1, \ldots, c_{n/2} \rangle$$

$$= \sum_{i=1}^{n/2} \langle b_i \rangle + \sum_{i=1}^{n/2} \langle c_i \rangle = \sum_{i=1}^{n/2} (\langle b_i \rangle - 1) + \sum_{i=1}^{n/2} (\langle c_i \rangle + 1)$$

com $\langle b_i \rangle - 1 \in N$ e $\langle c_i \rangle + 1 \in N$, ou seja, $\langle b_i \rangle - 1 \in I$ e $\langle c_i \rangle + 1 \in I$.

Logo $q = \langle a_1, a_2, \ldots, a_n \rangle \in I$.

Demonstrado que $N \subset I$, veremos que $N = I$.

Temos que $W(F)/N \simeq Z$ e assim o ideal $I/N \simeq (d)$

Consideremos $(d) \neq (0)$.

Como $\theta(d\langle 1\rangle) \in \theta(I)$ vem que $\theta(d\langle 1\rangle) = \theta(x)$, $x \in I$.

Logo $\theta(d\langle 1\rangle - x) = 0$, ou seja, $d\langle 1\rangle - x \in N$.

Assim $d\langle 1\rangle \in I$

De $(\langle d\rangle)^2 = 1$, vem que $\langle d\rangle + 1 \in N \subset I$ ou $\langle d\rangle - 1 \in N \subset I$.

Concluímos assim que $1 \in I$ ou $-1 \in I$, que é uma contradição, pois $I \neq W(F)$.

Portanto $I/N = (0)$, isto é, $I = N$.

(4) $\Longrightarrow$ (1). Imediato

A última afirmação no teorema 2 decorre da própria demonstração das anteriores.

Proposição 2: Seja M um ideal maximal de W(F), $M \neq IF$. Então existe um único ideal primo Y com $Y \subsetneq M$.

Demonstração: Já vimos que para M maximal, $W(F)/M \simeq F_p$, com p primo ímpar, pois $M \neq IF$.

Sabemos então que existe um isoformismo

$$g : W(F)/M \longrightarrow F_p$$

Consideremos a relação $<$, sobre F, definida por

$$a < b \Longleftrightarrow g(\langle b - a\rangle + M) = 1$$

Vejamos que $<$ é uma relação de ordem.

1) se $a < b$ e $b < c$ então $g(\langle b-a\rangle + M) = 1$ e $g(\langle c-b\rangle + M) = 1$

Mas, por iv - teorema 8

$\langle b-a\rangle + \langle c-b\rangle + M = \langle c-a\rangle(1 + \langle b-a\rangle\langle c-b\rangle) + M$ e assim

$\langle b-a\rangle + M + \langle c-b\rangle + M = \langle c-a\rangle + M + (\langle c-a\rangle + M)(\langle b-a\rangle + M)(\langle c-b\rangle + M)$

Aplicando g em ambos os lados da última igualdade, vem

$1 + 1 = g(\langle c-a\rangle + M) + g(\langle c-a\rangle + M) \cdot 1 \cdot 1 = 2(\langle c-a\rangle + M)$

Como $2 \neq 0$, temos $g(\langle c-a\rangle + M) = 1$, isto é, $a < c$

2) tricotomia

Supondo $b - a \neq 0$, vem que $(\langle b-a\rangle)^2 = 1$ assim $\langle b-a\rangle = \pm 1$.

Logo, desde que $p \neq 2$, vem que

$g(\langle b-a\rangle + M) = \pm 1$, isto é, $a < b$ ou $b < a$

3) se $a < b$ e $a < c$ então $g(\langle c\rangle + M) = 1$ e $g(\langle b-a\rangle + M) = 1$

Como $g(\langle bc-ac\rangle+M) = g(\langle c\rangle(b-a)+M) = g(\langle c\rangle + M) \cdot g(\langle b-a\rangle +M) = 1$ temos que $ac < bc$.

4) se $a < b$ então $1 = g(b-a+M) = g(\langle b+c-(a+c)\rangle+M)$. Assim $a+c<b+c$. Observamos, pelo teorema 2', que existe um ideal primo não-maximal Y, com $a < b \Longleftrightarrow \langle b-a\rangle - 1 \in Y$. Mas $a < b \Longleftrightarrow g(\langle b-a\rangle+M)=1 \Longleftrightarrow g(\langle b-a\rangle-1+M)=0$

Assim $\langle b-a\rangle - 1 \in M$.

Temos então que para qualquer $a \neq 0$, $a \in F$,

$$\langle a\rangle - 1 \in Y \Longleftrightarrow \langle a\rangle - 1 \in M \quad (A)$$

Consideremos $u = \langle a_1\rangle + \ldots + \langle a_n\rangle$ em $W(F)$, com $a_i \neq 0$, para todo i. Sabemos que $\langle a_i\rangle \in \pm 1 + Y$ e com o $W(F)/Y \simeq Z$, vem que $u \in Y$ se e somente se para metade dos índices i, $\langle a_i\rangle - 1 \in Y$. Temos também que se M é maximal então $W(F)/M \simeq F_p$ e $\langle a_i\rangle \in \pm 1 + M$. Assim, vem que, se para metade dos índices i, $\langle a_i\rangle - 1 \in M$, então $u \in M$ (observe que aqui não vale a recíproca). Agora de (A), vemos que se $\langle a_i\rangle - 1 \in Y$ então $\langle a_i\rangle - 1 \in M$ e assim se $u \in Y$, $u \in M$, donde se conclui que $Y \subsetneq M$.

Vejamos, por fim, a unicidade de Y.

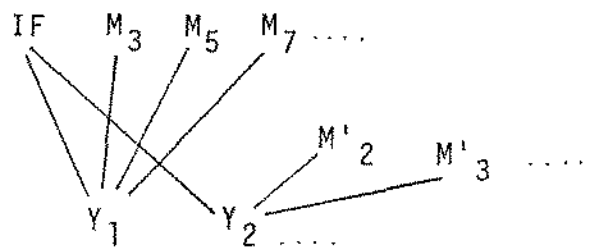
Supondo que Y_0 seja outro ideal primo não-maximal de $W(F)$ com $Y_0 \subsetneq M$, então pelo teorema 2, existe uma ordem $<_0$ com $\langle b-a\rangle - 1 \in Y_0 \Longleftrightarrow a <_0 b$. Notemos que se $a <_0 b$ então $\langle b-a\rangle - 1 \in M$ e assim $a < b$. Vemos então $<_0$ e $<$ são as mesmas ordens e pela correspondência biunívoca entre ordem e ideais primos não-maximais, temos $Y_0 = Y$. ■

Corolário: Se F não é ordenável então IF é o único ideal primo de $W(F)$ e $W(F)$ é local.

Demonstração: Sabemos pelo teorema 2 que não existe um ideal primo Y, não-maximal e, pela proposição 2, vem que não existe um ideal

maximal $M \neq IF$. ■

Observação 2: Pela última proposição, cada ideal maximal contém um único ideal primo. Além disso todo ideal primo, não-maximal, está contido em IF e numa coleção de ideais maximais, sendo um para cada primo. O esquema abaixo nos ajuda a perceber melhor essa situação.



Observação 3: Vale ressaltar que, em geral, W(F) não é um anel de integridade, mas quando isto acontece, podemos afirmar que (0) é o único ideal primo não-maximal de W(F).

Exemplo 1: Como veremos a seguir, $W(R) \approx Z$ e $W(F_3) \approx Z/4Z$. Assim (o) é o único ideal primo não-maximal de W(R), o que não ocorre em $W(F_3)$.

Exemplo 2: Seja F = R, o conjunto dos números reais. Sabemos que em R todo elemento é um quadrado ou o simétrico de um quadrado. Assim $\dot{F}/\dot{F}^2 = \{\pm 1\}$, ou seja, temos apenas duas classes distintas de quadrados. Logo uma forma anisotrópica de dimensão n, sobre W(R), diagonalizada, não pode ter coeficientes diferentes. Portanto para cada n, temos duas formas anisotrópicas, n<1> e n<-1>. Pela correspondência bijetora entre os elementos de W(F) e formas anisotrópi

cas, vemos que $W(F) \simeq Z$.

Como em R está definido apenas um cone positivo, temos que W(R) admite um único ideal primo não-maximal. A saber $I = (0)$. Podemos observar ainda que o ideal das formas pares $IF \simeq 2Z$.

Aproveitamos este exemplo para fazer mais alguns comentários a respeito da "assinatura" de uma forma quadrática em W(R), válidos também para corpos reais fechados.

Na diagonalização de uma forma quadrática q, o número de coeficientes positivos e o número de coeficientes negativos é unicamente determinado. De fato, seja q n-dimensional, onde $r\langle 1\rangle \perp (n-r)\langle -1\rangle$ e $s\langle 1\rangle \perp (n-s)\langle -1\rangle$ são duas diagonalização de q.

Passando para o anel de Witt, obtemos

$$r\langle 1\rangle - (n-r)\langle 1\rangle = s\langle 1\rangle - (n-s)\langle 1\rangle$$

em W(R), e consequentemente $2r\langle 1\rangle = 2s\langle 1\rangle$. Como $W(R) \simeq Z$, teremos $r = s$.

Se $n_+ = r$ representa o número de termos com coeficientes positivos e $n_- = n - r$ o número de termos com coeficientes negativos, então a **assinatura** de q é definida por

$$n_+ - n_- = n_+ - n + n_+ = 2n_+ - n$$

Nestes casos a assinatura ajuda na verificação de equivalências de formas quadráticas, pois duas formas serão equivalentes se e só se tiverem a mesma dimensão n e a mesma assinatura.

Antes de calcularmos o anel de Witt de um corpo finito qualquer, veremos um caso particular.

Exemplo 3: Seja $F = F_3$. Como $car(F_3) \neq 0$, F_3 não é ordenável, logo $W(F_3)$ não possui ideais primos não-maximais.

As únicas formas anisotrópicas de $W(F_3)$ são $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 1, 1 \rangle$, $\langle 2 \rangle = \langle -1 \rangle$ e assim $W(F_3) \simeq Z/4Z$. Todas as outras formas são isotrópicas; pois qualquer forma $q = \langle a_1, \ldots, a_n \rangle$ que contenha $q_1 = \langle 1, 1, 1 \rangle$ ou $q_2 = \langle 1, -1 \rangle$. Vemos que $q_3 = \langle -1, -1 \rangle$ como uma subforma será anisotrópica. Esta última é anisotrópica pois é equivalente a $X_1^2 + X_2^2$ e ambas representam um mesmo elemento de F_3.

Neste exemplo $IF = \{0, 2\}$, onde $2 = \langle 1, 1 \rangle$.

Observação 4: Com o exemplo acima podemos perceber a dificuldade em se calcular o anel de Groethendieck de um corpo, pois mesmo num caso relativamente simples como F_3, $\widehat{W}(F_3)$ terá infinitos elementos consistindo das combinações possíveis de $\langle 1 \rangle$ e $\langle -1 \rangle$.

Exemplo 4 - Analizemos $W(F)$ quando F for um corpo com q elementos, $q = p^m$, p primo diferente de 2 e m natural.

É sabido que $-1 \in F_p^2$ se e só se $p \equiv 1 \pmod 4$ e que $-1 \notin F_p^2$ quando $p \equiv 3 \pmod 4$

Veremos primeiramente o caso em que $p \equiv 1 \pmod 4$.

Temos então que $-1 \in F_p^2$, isto é, existe $w \in F_p$ com $w^2 = -1$.

Consideremos F de característica p. Como todo corpo

finito possui apenas duas classes de quadrados distintas, $\dot{F}/\dot{F}_2 = \{1, \bar{u}\}$, então $\dot{F} = \dot{F}^2 \cup u\dot{F}^2$. Assim se $\langle a_1, a_2, \ldots, a_n\rangle \in W(F)$, com $a_i \neq 0$, vem que $a_i = b_i^2$ ou $a_i = u\, b_i^2$. Logo

$$\langle a_1, a_2, \ldots, a_n\rangle \cong \langle b_{i_1}^2, \ldots, b_{i_r}^2, ub_{j_1}^2, \ldots, ub_{j_s}^2\rangle,$$

onde $r + s = n$.

Podemos ver então que

$$\langle a_1, \ldots, a_n\rangle \cong \langle 1, \ldots, 1\rangle + \langle u\rangle\langle 1, \ldots, 1\rangle$$

Vamos estudar a forma $\langle 1, 1, \ldots, 1\rangle$, de dimensão m, separadamente.

i) se $m = 2t$, então $\langle 1, \ldots, 1\rangle \cong \langle 1, w^2, 1, w^2, \ldots, 1, w^2\rangle$

$$\cong \langle 1, -1, \ldots, 1, -1\rangle = tH$$

ii) se $m = 2t + 1$, então $\langle 1, 1, \ldots, 1\rangle \cong \langle 1, w^2, 1, w^2, \ldots, 1\rangle$

$$\cong \langle 1, -1, \ldots, 1, -1\rangle + \langle 1\rangle = tH + 1$$

Vemos então que

$$\langle a_1, \ldots, a_n\rangle \cong \langle 1, 1, \ldots, 1\rangle \perp u\langle 1, \ldots, 1\rangle = \begin{cases} 0 \\ u\langle 1\rangle \\ \langle 1\rangle + \langle u\rangle = \langle 1, u\rangle \\ \langle 1\rangle \end{cases}$$

e esses são os únicos elementos distintos de W(F), isto é, W(F) tem ordem 4.

W(F), como grupo, não pode ser Z/4Z, pois no caso estudado todo elemento tem ordem 2. Logo, como grupo W(F) é isomorfo ao grupo de Klein. Como anel, W(F) é isomorfo a álgebra de grupo $F_2[\dot{F}/\dot{F}^2]$, pois $\{1, \bar{u}\}$ é uma base de tal álgebra e

$$0 = \langle 0 \rangle = 0 \cdot 1 + 0 \cdot \bar{u}$$

$$\langle u \rangle = u\langle 1 \rangle = 0 \cdot 1 + 1 \cdot \bar{u}$$

$$1 = \langle 1 \rangle = 1 \cdot 1 + 0 \cdot \bar{u}$$

$$\langle 1, u \rangle = \langle 1 \rangle + \langle u \rangle = 1 \cdot 1 + 1 \cdot \bar{u}$$

Vamos ver o caso em que $p \equiv 3 \pmod 4$ e assim $-1 \notin F_p^2$.
Dividiremos esse estudo em duas partes

1ª) Vamos supor $[F : F_p] = n$, n ímpar

Aqui teremos também que $-1 \notin F^2$, pois caso contrário $\sqrt{-1} \in F$ e $F_p \subset F_p(\sqrt{-1}) \subset F$. Como $[F : F_p] = [F : F_p(\sqrt{-1})][F_p(\sqrt{-1}) : F_p]$, teríamos grau de $[F : F_p]$ par, pois $[F_p(\sqrt{-1}) : F_p] = 2$. (Absurdo).

Agora como $-1 \notin F^2$, podemos tomar

$$\dot{F} = \dot{F}^2 \cup (-1)\dot{F}^2$$

Assim, se $q = \langle a_1, \ldots, a_n \rangle \in W(F)$, com $a_i \neq 0$, então

$$\langle a_1, \ldots, a_n \rangle \simeq \langle 1, \ldots, 1 \rangle + \langle -1 \rangle \langle 1, 1, \ldots, 1 \rangle$$

Como num corpo finito -1 sempre é soma de dois quadrados, pois se $-1 \in \dot{F}^2$ então $-1 \in D(\langle 1, 1 \rangle)$. Agora se $-1 \notin \dot{F}^2$ consideremos os conjuntos $\dot{F}^2$ e $1 + \dot{F}^2$ que são subconjuntos de F de mesma cardinalidade. Observamos que $1 + F^2 \neq F^2$ pois $1 \in F^2$ e $1 \notin 1 + \dot{F}^2$. Assim existe $x = 1 + z^2 \notin \dot{F}^2$. Como $-1 \notin \dot{F}^2$, vem que $1 + z^2 \neq 0$ e portanto $\dot{F}/\dot{F}^2 = \{1, 1 + z^2\}$. Como $1 \in D(\langle 1, 1 \rangle)$ e $1 + z^2 \in D(\langle 1, 1 \rangle)$, tem-se que $\dot{F} = D(\langle 1, 1 \rangle)$, ou seja, $-1 \in D(\langle 1, 1 \rangle)$. Tomando então $-1 = u^2 + v^2$, $u, v \in \dot{F}$ teremos $\langle 1, 1 \rangle \simeq \langle -1, -1 \rangle$.

Analisando a forma de dimensão m

$$\langle 1, 1, \ldots, 1 \rangle$$

e considerando $m = 2t$ então:

se $m = 4\ell$, teremos $q = 0$

se $m = 4\ell + 2$, teremos $q = \langle 1, 1 \rangle$

Tomando m ímpar teremos:

se $m = 4\ell + 1$, então $q = \langle 1 \rangle$

se $m = 4\ell + 3$, então $q = \langle 1, 1\rangle + \langle 1\rangle = \langle -1, -1\rangle + \langle 1\rangle = \langle -1\rangle$

Observamos, portanto que $W(F) = \{0, \langle 1\rangle, \langle -1\rangle, \langle 1, 1\rangle\}$ é cíclico com gerador $q_0 = \langle 1\rangle$, pois $\langle 1, 1\rangle = 2q_0$ e $\langle -1\rangle = 3q_0$. Assim $W(F) \simeq Z/4Z$. O isomorfismo do anel acima é facilmente comprovado tomando $\phi : Z/4Z \longrightarrow W(F)$, com $\phi(\bar{n}) = n\langle 1\rangle$.

2ª - Consideremos F uma extensão de F_p de grau n, n par.

Sabemos que qualquer extensão de um corpo finito é galoisiana cíclica. Assim o grupo de Galois $G(F, F_p) = Z/nZ = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ tem um subgrupo $H = \{0, \bar{2}, 2.\bar{2}, 3.\bar{2}\ldots\}$ de ordem $n/2$ e portanto $|G/H| = 2$.

Vemos então que F_p admite uma extensão intermediária $N = F_p(\sqrt{x})$, de grau 2. Como $x = y^2$ ou $x = -y^2$, pois $\dot{F}_p = \dot{F}_p^2 \cup (-1)\ \dot{F}_p^2$, podemos tomar $N = F_p(\sqrt{-1})$. Mas então $\sqrt{-1} \in F$, isto é, -1 é um quadrado em F e recaímos no caso onde $p \equiv 1 \pmod 4$ e $W(F) \simeq Z_2[\dot{F}/\dot{F}^2]$.

Vimos assim que se F é um corpo finito, então W(F) será isomorfo a álgebra de grupos $Z_2[\dot{F}/\dot{F}^2]$ ou ao anel $Z/4Z$.

CAPÍTULO III

CORPOS FORMALMENTE REAIS

Parte 2

Neste capítulo estudaremos os conceitos de corpo formalmente real, real fechado e pitagórico e veremos alguns resultados envolvendo o anel de Witt de tais corpos. Também, com o intuito de se demonstrar a Forma Fraca do Teorema de Springer introduziremos o conceito de transferência de Scharlau.

Aqui F representará um corpo qualquer.

Definição 1 - Dizemos que F é um corpo formalmente real se -1 não é soma de quadrados em F ou se para qualquer número natural n, a forma quadrática $n\langle 1\rangle = \langle 1, 1, \ldots, 1\rangle$ é anisotrópica sobre F.

Observação 1 - Se F é formalmente real então car (F) = 0, pois caso contrário teríamos

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ vezes}} = 0$$

ou seja

$$-1 = \underbrace{1 + 1 + \ldots + 1}_{(n-1) \text{ vezes}} = 1^2 + 1^2 + \ldots + 1^2 \text{ (Absurdo)}$$

Para um corpo F qualquer $\sigma(F)$ denotará o conjunto dos elementos de F que podem ser expressos como soma de quadrados.

Assim $\sigma(F) = \{a \in F,\ a = a_1^2 + \ldots + a_n^2$, para algum n natural$\}$.

Teorema 1

i) $\sigma(F)$ é fechado em relação à adição

ii) $\sigma(F) - \{0\}$ é um grupo multiplicativo

iii) se F não é formalmente real então $\sigma(F) = \begin{cases} F & \text{se car } (F) \neq 2 \\ \dot{F}^2 & \text{se car } (F) = 2 \end{cases}$

Demonstração

i) óbvia.

ii) seja $x \neq 0$, $x \in \sigma(F)$. Então

$$x = x_1^2 + x_2^2 + \ldots + x_n^2 \text{ e } \frac{1}{x} = \frac{x}{x^2} = \left(\frac{x_1}{x}\right)^2 + \ldots + \left(\frac{x_n}{x}\right)^2 \in \sigma(F) - \{0\}$$

Assim todo elemento $x \in \sigma(F) - \{0\}$ tem um inverso $\frac{1}{x} \in \sigma(F) - \{0\}$. As outras exigências têm verificações imediatas.

iii) se car (F) = 2, então para qualquer $x \in \dot{F}^2$, vem

$$x = a^2 = a^2 - b^2 + b^2 = (a-b)^2 + b^2 \in \sigma(F)$$

e se $x \in \sigma(F)$ então $x = a_1^2+\ldots+a_n^2=(a_1+\ldots a_n)^2 \in \dot{F}^2$. Logo $\sigma(F) = \dot{F}^2$.

Agora sejam car (F) $\neq$ 2 e $x \in F$. Sabemos que o plano hiperbólico é universal e portanto existe y e z $\in$ F com $x = y^2 - z^2$.

Desde que $(-1) \in \sigma(F)$, vem que $x = y^2 + (-1)z^2 \in \sigma(F)$, isto é, $F \subset \sigma(F)$. Como $\sigma(F) \subset F$, tem-se $\sigma(F) = F$. ■

Observação 2: Sejam P um cone positivo de F e F_0 um subcorpo de F. Podemos ordenar F_0 tomando como cone $P_0 = F_0 \cap P$. Diremos então que a ordem em F_0 é induzida pela ordem de F.

Teorema 2: Sejam F um corpo com cone positivo P. Então

i) $\sigma(F) - \{0\} \subset P$, isto é, soma de quadrados é sempre positivo.

ii) F é formalmente real.

iii) se $P' \subset F$, dá outro cone em F e $P \subset P'$ então $P = P'$.

Demonstração:

i) Seja $x \neq 0$ em $\sigma(F)$, $x = x_1^2 + x_2^2 + \ldots + x_n^2$. Sempre podemos assumir $x_i \neq 0$, e se mostrarmos que $x_i^2 \in P$ então $x \in P$, pois

P é fechado em relação à adição.

Temos $x_i^2 = (x_i)(x_i) = (-x_i)(-x_i) \in P$, pois ou $x_i \in P$ ou $-x_i \in P$.

ii) Desde que $1 \in P$, vem que $-1 \notin P$ e assim por i), vem que $-1 \notin \sigma(F)$, isto é, -1 não é soma de quadrados.

iii) Suponhamos que exista $x \in P'$ tal que $x \notin P$.

Então $-x \in P \subset P'$. Absurdo. ■

Observamos, pelos teoremas 1 e 2, que para corpos não formalmente reais, onde $car(F) \neq 2$, todos os elementos são soma de quadrados, o que impossibilita a existência de um cone positivo. Assim corpos não-formalmente reais não são ordenáveis.

Proposição 1: Se F é formalmente real e a extensão quadrática $F(\sqrt{a})$ não o é, então $-a \in \sigma(F)$.

Demonstração: Como $F(\sqrt{a})$ não é formalmente real, temos

$$-1 = (b_1 + c_1 \sqrt{a})^2 + \ldots + (b_n + c_n \sqrt{a})^2,$$

com $b_i, c_i \in F$.

Então $-1 = b_1^2 + ac_1^2 + b_n^2 + ac_n + 2b_1c_1 \sqrt{a} + \ldots + 2b_nc_n \sqrt{a}$

$$= \sum_{i=1}^{n} b_i^2 + a\sum_{i=1}^{n} c_i^2 + 2\sum_{i=1}^{n} b_i c_i \sqrt{a}$$

Observemos que $\sum_{i=1}^{n} c_i^2 \neq 0$, pois caso contrário teríamos $-1 = \sum b_i^2$ em F. Logo

$$\frac{-1}{\sum c_i^2} = \frac{\sum b_i^2}{\sum c_i^2} + a \quad \text{ou} \quad -a = \frac{\sum b_i^2 + 1}{\sum c_i^2} = (1+\sum b_i^2)(\sum c_i^2)^{-1}$$

Desde que $\sigma(F) - \{0\}$ é um grupo multiplicativo, vem que $-a \in \sigma(F)$.

Definição 2: Um corpo F é dito pitagórico se a soma de dois quadrados ou mais, em F, é um quadrado.

Observação 3: Na verdade, basta exigir que a soma $1 + y^2$ seja um quadrado, pois se a e b são quadrados, $a+b = x^2+c^2 = x^2(1+\frac{c^2}{x^2}) = x^2(1+y^2)$.

Observação 4: Se F é pitagórico então $\sigma(F) = \dot{F}^2$.

Definição 3: Um corpo F é dito real fechado se F é formalmente real mas nenhuma extensão algébrica própria de F o é.

Teorema 3: Se F é real fechado então F é pitagórico.

Demonstração: Vamos supor que $x = 1 + y^2$ não seja um quadrado em F. Então $F(\sqrt{x})$ é uma extensão algébrica própria de F e assim não formalmente real. Então pela proposição 1, $-x = -1 - y^2 \in \sigma(F)$, isto é, $-1 - y^2 = \sum z_i^2$, $z_i \in F$.

Temos então que $-1 = (\sum z_i^2) + y^2 \in \sigma(F)$, que é uma contradição. ■

O próximo resultado dá uma caracterização dos corpos reais fechados, corpos estes onde todo positivo é um quadrado e que possuem uma única ordem.

Teorema 4: Seja F um corpo real fechado. Então

(1) Para qualquer $x \in \dot{F}$, ou $x \in \dot{F}^2$ ou $-x \in \dot{F}^2$.

(2) F tem uma única ordem, onde $P = \dot{F}^2$.

Demonstração: Vamos assumir (1) e mostrar (2).

Temos que $0 \notin P$ e agora a condição 0 - 1 (pág. 45) segue de (1).

Vemos ainda que $P = \dot{F}^2$ é grupo multiplicativo e ainda, pelo teorema anterior, $P + P \subset P$. Logo 0 - 2 (pág. 45) está satisfeito.

Tomando $P' \subset P$, outro cone de F, teremos

$$\sigma(F) = P = \dot{F}^2 \subset P'$$

Assim $P' = P$.

Agora mostraremos (1).

Vamos supor que $x \notin \dot{F}^2$. Então $F(\sqrt{x})$ não é formalmente real, desde que F é real fechado.

Pela proposição 1, $-x \in \sigma(F) - \{0\}$. Mas F é pitagórico, logo $\sigma(F) - \{0\} = \dot{F}^2$. Assim $-x \in \dot{F}^2$. ■

Observação 5: Tudo o que foi feito no cálculo do anel de Witt do corpo dos números reais, é válido para um corpo F real fechado. Então, aqui também, $W(F) \simeq Z$.

A seguinte proposição nos garante a existência de corpos reais fechados e ainda apresenta uma forma de obtê-los.

Proposição 2: Sejam F um corpo formalmente real e $\overline{F}$ seu fecho algébrico. Então existe um corpo real fechado F' com $F \subset F' \subset \overline{F}$.

Demonstração: Consideremos a coleção S de todos os subcorpos formalmente reais de $\overline{F}$ contendo F. Temos que $S \neq \phi$, pois $F \in S$. Seja $\{F_\alpha\}$ uma família ordenada (pela inclusão) de tais subcorpos. Então $F_0 = \bigcup_\alpha F_\alpha \in S$. Assim, pelo Lema de Zorn, existe um elemento $F' \in S$ que é maximal relativamente à inclusão. Podemos ver que F' é real fechado.

O corolário a seguir dará uma melhor caracterização dos corpos formalmente reais.

Corolário 1: Um corpo F é formalmente real se e somente se possui

pelo menos uma ordem.

Demonstração:

<=) Segue do teorema 2

=>) Pela proposição anterior, existe uma extensão algébrica $F' \geq F$ que é real fechado. Tal extensão possui uma única ordem (teorema 4). Isso nos leva a induzir uma ordem sobre F, colocando $P_0 = F \cap P$, onde P é o cone positivo de F'.■

Proposição 3: Seja F um corpo. Então

i) se F é quadraticamente fechado, isto é, todo elemento é um quadrado, então F é pitagórico.

ii) se F é pitagórico e não formalmente real então F é quadraticamente fechado.

iii) se F é real fechado então F é pitagórico.

iv) se F_i são subcorpos de um corpo Ω, onde cada F_i é pitagórico, então $K = \bigcap_i F_i$ é pitagórico.

Demonstração

i) óbvio.

ii) consequência imediata de iii) teorema 1.

iii) (teorema 3).

iv) Consideremos $x^2 + y^2$, com $x, y \in K$. Devemos mostrar que existe $a \in K$ com $a^2 = x^2 + y^2$.

Observe que para cada i, existe $z_i \in F_i$ com $z_i^2 = x^2 + y^2$. Assim, para cada par de índices i, j, teremos $z_i = \pm z_j$.

Fixando z_{i_0}, teremos $z_{i_0} \in K$ e $z_{i_0}^2 = x^2 + y^2$. Assim tomamos $a = z_{i_0}$. ■

Teorema 5: Seja F um corpo. Então

i) F é pitagórico e formalmente real se e somente se $W(F)$ é livre de torção, isto é, o grupo de torsão é $W_t(F) = \{0\}$.

ii) F é pitagórico e não formalmente real se e somente se $W(F) \simeq Z/2Z$.

Demonstração: Vejamos primeiramente ii).

Por ii) da proposição 3, vem que F é quadraticamente fechado e logo $W(F) \simeq Z/2Z$. A recíproca é imediata desde que -1 é um quadrado e $\langle 1, 1\rangle$ é universal.

i)($\Longrightarrow$) Aqui basta mostrar que se $q = \langle a_1, \ldots, a_n\rangle$ é anisotrópica então $r \cdot q$ é também anisotrópica, r inteiro positivo.

Suponhamos que $(e_{11}, \ldots, e_{1r}, \ldots, e_{n1}, \ldots, e_{nr})$ seja um vetor isotrópico para $r \cdot q$, isto é

$$a_1e_{11}^2 + \ldots a_1e_{1r}^2 + \ldots + a_ne_{n1}^2 + \ldots + a_ne_{nr}^2 = 0$$

Como F é pitagórico, fazendo $e_{11}^2 + \ldots + e_{1r}^2 = d_1^2, \ldots$ $e_{n1}^2 + \ldots + e_{nr}^2 = d_n^2$, $d_i \in F$, vem que $a_1d_1^2 + \ldots + a_nd_n^2 = 0$. Como q é anisotrópica, segue que $d_i = 0$ e assim $e_{ij} = 0$, pois senão a hipótese de ser formalmente real seria contrariada. Logo $W_t(F) = \{0\}$.

($\Longleftarrow$) Observe que aqui basta supormos que W(F) não tem 2 - torsão.

Vamos mostrar que F é pitagórico.

Assumindo $d \neq 0$, $d = 1 + y^2$, $y \in F$, teremos $\langle 1, 1\rangle = \langle d, d\rangle$, pelo teorema 5, capítulo 1 e portanto $2\langle d\rangle = 2\langle 1\rangle$ em W(F). Desde que W(F) não tem 2 - torsão, vem que $\langle d\rangle = \langle 1\rangle$, isto é, $d \in \dot{F}^2$.

Concluímos assim que F é pitagórico.

Agora por (ii), necessariamente, devemos ter F formalmente real. ■

De agora em diante usaremos a denominação **corpo ordenável** em lugar de formalmente real.

Definição 4 - Seja F um corpo ordenado com cone positivo P. Uma extensão Δ de F é denominada fecho real de F se:

i) Δ é real fechado

ii) Δ é algébrica sobre F

iii) a ordem sobre F é induzida pela única ordem de Δ, isto é, $P = \dot{\Delta}^2 \cap F$.

Observação 6: Cada corpo ordenado F admite um fecho real F_α relativo a cada ordem α (ver 2.8, capítulo 8, [L]).

Existe na literatura sobre formas quadráticas um resultado, conhecido como Teorema de Springer, que garante que se uma forma quadrática é anisotrópica sobre um corpo F, ela permanecerá anisotrópica sobre qualquer extensão de F de grau ímpar. Demonstraremos um resultado mais fraco, chamado forma fraca do Teorema de Springer, mas que está coerente com o enfoque escolhido neste trabalho.

Antes do teorema de Springer, faremos uma rápida introdução da função transferência de Sharlau.

Seja K uma extensão de F. A partir de um F-espaço quadrático (V, B, q), vamos construir um outro K-espaço (V_K, B_K, q_K), tomando $V_K = K \otimes_F V$, com $\otimes_F$ sendo o produto tensorial sobre F.

$$B_K(k_1 \otimes v_1, k_2 \otimes v_2) = k_1 k_2 B(v_1, v_2)$$

para todo $k_1, k_2 \in k$ e $v_1, v_2 \in V$, e

$$q_K(k \otimes v) = k^2 q(v)$$

Notemos que se $\{v_1, v_2, \ldots, v_n\}$ é base para V então $\{1 \otimes v_1, 1 \otimes v_2, \ldots, 1 \otimes v_n\}$ é base para V_K e a matriz simétrica associada a q é a mesma que a associada a q_K. Logo, se q é regular, q_K também será.

Observação 7: A função $r^* : W(F) \longrightarrow W(K)$, induzida por $r^*(\langle a \rangle_F) = \langle a \rangle_K$, é um homomorfismo de anel.

Demonstração: Seja $t : F \longrightarrow W(K)$ dada por $t(a) = \langle a \rangle_K, \forall a \in F$.

Notemos que t satisfaz as condições i - iv do teorema 8, do capítulo um, logo existe um único homomorfismo de anel $r^*: W(F) \longrightarrow W(K)$ com $r^*(\langle a \rangle_K) = t(a) = \langle a \rangle_K$.

Observação 8: Em geral r^* não é um monomorfismo. Basta tomar $r^* : W(R) \longrightarrow W(C)$ e vermos que $r^*(\langle 1, 1 \rangle) = H_c$. Na verdade, para termos o monomorfismo, devemos exigir que $[K : F]$ seja ímpar.

Tomemos agora uma extensão finita K de F e o K-espaço quadrático (V, B). Se $g : K \longrightarrow F$ é um F-funcional linear não nulo, então $gB : V \times V \longrightarrow F$ dá origem a uma forma bilinear. Assim, do K-espaço (V, B) conseguimos um F-espaço (V, gB).

Observação 9: Se (V, B) é regular então (V, gB) também o é.

Demonstração: Vamos supor que (V, gB) não é regular, isto é, existe um vetor $x_0 \neq 0$, $x_0 \in V$ com $(gB)(x_0, y) = 0$ para todo $y \in V$. Como (V, B) é regular, existe $y_0 \in V$ com $B(x_0, y_0) \neq 0$. Para qualquer escalar $k \in K$, temos

$$B\left(x_0, \frac{k}{B(x_0, y_0)}\, y_0\right) = \frac{k}{B(x_0, y_0)} \cdot B(x_0, y_0) = k \text{ em } K$$

Aplicando g vem

$$g(k) = gB\left(x_0, \frac{k}{B(x_0, y_0)}\right) = 0$$

o que contraria o fato de g ser não nulo.■

Observação 10 - O F - espaço quadrático (V, gB) é chamado "a transferência de V" e denotado por gV.

Passaremos, a seguir, a definir um homomorfismo de grupo $g^* : W(K) \longrightarrow W(F)$.

Observemos, primeiramente que gK é o próprio K com forma bilinear $gB(\alpha, \beta) = g(\alpha \cdot \beta)$, $\alpha, \beta \in K$ e $B(\alpha, \beta) = \alpha\beta$.

Lema 1: Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ uma base ortogonal de gK e façamos $b_i = gB(\alpha_i, \alpha_i)$, para todo i. Então $b_i \neq 0$.

Demonstração: Vamos supor que exista i tal que $b_i = gB(\alpha_i, \alpha_i) = g(\alpha_i^2) = 0$.

Temos

$$\alpha_i^{-1} = \sum_{j=1}^{m} t_j \alpha_j$$

Logo

$$1 = \sum t_j \alpha_j \alpha_i$$

e assim

$$g(1) = t_i g(\alpha_i^2) = 0$$

Agora, para qualquer j, temos

$$\alpha_j^{-1} = \sum_s t_s \alpha_s$$

portanto

$$1 = \sum_s t_s \alpha_s \alpha_j$$

e assim

$$0 = g(1) = t_j g(\alpha_j^2)$$

Também

$$1 = \sum_k t_k \alpha_k$$

e portanto para todo i, vem que $1 . \alpha_i = \sum_k t_k \alpha_k \alpha_i$ e assim

$$g(\alpha_i) = t_i \, g(\alpha_i^2) = 0$$

Concluimos então que $g(\alpha_i) = 0$, para todo i. Absurdo, pois $g \neq 0$.

Lema 2: Seja (V, B) um K - espaço quadrático com base ortogonal $\{u_1, u_2, \ldots, u_n\}$. Suponhamos que $B(u_i, u_i) = c_i \in F$, para todo i. Então $\{u_i \alpha_j\}$ é uma base ortogonal de gV.

Demonstração: Basta observarmos que os vetores $u_i \alpha_j$ são ortogonais e assim linearmente independentes.

Corolário: Se V é hiperbólico então gV é hiperbólico.

Demonstração: Tomemos $c_1 = 1$, $c_2 = -1$, $c_3 = 1$, $c_4 = -1$, etc e n par. Então gV é uma soma ortogonal de espaços que tem bases ortogonais como $u_1 \alpha_j$, $u_2 \alpha_j$.

Agora $gB(u_1 \alpha_j, u_1 \alpha_j) = g(\alpha_j^2 B(u_1, u_1)) = b_j$ e

$$gB(u_2\ \alpha_j,\ u_2\ \alpha_j) = g\left(\alpha_j^2\ B(u_2,\ u_2)\right) = -\ b_j$$

Assim as formas quadráticas associadas são somas ortogonais de $b_jX_1^2 - b_jX_2^2$ que são equivalentes a somas do tipo $X_1^2 - X_2^2$. ■

Observação 11: $g(V_1 \oplus V_2) = gV_1 \oplus gV_2$

Demonstração - Óbvio, desde que $g(B(u, v)) = g(B_1(u_1, v_1)) + g(B_2(u_2, v_2))$ onde B_1, B_2 são as bilineares associadas a V_1 e V_2 e $u = (u_1, u_2)$ e $v = (v_1, v_2)$. ■

Definimos então a função $g^* : W(K) \longrightarrow W(F)$ fazendo $g^*(V) = gV$, que, pela observação e corolário acima, é, de fato, um homomorfismo de grupo.

Lema 3: A composição $W(F) \xrightarrow{r^*} W(K) \xrightarrow{g^*} W(F)$ coincide com a multiplicação em $W(F)$ por gK, isto é, $(g^* o\ r^*)(V) = V \otimes gK$.

Demonstração: Seja $V = \langle a_1, \ldots, a_n \rangle$, onde $a_i \in F$ e $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é uma base ortogonal de V_F com $B(\beta_i, \beta_i) = a_i$. Tomando $\{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ uma base ortogonal de gK, temos que $\{\beta_i \otimes \gamma_j\}$ é uma base para gV pelo Lema 2.

Agora, como $gB(\beta_i \otimes \gamma_j, \beta_i \otimes \gamma_j) = B(\beta_i, \beta_i)\, g(\gamma_i^2) = a_ib_i$, vem que

$$g^*(r^*(V)) = \langle a_1, \ldots, a_n \rangle \otimes \langle b_1, \ldots, b_m \rangle = V \otimes gK$$

Teorema 6: (Forma Fraca do Teorema de Springer)

Seja K uma extensão finita de F de grau ímpar.

Então a função $r^* : W(F) \longrightarrow W(K)$ é injetora. Temos ainda que W(K) é uma extensão inteira de W(F).

Demonstração: Escolhemos F e K com $F \subsetneq K$ e $[K : F]$ o menor possível, contrariando o teorema, isto é, r^* não injetora.

Tomamos $a \in K$ tal que $a \notin F$.

Então $[K : F] = [K : F(a)][F(a) : F]$ e a composta $W(F) \to W\,F(a) \longrightarrow W(K)$ é $W(F) \to W(K)$. Assim pelo menos uma das funções envolvidas deve ser não injetora. Se fosse a primeira teríamos $F = F(a)$ e chegaríamos a uma contradição, pois $a \notin F$. Logo deve ser a segunda e então chegamos que $K = F(a)$. Observamos que nas duas conclusões usamos a condição de minimalidade.

Tomemos então $[K : F] = 2m + 1$. Então $\{1, a, a^2, \ldots, a^{2m}\}$ é uma base para K sobre F.

Vamos definir $g \in \mathrm{Hom}_F(K, F)$ por

$$g(b_0 + b_1 a + b_2 a^2 + \ldots + b_{2m}\, a^{2m}) = b_0$$

para todo $b_0, \ldots b_{2m} \in F$.

Observemos que $gB(a^i, a^j) = g(a^i \cdot a^j) = g(a^{i+j}) = 0$, para $1 \leq i, j \leq m$ e consideremos o subespaço $U = Fa + Fa^2 + \ldots Fa^m$. Temos $gB(u_1, u_2) = 0$ para todo $u_1, u_2 \in U$, isto é, U é trivial. Temos também que $\dim U = m$ e que $(gK)_{tr} = \{0\}$ pois para $\beta \neq 0 \in K$, vem que $gB(\beta, \beta^{-1}) = g(1) \neq 0$.

Pelo teorema 4, capítulo 1, vem que $\dim(gK)_{hy} \geq 2\dim U = 2m$. Mas $gK = (gK)_{an} \oplus (gK)_{hy}$ (ver Teorema da Decomposição). Assim

$$2m + 1 = \dim(gK) = \dim(gK)_{an} + \dim(gK)_{hy}$$

Desde que $\dim(gK)_{hy}$ é par e $2m \leq \dim(gK)_{hy} \leq 2m+1$, temos que $\dim(gK)_{an} = 1$.

Tomemos agora $u_1 \in K$, um vetor anisotrópico.

Então $gB(u_1, u_1) = g(u_1 . u_1) = b \neq 0$ e para $x \in gK$, $x = \alpha u_1 + v$, $v \in (gK)_{hy}$ vem que $gB(x, x) = \alpha^2 g(u_1 . u_1)$ e assim gK é $\langle b \rangle_F$ em $W(F)$. Desde que $1 = \langle b \rangle \langle b^{-1} \rangle$, vem que (gK) é uma unidade.

Como já foi visto, a composta $W(F) \xrightarrow{r^*} W(K) \xrightarrow{g^*} W(F)$ é a multiplicação em $W(F)$ por gK, que é uma unidade, logo injetora. Assim r^* também é injetora e chegamos a uma contradição. Mostramos assim a primeira parte do teorema.

A segunda parte decorre do fato de $W(K)$ ser gerado por elementos da forma $\langle b \rangle_K$, de cada uma dessas formas satisfazer $x^3 - x = 0$ e soma de inteiros ser inteiro. ■

Corolário: Seja $<$ uma ordem sobre F. Então para qualquer extensão finita de grau ímpar K de F, existe uma ordem sobre K, que restrita a F, coincide com $<$.

Demonstração: Seja Y um ideal primo não-maximal de $W(F)$ correspondente a ordem $<$. O teorema Going Up (ver [Z]) garante que se $W(K)$

é inteira sobre W(F) e Y é um ideal primo em W(F) então existe um primo P de W(K) com $P \cap W(F) = Y$. Sabemos também que Y é não-maximal se e somente se P o é.

Seja então $<_p$ a ordem sobre K correspondente a P. Para a, b $\in$ F, temos

$$a <_p b \Longleftrightarrow <b-a>-1 \in P \cap W(F) = Y \Longleftrightarrow a < b. \blacksquare$$

Proposição 4 - Se F é ordenável então assim é toda extensão K de F, finita de grau ímpar.

Demonstração: Consequência imediata do corolário anterior.

Veremos a seguir alguns exemplos.

Exemplo 1: Seja F um corpo formalmente real com

$$\dot{F} = \dot{F}^2 \cup (-\dot{F}^2) \cup (2\dot{F}^2) \cup (-2\dot{F}^2)$$

Observemos que W(F) é aditivamente gerado por <1> e <2>, pois se $q = \langle a_1, \ldots, a_n \rangle$, $a_i \in \dot{F}$, então $a_i = \pm t^2$ ou $a_i = \pm 2t^2$. Assim $q \simeq t_1 \langle 1 \rangle \perp t_2 \langle 2 \rangle$, com t_1, t_2 e Z.

Podemos dizer também que <1> e a forma binária $\tau = \langle 1, -2 \rangle$ geram W(F), pois

$$[\langle 1\rangle] - [\langle 1, -2\rangle] = [\langle 1\rangle] + [\langle -1, 2\rangle] = [\langle 1\rangle \perp \langle -1, 2\rangle] = [\langle 1, -1, 2\rangle] = [\langle 2\rangle]$$

Aqui $[q]$ representa a classe da forma quadrática q.

Temos também que $2\tau = \tau \perp \tau = \langle 1, -2, 1, -2\rangle$ é isotrópica. Logo, pelo teorema 4, capítulo 1, $2\tau \simeq \langle 1, -1\rangle \perp \langle a, b\rangle$.

Desde que $\mathrm{disc}(2\tau) = 1$, vem que $\mathrm{disc}(\langle a, b\rangle) = ab = -1$. Logo, pelo teorema 3, capítulo I, tem se $\langle a, b\rangle \simeq \langle 1, -1\rangle$ e assim

$$2\tau \simeq 2H = 0$$

Também, pelo argumento acima, $\tau^2 = \langle 1, -2\rangle \otimes \langle 1, -2\rangle = \langle 1, -2, -2, 4\rangle \simeq 2H = 0$.

Tomemos a aplicação $\varphi : Z[t] \to W(F)$ dada por

$\varphi\left(\sum a_i t^i\right) = \sum a_i \tau^i$, que, obviamente, é um homomorfismo de anel, sobrejetor.

Mostremos que $\ker \varphi = \langle 2t, t^2\rangle$

Claramente $\langle 2t, t^2\rangle \subset \ker\varphi$, pois $\varphi(2t) = 0$ e $\varphi(t^2) = 0$

Agora seja $\sum a_i t^i \in Z[t]$ com $\varphi\left(\sum a_i t^i\right) = 0$.

Temos que $\sum a_i t^i = a_0 + a_1 t + \sum_{i \geq 2} a_i t^i$.

Observemos que

$$\varphi\left(\sum_{i \geq 2} a_i t^i\right) = \sum a_i \tau^i$$

com

$$\tau^i = \begin{cases} (\tau^2)^j \text{ se } i \text{ par} \\ (\tau^2)^j\ \tau, \text{ se } i \text{ ímpar.} \end{cases}$$

Em qualquer caso, teremos

$$\varphi(\sum_{i\geq 2} a_i\ t^i) = 0$$

Assim

$$0 = \varphi(\sum a_i t^i) = \varphi(a_0 + a_i t + \sum_{i\geq 2} a_i t^i) = \langle a_0\rangle + a_1\tau$$

Temos então que $\langle a_0\rangle + a_1\tau$ é hiperbólica, isto é, $\langle a_0\rangle + a_1\tau = n\ H$.. Logo $\dim(\langle a_0\rangle + a_1\tau)$ é par e portanto $a_0 = 0$.

Chegamos então a $a_1\tau = 0$. Colocando $a_1 = 2r + s$ com $s = 0$ ou $s = 1$, concluímos que

$$a_1\tau = r\,.\,2\tau + s\tau = s\tau = \begin{cases} \tau, \text{ para } s = 1 \\ 0, \text{ para } s = 0 \end{cases}$$

Como τ não é hiperbólica, pois -2 não é um quadrado em F, se $s\tau = 0$ então $s = 0$. E portanto $a_1 = 2r$.

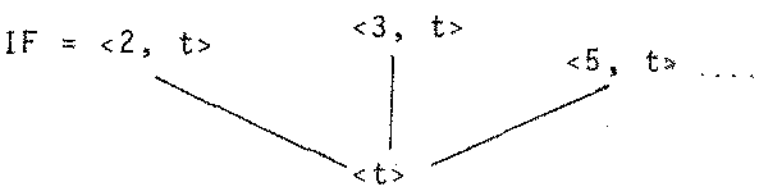
Temos então

$$\sum a_i t^i = a_0 + a_1 t + \sum_{i\geq 2} a_i t^i = r\,.\,2t + (\sum_{i\geq 2} a_i t^{i-2})t^2 \in \langle 2t,\ t^2\rangle$$

Concluímos assim que $\ker \varphi = \langle 2t, t^2 \rangle$ e $W(F) \simeq \frac{Z[t]}{\langle 2t, t^2 \rangle}$

Temos $\langle 2t, t^2 \rangle \subset \langle t \rangle \subset \langle p, t \rangle$ para qualquer primo p. Assim $\langle p, t \rangle$ são os ideais primos maximais de W(F). Também $\langle t \rangle$ é o único primo não-maximal. Observamos ainda que $W_t = \langle t \rangle$. .Nesse caso $IF = \langle 2, t \rangle$.

Segundo a representação usada na página-59 teremos



Exemplo 2: Sejam R_1 e R_2 corpos reais fechados contidos em $\bar{Q}$ e $K = R_1 \cap R_2$.

Como R_1 e R_2 são reais fechados vem que R_1 e R_2 são pitagóricos e assim $K = R_1 \cap R_2$ é pitagórico.

Podemos observar que K tem pelo menos uma ordem, pois a ordem de R_1 ou R_2 induzirá uma ordem em K. Assim K é formalmente real. Veremos abaixo que K tem no máximo duas ordens. Ou, ainda mais, que as duas possíveis ordem de K são as induzidas por R_1^2 e R_2^2.

Suponhamos que K possui três ordens $P_1 = R_1^2 \cap K$, $P_2 = R_2^2 \cap K$ e P_3, com $P_3 \neq P_1$ e $P_3 \neq P_2$, ou seja, $P_3 \not\subset P_1$ e $P_3 \not\subset P_2$. Assim existem $x_1 \in P_3 - P_1$ e $x_2 \in P_3 - P_2$

Mostremos agora que existe $x \in P_3 - P_1 \cup P_2$.

Se $x_1 \notin P_2$ ou $x_2 \notin P_1$ então $x = x_1$ ou $x = x_2$ satisfaz o requerido.

Se $x_1 \in P_2$ e $x_2 \in P_1$, $x = x_1 + x_2 \in P_3 - P_1 \cup P_2$.

Tomando o x encontrado acima, temos que $-x \in P_1 \cap P_2$, o que implica $-x \in R_1^2 \cap R_2^2 \subseteq K^2 \subseteq P_3$, o que é uma contradição, pois $x \in P_3$. Portanto K tem no máximo duas ordens.

i) Estudemos o caso em que K tem apenas uma ordem.

Aqui todo elemento é um quadrado ou menos um quadrado e portanto $W(K) \simeq Z$.

Sabemos ainda que W(K) é livre de torsão, isto é, $W_t(K) = \{0\}$, pois K é pitagórico e formalmente real.

ii) Para estudar K com duas ordens usaremos um resultado, clássico da teoria das formas quadráticas, conhecido como **Princípio Local - Global de Pfister**, que pode ser encontrado em [L]. Esse princípio garante a existência de um homomorfismo

$$r^* : W(K) \longrightarrow W(R_1) \times W(R_2) \simeq Z \times Z$$

Aqui $r^* = \prod_\alpha r^*_\alpha$ onde r_α é a inclusão $F \subset F_\alpha$, F_α o fecho real de F relativo a ordem α.

Como $W_t(K) = 0$, tal homomorfismo é injetor e assim podemos identificar W(K) com um subanel de Z x Z.

Tomemos $a \in K$ com $a \in P_1$ e $a \notin P_2$. Para qualquer $x \in K = R_1 \cap R_2$, teremos

i) se $x \in R_1^2$ e $x \in R_2^2$ então $x \in K^2$.

ii) se $x \in R_1^2$ e $x \notin R_2^2$ então $ax \in R_1^2$ e $ax \in R_2^2$, assim $ax \in K^2$, ou seja, $x \in aK^2$.

iii) se $x \notin R_1^2$ e $x \in R_2^2$ então $x \in -aK^2$

iv) se $x \notin R_1^2$ e $x \notin R_2^2$ então $x \in -K^2$

Vemos então que $\dot{K} = \dot{K}^2 \cup \dot{K}^2 \cup a\dot{K}^2 \cup -a\dot{K}^2$

Tomando $q = \langle a_1, \ldots, a_n \rangle$, $a_i \in K$, temos que

$$q = \begin{cases} \langle 1, \ldots, 1, a, \ldots, a \rangle \text{ ou} \\ \langle 1, \ldots, 1, -a, \ldots, -a \rangle \text{ ou} \\ \langle -1, \ldots, -1, a, \ldots, a \rangle \text{ ou} \\ \langle -1, \ldots, -1, -a, \ldots, -a \rangle \end{cases}$$

pois

$$a_i = b_i^2 \text{ ou } ab_i^2 \text{ ou } -b_i^2 \text{ ou } -ab_i^2$$

Assim

$$q = n\langle 1 \rangle + m\langle a \rangle \text{ , com } n, m \in Z$$

Vem então que

$$r^*(q) = n\langle 1, 1 \rangle + m\langle 1, -1 \rangle$$

Tomando (a, b) em $Z \times Z$ vemos que $(a, b) \in W(K)$ se $(a, b) = n\langle 1, 1\rangle + m\langle 1, -1\rangle$, ou seja, devemos ter $n = \frac{a+b}{2}$ e $m = \frac{a-b}{2}$. Temos então que $W(K) = \{(a, b) \in Z \times Z \text{ com } a \equiv b(\text{mod}2)\}$

Podemos observar também que o ideal das formas de dimensão par é

$$IF = \{(a, b) \in Z \times Z \quad \text{com} \quad a \equiv 0 \ (\text{mod } 2)\}$$

Como aqui K possui duas ordens, devemos ter dois ideais primos não-maximais e esses são:

$$I_1 = \{(a, b) \in Z \times Z \quad \text{com} \quad a \equiv 0 \ (\text{mod } 2) \text{ e } b = 0\} \quad \text{e}$$

$$I_2 = \{(a, b) \in Z \times Z \quad \text{com} \quad b \equiv 0 \ (\text{mod } 2) \text{ e } a = 0\}$$

Verificaremos a afirmação apenas para I_1.

De maneira análoga se confirma para I_2.

Seja $s : W(K) \longrightarrow Z$ dada por $s(x, y) = y$. Como s é a restrição de um homomorfismo, é também ela, um homomorfismo e ainda mais, é sobrejetor.

Tomando I_1 acima, veremos que $I_1 = \ker s$.

Sendo $(x, y) \in I_1$ então $y = o$ e $s(x, y) = 0$. Assim $I_1 \subset \ker s$.

Agora se $(x, y) \in \ker s$ então $s(x, y) = 0$, ou seja, $y = 0$. Como x e y devem ter a mesma paridade chegamos que x é par

e logo $\ker s \subset I_1$.

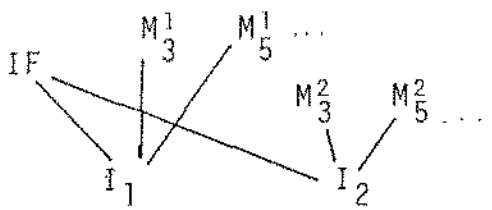
Temos portanto que $W(K)/I_1 \cong Z$. Assim I_1 é não-maximal e comprova-se facilmente que é um ideal primo.

Para acharmos os primos maximais basta notarmos que

$M_p^2 = s^{-1}(p\ Z) = \{(a, b) \in Z \times Z \text{ com } p|_a\}$

Observemos que esses ideais contêm I_2. Do mesmo modo $M_p^1 = \{(a, b) \in Z \times Z/p|_b\}$ são os ideais primos maximais contendo I_1.

Esquematicamente tem-se



CAPÍTULO IV

O ANEL DE WITT DE CORPO DOS NÚMEROS RACIONAIS

Antes de entrarmos no estudo, propriamente dito, da estrutura do anel de Witt de corpo dos números racionais, teceremos alguns comentários a respeito de valorização e corpo dos números p-ádicos.

O leitor interessado poderá encontrar mais informações em [R].

Primeiramente damos uma definição genérica de valorização e quando preciso, esta será particularizada.

Consideremos então um grupo G, totalmente ordenado, e um corpo F.

Definição 1 - Uma aplicação $v : F^* \longrightarrow G$ é dita uma valorização se para quaisquer $x, y \in F^*$ tem-se

i) $v(xy) = v(x) + v(y)$

ii) $v(x + y) \geq \min \{v(x), v(y)\}$

Exemplo 1 - Seja $x \in Q^*$ e consideremos sua decomposição em fatores primos, isto é, $x = \pm \Pi p^{v_p(x)}$, onde o produto é considerado sobre todos os primos p e $v_p(x) = 0$ para quase todo p.

Observemos que $v_p(x) \in Z$ e que $v_p(x) \geq 0$ para $x \in Z$.

Neste caso temos uma valorização $v_p : Q^* \to Z$, chamada valorização p - ãdica. Quando $v_p(x) \geq 0$, x é dito um p - inteiro.

Sempre que tivermos a situação acima, diremos que o par (F, V) é um corpo valorizado.

Observação 1: Se quizermos definir a valorização sobre F, devemos tomar um certo cuidado, pois teremos que fazer $v(0) = \infty$, pois caso contrário v será a aplicação nula. Senão, vejamos.

Fazendo $v(0) = k$, teremos $k = v(0) = v(0 \cdot x) = v(0) + v(x) = k + v(x)$

Assim $v(x) = 0$, para todo x de F.

Temos então

Definição 2: Uma aplicação $v : F \to G \cup \{\infty\}$ será uma valorização se:

i) $v(0) = \infty$ e $v(x) \in G, \forall x, x \neq 0, x \in F$

ii) $v(x, y) = v(x) + v(y)$

iii) $v(x + y) \geq \min \{ v(x), v(y)\}$

Definição 3: Uma aplicação $|\ | : F \to R^+$ tal que

i) $|0| = 0$ e se $x \neq 0$ então $|x| > 0$

ii) $|x\ y| = |x|\ |y|$

iii) $|x + y| \leq |x| + |y|$, é denominado valor absoluto de F.

Como veremos a seguir, todo valor absoluto, exceto o usual, dá origem a uma valorização, e assim o par $(F, |\ |)$ também será denominado corpo valorizado.

Exemplo 2: Fazendo $|x|_p = p^{-vp(x)}$, para $x \in Q^*$ e $|0| = 0$, a aplicação $|\ |_p : Q \to R^+$ tem as propriedades acima e é denominado valor absoluto p - ádico de Q. Temos ainda em Q o valor absoluto trivial $\{|x| = 1$ se $x \neq 0$ e $|0| = 0\}$ e o valor absoluto ordinário ou usual $(|x|_\infty = \max\{x, -x\})$.

Definição 4 - Um valor absoluto $|\ |$, de F, é dito não arquimediano quando $|n \cdot 1_F| \leq 1$ para todo $n \in Z$. Caso contrário, $|\ |$ é dito arquimediano.

Exemplo 3 - Como não-arquimedianos temos o valor absoluto trivial e o p - ádico de Q.

Observação 2 - Podemos relacionar valorizações e valores absolutos colocando $|a| = e^{-v(a)}$.

No contexto, quando não especificado, o termo valorização significa valorização não-arquimediana.

Observação 3 - Seja $(K, |\ |)$ um corpo valorizado. Então K é um espaço métrico com distância $d : k \times K \to R^+$ dada por $d(x, y) = |x - y|$

Podemos então, em K, falar em sequência convergente, sequência de Cauchy, etc.

Definição 5: Diremos que um corpo valorizado $(K_1, |\ |_1)$ é um completamento de $(K, |\ |)$ quando as propriedades abaixo se verificarem.

i) K é um subcorpo de K_1 e $|\ |$ é a restrição de $|\ |_1$.

ii) $(K_1, |\ |_1)$ é um corpo completo, isto é, toda sequência de Cauchy de elementos de K_1 tem um limite em K_1.

iii) todo elemento de K_1 é o limite de uma sequência de Cauchy de elementos do subcorpo K.

O par $(K, |\ |)$ é chamado corpo valorizado completo quando coincide com seu completamento, isto é, toda sequência de Cauchy de elementos de K, tem um limite em K.

Exemplo 4: Temos que o corpo R dos números reais é o completamento do corpo Q relativamente ao valor absoluto usual e ainda que o completamente de Q em relação ao valor absoluto p-ádico é o chamado **corpo dos números p - ádicos**, denotado por Q_p.

Com a continuada intenção de estudar o anel de Witt de Q, veremos alguns resultados.

Trabalharemos, como mencionado, com corpos valorizados não-arquimedianos. Assim, se F é um corpo valorizado, $v : F \to Z \cup \{\infty\}$ denotará uma valorização, que admitiremos sobrejetora.

O conjunto $A_v = \{ x \in F,\ v(x) \geq 0 \}$ é um sub-anel de F, chamado **anel de valorização de F.**

Também A_v tem um único ideal maximal $P_v = \{ x \in F,\ v(x) \geq 1 \}$, principal e gerado por qualquer elemento π com $v(\pi) = 1$. De fato, seja $x \in P_v$. Então $v(x) \geq 1$, isto é, $v(x) = 1 + k$, com $k \in Z$. Podemos assim tomar $y \in F$ tal que $v(y) = k$ e escolher π com $v(\pi) = 1$. Assim $v(x) = v(\pi) + v(y) = v(\pi y)$. Logo $v(x) - v(\pi y) = 0$ ou $v(xy^{-1}\pi^{-1}) = 0$

Fazendo $xy^{-1}\pi^{-1} = z$, tem-se $z \in A_v - P_v$ e segue que $x = (zy)\pi$, donde se conclui que P_v é gerado por π.

O conjunto $U_v = \{ x \in A_v;\ x \notin P_v \} = \{ x \in F;\ v(x) = 0 \}$ é chamado grupo das unidades de A_v.

Observação 4: Para qualquer $x \in F^*$, vem que $x = u\ \pi^{v(x)}$, com $u \in U_v$, pois se $x \in F^*$ então

$$v(x) = k = 1 + 1 + \ldots + 1 = v(\pi) + \ldots + v(\pi) = v(\pi^k)$$

Logo

$$v(\pi^k x^{-1}) = 0$$

ou seja

$$\pi^k x^{-1} = u_1,\ u_1 \in U_v$$

Assim $\pi^k = u_1 x$, donde vem que $x = u_1^{-1}\pi^k = u\pi^{v(x)}$, com

$$u = u_1^{-1} \in U_v$$

Notemos que a escolha do uniformizador π, tal que $v(\pi) = 1$, poderia ter recaido sobre $u\pi$ com $u \in U_v$.

O corpo $\bar{F} = A_v/P_v$ é denominado **corpo das classes residuais** de F.

Observação 5: Para todo $\bar{a} \in \bar{F}$ tem-se que

$$\bar{a} = \bar{0} \text{ ou } a \in U$$

Definição 6: Um corpo valorizado (F, v) é dito local se for completo relativamente a v.

Lema 1 - Seja (F, v) um corpo local com $car(\bar{F}) \neq 2$.

Então para qualquer $u \in U_v$, u é um quadrado em F se e somente se $\bar{u}$ é um quadrado em $\bar{F}$.

Demonstração:

($\Longrightarrow$) se $u \in \dot{F}^2$ então $u = a^2$. Logo $u - a^2 = 0$ e assim $\overline{u - a^2} = \bar{u} - \bar{a}^2 = \bar{0}$, ou seja, $\bar{u} = \bar{a}^2$

($\Longleftarrow$) para tanto, contruiremos uma sequência $\{b_i\}$ em U_v tal que

$$b_i^2 \equiv u \pmod{P_v^i} \quad e \quad b_{i+1} \equiv b_i \pmod{P_v^i}$$

para $i \geq 1$, ou seja, uma sequência $\{b_i\}$ com

$$b_i^2 - u \in P_v^i \quad e \quad b_{i+1} - b_i \in P_v^i$$

Como $P_v^i \subset P_v$, temos $b_i^2 - u \in P_v$ e $b_{i+1} - b_i \in P_v$

Uma vez contruída tal sequência, resultará que

$$\lim_{i \to +\infty}(b_i^2 - u) = b^2 - u = 0$$

desde que

$$b_i^2 - u \in P_v^i$$

Teremos então que $u \in \dot{F}^2$.

Passamos a construção, por indução, da sequência citada acima.

A existência de b_1 é garantido pelo fato de $\bar{u}$ ser um quadrado em $\bar{F}$, pois assim $\bar{u} = \bar{b}_1^2$, isto é, $b_1^2 \equiv u \pmod{P_v}$.

Supondo que temos b_i como requerido, seja

$$b_{i+1} = b_i + \pi^i z$$

onde $z \in A$ deve ser determinado. Sabemos que

$$b_i^2 - u = \pi^i c, \; c \in A$$

Então

$$b_{i+1}^2 - u = (b_i + \pi^i z)^2 - u = b_i^2 + 2b_i\pi^i z + \pi^{2i}z^2 - u$$

$$= 2b_i\pi^i z + \pi^{2i}z^2 + \pi^i c = \pi^i(2b_i z + \pi^i z^2 + c)$$

Como $\pi^{2i} z^2 \in P_v^{i+1}$, vem que

$$b_{i+1}^2 - u \equiv \pi^i(c + 2b_i z) \pmod{P_v^{i+1}}$$

Notemos que $v(2b_i) = v(2) + v(b_i) = v(2)$.

Como $v(2) = v(1 + 1) \geq \min\{V(1), V(1)\}$, vem que $v(2) \geq 0$. Mas $v(2)$ não pode ser maior que zero, pois $car(\bar{F}) \neq 2$, logo $v(2)=0$.

Usando que $2b_i \in U_v$, podemos escolher

$$z = \frac{\pi - c}{2b_i}$$

tal que $c + 2b_i z = \pi$ e teremos que $b_{i+1}^2 \equiv u \pmod{P_v^{i+1}}$

Sabemos que $b_{i+1} = b_i + \pi^i z$. Assim

$$v(b_{i+1}) = v(b_i + \pi^i z) \geq \min\{v(b_i), v(\pi^i z)\} = \min\{0, v(\pi^i z)\}$$

Ainda,

$$v(\pi^i z) = i\, v(\pi) + v\left(\frac{\pi - c}{2b_i}\right) = i + v(\pi - c)$$

Como $v(\pi - c) \in A_v$, vem que $v(\pi - c) \geq 0$.

Logo $v(\pi^i z) \geq i$ e então $v(b_{i+1}) = \min\{v(b_i), v(\pi^i z)\} = 0$

Concluímos assim que $b_{i+1} \in U_v$ e $b_{i+1} \equiv b_i \pmod{P_v^i}$ ■

Corolário: Sob as mesmas hipóteses do lema anterior, um elemento não-nulo $u\pi^m$, $u \in U_v$, $m \in Z$, é um quadrado em F se e somente se m é par e $\bar{u} \in \bar{F}^2$.

Demonstração:

($\Leftarrow$) Como $\bar{u} \in \bar{F}^2$, então $u = x^2$. Assim $u\pi^m = x^2\pi^m$, com $m = 2n$. Logo $u\pi^m = x^2(\pi^n)^2 = (x\pi^n)^2$. Portanto $u\pi^m$ é um quadrado em F.

($\Rightarrow$) Temos que

$$u\pi^m = x^2$$

Então

$$v(u\,\pi^m) = 2v(x) \text{ ou } v(u) + mv(\pi) = 2v(x)$$

Desde que $v(u) = 0$ e $v(\pi) = 1$, vem que $m = 2v(x)$, isto é, m é par.

Como $u\,\pi^m = u\,\pi^{2n} = x^2$, tiramos

$$u(\pi^n)^2 = x^2$$

isto é,

$$u = \left(\frac{x}{\pi^n}\right)^2$$

Portanto

$$\bar{u} = \left[\left(\frac{\overline{x}}{\pi^n}\right)\right]^2 \in \bar{F}^2 \blacksquare$$

Considerando car $(\bar{F}) \neq 2$, veremos mais alguns resultados que serão úteis no cálculo do anel W(Q).

Teorema 1 - Seja F um corpo local com car $(\bar{F}) \neq 2$.

Então existe um isoformismo de grupo $g : W(F) \rightarrow W(\bar{F}) \oplus W(\bar{F})$

Para possibilitar uma demonstração mais simples, lembremos que o grupo de Witt W(F) é um grupo livre gerado por $< a >$, com seus geradores satisfazendo:

i) $\langle x \rangle = \langle xy^2 \rangle$

ii) $\langle x \rangle + \langle -x \rangle = 0$

iii) $\langle x \rangle + \langle y \rangle = \langle x + y \rangle + \langle xy(x + y) \rangle$, com $x, y, x + y \in F^*$

Assim se g for definida nos geradores de W(F) e verificando as relações acima, teremos que g se estende a um único homomorfismo bem definido.

Sabemos ainda que para cada $x \in F^*$, $x = \pi^m u$, com $u \in U_v$ e $v(\pi) = 1$.

Definamos então

$$g([\langle x\rangle]) = \begin{cases} ([\langle \bar{u}\rangle], 0) & \text{se } m \text{ é par} \\ (0, [\langle \bar{u}\rangle]) & \text{se } m \text{ é ímpar} \end{cases}$$

Para efeito de simplificação, usaremos simplesmente $\langle x\rangle$ no lugar de $[\langle x\rangle]$.

Verifiquemos que g respeita as relações que caracterizam o grupo de Witt.

i) Como $y = \pi^n z$, $z \in U_v$, tem-se $xy^2 = u\pi^m \cdot \pi^{2m} z^2 = u z^2 \pi^{m+2n}$

Agora, de $\langle x\rangle = \langle xy^2\rangle$, vem que:

a) para m par

$$g(\langle x\rangle) = g(\langle u\pi^m\rangle) = (\langle \bar{u}\rangle, 0) \text{ e}$$

$$g(\langle xy^2\rangle) = g(\langle uz^2\pi^{m+2n}\rangle) = (\langle \bar{u}\,\bar{z}^2\rangle, 0) = \langle \bar{u}, 0\rangle$$

b) para m ímpar

$$g(\langle x\rangle) = (0, \langle \bar{u}\rangle) \text{ e}$$

$$g(\langle xy^2\rangle) = g(\langle uz^2\pi^{m+2m}\rangle) = (0, \langle \bar{u}\,\bar{z}^2\rangle) = (0, \langle \bar{u}\rangle)$$

Assim, tanto em a) como em b) vemos que

$$g(\langle x\rangle) = g(\langle xy^2\rangle)$$

ii) Tomando $x = u\,\pi^m$, vem que:

a) para m par

$$g(\langle x\rangle) + g(\langle -x\rangle) = (\langle \bar{u}\rangle, 0) + (\langle -\bar{u}\rangle, 0) = (\langle \bar{u}\rangle + \langle -\bar{u}\rangle, 0) = (0,0)$$

b) para m ímpar

$$g(\langle x\rangle) + g(\langle -x\rangle) = (0, \langle \bar{u}\rangle) + (0, \langle -\bar{u}\rangle) = (0, \langle \bar{u}\rangle + \langle -\bar{u}\rangle) = (0, 0)$$

Em qualquer dos casos teremos

$$g(\langle x\rangle) + g(\langle -x\rangle) = 0$$

iii) Tomando $x + y \neq 0$, $x = u\pi^m$, $y = z\pi^n$, devemos mostrar que

$$g(\langle x\rangle) + g(\langle y\rangle) = g(\langle x + y\rangle) + g(\langle xy\ (x + y)\rangle)$$

Assumamos, sem perda de generalidade, que $m \leq n$.

Temos então que

$$x + y = u\pi^m + z\pi^n = \pi^m(u + z\pi^{n-m})$$

Para $m < n$, vem que $t = u + z\pi^{n-m} \in U_v$, pois

$$v(t) = v(u + z\pi^{n-m}) \geq \min\{v(u), v(\pi^{n-m} z)\} = \min\{0, n-m\} = 0$$

Como $v(t - u) = n - m > 0$, vem que $\bar{t} = \bar{u}$.

Considerando

a) m e n pares, teremos

$$g(\langle x+y\rangle) = (\langle\bar{t}\rangle, 0) = (\langle\bar{u}\rangle, 0)$$

$$g(\langle xy(x+y)\rangle) = g(\langle u\, z\, t\pi^{2m+n}\rangle) = (\langle\overline{u\, z\, t}\rangle, 0) = (\langle\bar{u}^2\, \bar{z}\rangle, 0) = (\langle\bar{z}\rangle, 0)$$

pois $\bar{u} = \bar{t}$ e

$$g(\langle x\rangle) = (\langle\bar{u}\rangle, 0),\ g(\langle y\rangle) = (\langle\bar{z}\rangle, 0)$$

b) m e n ímpares

Então

$g(\langle x\rangle)=(0, \langle\bar{u}\rangle)$, $g(\langle y\rangle)=(0, \langle\bar{z}\rangle)$, $g(\langle x+y\rangle)=(0, \langle\bar{t}\rangle)=(0, \langle\bar{u}\rangle)$ e

$g(\langle xy(x+y)\rangle)=g(\langle uzt\pi^{2m+n}\rangle)=(0, \langle\overline{uzt}\rangle)=(0, \langle\bar{z}\rangle)$

c) m par e n ímpar

Então

$g(\langle x\rangle)=(\langle\bar{u}\rangle, 0)$, $g(\langle y\rangle)=(0, \langle\bar{z}\rangle)$, $g(\langle x+y\rangle)=(\langle\bar{t}\rangle, 0)=(\langle\bar{u}\rangle, 0)$ e

$g(\langle xy(x+y)\rangle)=g(\langle uzt\,\pi^{2m+n}\rangle)=(0, \langle\overline{uzt}\rangle)=(0, \langle\bar{z}\rangle)$

d) m ímpar e n par, o raciocínio acima se repete

Concluímos por a), b), c) e d), que para $m < n$, a condição iii) se verifica

Supondo agora $m = n$, teremos

$$x + y = \pi^m(u + z)$$

Fazendo $u + z = \pi^r w$, $w \in U_V$ e $r \geq 0$, e, considerando primeiramente m e n ímpares, obtemos

$g(\langle x\rangle) = (0, \langle \bar{u}\rangle)$ e $g(\langle y\rangle) = (0, \langle \bar{z}\rangle)$

Se $r = 0$, então $u + z = w$, $\bar{u} + \bar{z} = \bar{w} \neq \bar{0}$ e

$$g(\langle x+y\rangle) + g\langle xy(x+y)\rangle) = (0, \langle \bar{w}\rangle) + g(\langle uzw\ \pi^{2m+n}\rangle) = (0, \langle \bar{w}\rangle) +$$

$$+ (0, \langle \bar{u}\,\bar{z}\,\bar{w}\rangle) = (0, \langle \bar{u}+\bar{z}\rangle) + (0, \langle \bar{u}\bar{z}(\bar{u}+\bar{z})\rangle) = (0, \langle \bar{u}+\bar{z}\rangle) +$$

$$+ \langle \bar{u}\bar{z}(\bar{u}+\bar{z})\rangle = (0, \langle \bar{u}\rangle + \langle \bar{z}\rangle) = (0, \langle \bar{u}\rangle) + (0, \langle \bar{z}\rangle)$$

Agora se $r \geq 1$, então $\bar{u} + \bar{z} = \bar{0}$ e

$$g(\langle x\rangle)+g(\langle y\rangle) = (0, \langle \bar{u}\rangle)+(0, \langle \bar{z}\rangle) = (0, \langle \bar{u}\rangle+\langle \bar{z}\rangle) = (0, \langle \bar{u}\rangle+\langle -\bar{u}\rangle) = (0, 0)$$

Como $x + y = \pi^m(u + z) = \pi^m \pi^r w = \pi^{m+r} w$, teremos

$$g(\langle x+y\rangle) + g(\langle xy(x+y)\rangle) = g(\langle \pi^{m+r} w\rangle) + g(\langle u\, z\, w\ \pi^{m+n+(m+r)}\rangle)$$

$$= \begin{cases} (\langle \bar{w}\rangle, 0) + (\langle \bar{u}\bar{z}\bar{w}\rangle, 0) = (\langle \bar{w}\rangle + \langle -\bar{u}^2\, w\rangle, 0) = (0, 0) \text{ se } r \text{ é ímpar} \\ (0, \langle \bar{w}\rangle) + (0, \langle \bar{u}\bar{z}\bar{w}\rangle) = (0, \langle \bar{w}\rangle + \langle -\bar{u}^2 w\rangle) = (0, 0) \text{ se } r \text{ é par} \end{cases}$$

De modo análogo a igualdade se verifica para m e n pares.

Temos então que g se estende de maneira única a um único homomorfismo de grupo, que por abuso de notação, também será

denotado por g.

Lembremos ainda que qualquer forma unidimensional sobre F pode ser escrita como $\langle u \rangle$ ou $\langle \pi u \rangle$, com $u \in U_v$. Assim, uma forma arbitrária q pode ser escrita como $q = q_1 \perp \langle \pi \rangle q_2$, onde

$$q_1 = \langle u_1, \ldots, u_r \rangle \text{ e } q_2 = \langle \pi \rangle \langle u_{r+1}, \ldots, u_n \rangle, \; u_i \in U_v$$

Chegamos então que o único homomorfismo

$$g : W(F) \longrightarrow W(\bar{F}) \oplus W(\bar{F})$$

construído acima, fica definido por

$$g(q) = g(q_1 \perp \langle \pi \rangle q_2) = (\bar{q}_1, \bar{q}_2)$$

onde por $\bar{q}$, $\bar{q}_1$, $\bar{q}_2$ entendemos suas classes

Veremos, a seguir, a bijetividade de g.

Lema 2: Seja F um corpo local com $car(\bar{F}) \neq 2$.

i) $q = \langle a_1, \ldots, a_n \rangle$, com $a_i \in U_v$, é isotrópica se e somente se $\bar{q} = \langle \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n \rangle$ é isotrópica.

ii) $q = q_1 \perp \langle \pi \rangle q_2$, com $q_1 = \langle a_1, \ldots, a_r \rangle$ e $q_2 = \langle a_{r+1}, \ldots, a_n \rangle$ $a_i \in U_v$, é anisotrópica sobre F se e somente se $\bar{q}_1$ e $\bar{q}_2$ são anisotrópicas sobre $\bar{F}$.

Demonstração:

i) Vamos supor $q = \langle a_1, \ldots, a_n \rangle$ isotrópica. Temos então um vetor isotrópico não-nulo $(x_1, x_2, \ldots, x_n) \in A^n$.

Após cancelarmos potências comuns de π, podemos assumir que o vetor $(x_1, x_2, \ldots, x_n)$ possui pelo menos um $x_i \in U_v$. Assim $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$ é um vetor isotrópico, não-nulo, para $\bar{q}$.

Reciprocamente tomemos $\bar{q}$ isotrópica,

$$\bar{q} = \sum_{i=1}^{n} \bar{a}_i \, X_i^2$$

Então existe um vetor não-nulo $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$ com $\bar{q}(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) = 0$, isto é, $\bar{a}_1\bar{x}_1^2 + \ldots + \bar{a}_n\bar{x}_n^2 = 0$.

Observemos que se deve ter pelo menos duas coordenadas do vetor isotrópico diferentes de zero, pois, caso contrário teríamos $\bar{a}_1\bar{x}_1^2 = 0$, o que acarretaria $\bar{x}_1 = 0$ para todo i.

Podemos escrever então

$$\bar{x}_i^2 = \frac{-(\bar{a}_1\bar{x}_1^2 + \ldots + \bar{a}_{i-1}\,\bar{x}_{i-1}^2 + \bar{a}_{i+1}\,\bar{x}_{i+1}^2 + \ldots \bar{a}_n\bar{x}_n^2)}{\bar{a}_i}$$

com $\bar{x}_i \neq 0$

Assim $\left(- \frac{\bar{a}_1\bar{x}_1^2 + \ldots + \bar{a}_n\bar{x}_n^2}{\bar{a}_i}\right)$ é um quadrado em $\bar{F}$ e pelo lema-1, vem que

$$-\left(\frac{a_1x_1^2 + \ldots + a_{i-1}x_{i+1}^2 + a_{i+1}x_{i+1}^2 + \ldots + a_nx_n^2}{a_i}\right)$$

é um quadrado em F e portanto

$$-(a_1x_1^2 + a_{i-1}x_{i-1}^2 + a_{i+1}x_{i+1}^2 + \ldots + a_nx_n^2) = a_ib_i^2$$

ou $a_1x_1^2 + \ldots + a_ib_i^2 + \ldots + a_nx_n^2 = 0$, com pelo menos um dos x_i não-nulo, isto é, q é isotrópica.

ii) Se q é anisotrópica assim são q_1 e q_2 e, por i), concluímos que $\overline{q}_1$ e $\overline{q}_2$ são anisotrópicas.

Para mostrarmos a recíproca, vamos supor que q seja isotrópica sem que $\overline{q}_1$ e $\overline{q}_2$ o sejam.

Sabemos então que existe um vetor não-nulo $(x_1, x_2, \ldots, x_n)$ com

$$\sum_{i=1}^{r} a_ix_i^2 + \pi \sum_{i=r+1}^{n} a_ix_i^2 = 0$$

Assim

$$v\left(\sum_{i=1}^{r} a_ix_i^2 + \pi \sum_{i=r+1}^{n} a_ix_i^2\right) = \infty > \min\{v(a_ix_i^2), v(\pi a_ix_i^2)\} = \min\{v(x_i^2), v(\pi x_i^2)\} \quad (I)$$

Segue então que devem existir, i, j tais que

$$\left.\begin{array}{ll} \text{a) } v(a_i x_i^2) = v(\pi a_j x_j^2) & \\ \text{b) } v(a_i x_i^2) = v(a_j x_j^2) & \\ \text{c) } v(\pi a_i x_i^2) = v(a_j x_j^2) & \text{seja o mínimo} \\ \text{d) } v(\pi a_i x_i^2) = v(\pi a_j x_j^2) & \end{array}\right\}$$

1º) se a) ocorrer então

$$t = v(a_i x_i^2) = 2v(x_i) \in 2Z \text{ e}$$

$$t = v(\pi a_j x_j^2) = 1 + 2v(x_j) \in 2Z + 1$$

claramente uma contradição.

2º) se b) ocorrer então

$$\min \{ v(x_i^2), v(\pi x_j^2) \} = v(x_{i_0}^2) \text{ e}$$

$$v(\pi a_i x_i^2) > v(x_{i_0}^2)$$

para todo $i = r + 1, \ldots, n$

Logo

$$v\left(\pi a_i\left(\frac{x_i}{x_{i_0}}\right)^2\right) > 0 \quad e \quad v\left(\sum_{i=r+1}^{n} \pi a_i\left(\frac{x_i}{x_{i_0}}\right)^2\right) > 0$$

De (I), vem que

$$v\left(\sum_{i=1}^{r} a_i\left(\frac{x_i}{x_{i_0}}\right)^2 + \sum_{i=r+1}^{n} \pi a_i\left(\frac{x_i}{x_{i_0}}\right)^2\right) > 0$$

Logo

$$\sum_{i=1}^{r} \bar{a}_i\left(\frac{\overline{x_i}}{x_{i_0}}\right)^2 + \bar{0} = \bar{0}$$

isto é, $\bar{q}$, é isotrópica. Novamente aqui uma contradição.

3º) pelo mesmo argumento usado em 1ª), c) não ocorre.

4º) se d) ocorre, então

$$\min\{v(x_i^2), v(\pi x_i^2)\} = v(\pi x_{i_0}^2) \quad e$$

$$v(a_i x_i^2) > v(\pi x_i^2), \forall i = 1, \ldots, r.$$

Assim

$$v\left(\frac{a_i}{\pi}\left(\frac{x_i}{x_{i_0}}\right)^2\right) > 0 \quad e \quad v\left(\sum_{i=1}^{r}\frac{a_i}{\pi}\left(\frac{x_i}{x_{i_0}}\right)^2\right) > 0$$

De (I) vem que

$$v\left(\sum_{i=1}^{r}\frac{a_i}{\pi}\left(\frac{x_i}{x_{i_0}}\right)^2 + \sum_{i=r+1}^{n} a_i\left(\frac{x_i}{x_{i_0}}\right)^2\right) > 0$$

e portanto

$$\bar{0} + \sum_{i=r+1}^{n} \bar{a}_i\left(\frac{\overline{x_i}}{x_{i_0}}\right)^2 = \bar{0}$$

isto é, $\bar{q}_2$ é isotrópica. E aqui, mais uma vez, chegamos a uma contradição.

Por 1º), 2º), 3º) e 4º) concluímos que q só pode ser anisotrópica. ■

A injetividade de g segue do lema 2, pois se $\bar{q}_1$ ou $\bar{q}_2$ for hiperbólica então $\bar{q}_1$ ou $\bar{q}_2$ será isotrópica e assim q será isotrópica. E isto contraria a escolha de q.

A sobrejetividade de g é óbvia.

Portanto $g : W(F) \longrightarrow W(\bar{F}) \oplus W(\bar{F})$ é um isomorfismo de grupo.

O teorema anterior pode ser colocado na seguinte forma.

Teorema 2 - Tem-se um isomorfismo $(\partial_1, \partial_2) : W(F) \to W(\bar{F}) \oplus W(\bar{F})$, com $\partial_i(q) = \bar{q}_i$, $i = 1, 2$ (∂_1, ∂_2 são denominados o primeiro e o segundo homomorfismos residuais, respectivamente).

Apenas como curiosidade, observamos que ∂_1 não depende da escolha de π enquanto o mesmo não ocorre com ∂_2.

Tomemos, como exemplo, a valorização 3 - ádica, onde $v_3(6) = 1$ e $v_3(3) = 1$. Tomando π como 6 ou como 3, teremos

$$\partial_2(\langle 12\rangle) = \partial_2(\langle 2 . 6\rangle) = \bar{2} \quad \text{e} \quad \partial_2(\langle 12\rangle) = \partial_2(\langle 3 . 4\rangle) = \bar{4}$$

respectivamente.

Antes de analisarmos a estrutura de $W(Q)$, calculemos $W(F)$, para F um corpo p - ádico.

Exemplo 5 - Seja F um corpo p - ádico, isto é, F é um corpo local com $\bar{F}$ finito e aqui tomamos $car(\bar{F}) \neq 2$.

Seja $\bar{F} = \bar{F}_q$, com $q = p^m$, m inteiro e p primo, $p \neq 2$.

Então, do capítulo anterior, sabemos que:

$$- W(\bar{F}) \simeq Z_2\left[\dot{\bar{F}}/\dot{\bar{F}}^2\right] = Z/2Z \oplus Z/2Z$$

pois $\dot{\bar{F}}/\dot{\bar{F}}^2 \simeq Z/2Z$, se $q \equiv 1 \pmod 4$

$$- W(F) \simeq Z/4Z \text{ se } q \equiv 3 \pmod 4$$

O teorema 1 nos diz que $W(F) \simeq W(\bar{F}) \oplus W(\bar{F})$, como gru

po. Então, para F p-ádico, teremos

$$W(F) \simeq Z/2Z \oplus Z/2Z \oplus Z/2Z \oplus Z/2Z \quad \text{ou}$$

$$W(F) \simeq Z/4Z \oplus Z/4Z$$

Observação 6: Sabemos que qualquer forma quadrática de dimensão maior ou igual a três, sobre um corpo finito, é isotrópica. Logo cada corpo local admite quatro formas anisotrópicas e pelo demonstrado acima, vemos que W(F) tem exatamente 16 formas anisotropicas.

Nesta altura já contamos com todas as informações para apresentarmos o anel de Witt dos números racionais.

A idéia explorada segue [L] e é atribuída a Gauss que foi redescoberta por Milnor e Tate.

O interessante deste argumento é que ele não pressupõe o conhecimento prévio do princípio de Hasse - Minkowski.

Em primeiro lugar consideremos o único homomorfismo $i : Z \to W(Q)$ que leva 1 em $\langle 1 \rangle$ e o fato de que para qualquer primo p, o corpo dos resíduos $\overline{Q}_p$ do corpo local Q_p é $Z/pZ = F_p$.

De acordo com o teorema 2, para $p \neq 2$, existe um segundo homomorfismo residual de $W(Q_p)$ em $W(F_p)$, que composto com o homomorfismo de $W(Q)$ em $W(Q_p)$, dado pela inclusão $Q \subset Q_p$, nos dá outro homomorfismo de grupo.

$$\partial_p : W(Q) \to W(F_p), \quad p \neq 2$$

Observemos, também, que se $a \in Q$ é primo com p, isto é, se **a** é uma unidade p - ádica, então

$$\delta_p(\langle a \rangle) = 0 \quad \text{e} \quad \delta_p(\langle pa \rangle) = \langle \bar{a} \rangle$$

pois sendo **a** primo com p, vem que $v_p(a) = 0$.

O teorema de Springer não se aplica a Q_2 e por isso damos outra definição para δ_2.

Colocamos simplesmente $\delta_2 : W(Q) \longrightarrow Z/2Z$, com

$$\delta_2(q) \equiv v_2(\det(q)) \pmod 2$$

onde v_2 representa a valorização 2 - ádica.

Observemos que

$$\delta_2(q_1 \perp q_2) \equiv v_2(\det(q_1) \cdot \det(q_2)) \pmod 2$$

$$\equiv v_2(\det(q_1) + v_2(\det(q_2) \pmod 2 \text{ e}$$

$$\delta_2(H) = v_2(-1) \equiv 0 \pmod 2$$

Temos portanto um homomorfismo de grupo bem definido.

Teorema 3 - A sequência

$$0 \to Z \xrightarrow{i} W(Q) \xrightarrow{\oplus \delta_p} Z/2Z \oplus \sum_{p\neq 2}^{\oplus} W(F_p) \longrightarrow 0$$

é exata cindida.

Demonstração: Veremos primeiramente que a sequência é exata.

Aqui $|\ |$ denotará o valor absoluto usual.

Seja $L_d \subset W(Q)$ gerado como sub-anel por $\langle a \rangle$, com $a \in Z$ e $|a| \leq d$

Observemos que se $b = a_1 a_2 \ldots a_r$, com $a_i \in Z$ e $|a_i| \leq d$, então $\langle b \rangle \in L_d$. Assim L_d é gerado aditivamente pelos elementos desse tipo, isto é,

$$L_d = \{\sum m_i \langle 2 \rangle^{i_2} \langle 3 \rangle^{i_3} \ldots \langle d \rangle^{i_d},\ m_i \in Z \text{ e } i_j = 0 \text{ ou } 1\}$$

Observemos que

1) $L_1 = \{\sum m_i \langle 1 \rangle,\ m_i \in Z\} = Z\langle 1 \rangle$

2) $L_d = L_{d-1}$ se d não é primo

Construimos assim uma cadeia ascendente de sub-anéis $L_1 \subset L_2 \subset W(Q)$.

Passamos a determinar L_p/L_{p-1}, com p primo.

Se $x \in L_2/L_1$ então $x = y + L_1$, onde y é uma soma finita de elementos do tipo $m_i \langle 2^i \rangle$.

Notemos que

$$m_i \langle 2^i \rangle \begin{cases} m_i\langle 1\rangle, \text{ se } i \text{ é par} \\ m_i\langle 2\rangle, \text{ se } i \text{ é ímpar} \end{cases}$$

Logo L_2/L_1 é gerado por $\langle 2\rangle$

Podemos dizer ainda que $\langle 2\rangle$ tem ordem 2 em L_2/L_1, isto é, $2.\langle 2\rangle \in L_1$. De fato, temos

$$\langle -1, 2\rangle = \langle 1, -2\rangle \text{ e } \langle -1, 2\rangle = \langle -1\rangle + \langle 2\rangle$$

Assim

$$\langle -1, 2\rangle + L_1 = \langle 2\rangle + L_1 \quad \text{e} \quad \langle 1, -2\rangle + L_1 = \langle -2\rangle + L_1$$

Logo

$\langle 2\rangle + L_1 = \langle -2\rangle + L_1$, isto é, $2\langle 2\rangle \in L_1$

Considerando o homomorfismo $\delta_2 : W(Q) \longrightarrow Z/2Z$, definido anteriormente, este induzirá um isomorfismo

$$f_1 : L_2/L_1 \longrightarrow Z/2Z$$

com

$$f_1(m\langle 2\rangle + L_1) = \delta_2(m\langle 2\rangle)$$

Temos que se $X = m\langle 2\rangle + L_1$ então

$$X = \begin{cases} L_1 \text{ se } m \text{ for par} \\ \langle 2\rangle + L_1 \text{ se } m \text{ for ímpar} \end{cases}$$

Concluímos então pela existência de um isomorfismo inverso

$$\varphi_2 : Z/2Z \longrightarrow L_2/L_1$$

Vamos definir para cada primo $p \neq 2$, um homomorfismo $\varphi_p : W(F_p) \longrightarrow L_p/L_{p-1}$. Para tanto necessitamos do seguinte.

Lema 3

i) Para qualquer primo p, L_p/L_{p-1} é gerado aditivamente por $\langle p\ a_1 \ldots a_s\rangle + L_{p-1}$, com $|a_i| < p$

ii) Se $|a| < p$ e $a \equiv a_1 \ldots a_s \pmod p$, com $|a_i| < p$, então $\langle pa_1 \ldots a_s\rangle \equiv \langle pa\rangle \pmod{L_{p-1}}$

Demonstração:

i) Se $x \in L_p$, x é soma finita de elementos do tipo

$$\sum m_i < 2^{i_2} \ldots p^{i_p}>$$

com cada forma unidimensional $<b^{i}b>$ envolvida, podendo ser reduzida a <1> ou <b>.

Então, na verdade, se

$$y \in L_p/L_{p-1},$$

temos que

$$y = \sum m_i <p\ a_1^i\ a_2^i \ldots a_s^i> + L_{p-1}$$

com $|a_i^j| < p$

Para mostrarmos ii), calculemos $<p\ a_1 \ldots a_s>$ módulo L_{p-1}.

Faremos a demonstração por indução sobre s.

Para s = 1, temos

$$|a| < p,\ |a_1| < p \quad e \quad a \equiv a_1 \pmod p$$

então $a = a_1$ e assim

$$<p\ a_1> \equiv <p\ a> \pmod{L_{p-1}}$$

Pela hipótese de indução, vamos supor que

$$a \equiv a_1 \ldots a_s \pmod{p}$$

é válido para todo $s' < s$.

Pelo algoritmo de Euclides, obtemos

$$a_1 a_2 = pk + h ,$$

com $|h| < p$.

Primeiramente, veremos que $|k| < p$. De fato,

$$|a_1 a_2 - h| = |pk| \leq |a_1 a_2| + |h| \leq (p-1)^2 + p - 1 = p^2 - p$$

Assim $|pk| = p\,|k| \leq p\,(p-1)$, isto é, $|k| < p$.

Vemos agora que $\langle h, pk\rangle \sim \langle a_1, a_2, a_1 a_2\, p\, h\, k\rangle$, pois ambas são formas binárias, com mesmo determinante e representam o mesmo elemento $a_1 a_2$. Assim, em $W(Q)$, $\langle a_1 a_2\rangle = \langle h\rangle + \langle pk\rangle - \langle a_1 a_2\, p\, h\, k\rangle$.

Multiplicando por $\langle p\ a_3 \ldots a_s\rangle$, obtemos

$$\langle p\, a_1\, a_2 \ldots a_s\rangle = \langle p\, h\, a_3 \ldots a_s\rangle + \langle k\ a_3 \ldots a_s\rangle - \langle h\, k\, a_1 \ldots a_s\rangle$$

Como $\langle k\, a_3 \ldots a_s\rangle$ e $\langle -h\, k\, a_1 \ldots a_s\rangle$ estão em L_{p-1}, vem que $\langle p\, a_1\, a_2 \ldots a_s\rangle \equiv \langle p\, h\, a_3 \ldots a_s\rangle \pmod{L_{p-1}}$.

Como $h \equiv a_1\ a_2 \pmod{p}$, temos, pela hipótese de indu

ção, que $\langle p^h a_3 \ldots a_s \rangle \equiv \langle p a \rangle \pmod{L_{p-1}}$. Assim

$$\langle p a_1 \ldots a_s \rangle \equiv \langle p a \rangle \pmod{L_{p-1}} \blacksquare$$

Observação 7: Seja $p \neq 2$. Para cada classe residual $\bar{a} \in \bar{Q}_p = F_p$, a denotará o único inteiro não-negativo, menor que p, que dá origem a $\bar{a}$.

Vamos mostrar que a regra $\langle \bar{a} \rangle \longrightarrow \langle pa \rangle + L_{p-1}$ dá origem a um homomorfismo de grupo bem definido, $\varphi_p : W(F_p) \to L_p/L_{p-1}$

Se $\bar{a} = \bar{b}$ então $\langle pa \rangle \equiv \langle pb \rangle \pmod{L_{p-1}}$, pelo lema anterior. Logo a função φ_p é bem definida

Verifiquemos que φ_p respeita as relações que caracterizam $W(F_p)$ como um grupo abeliano, isto é, φ_p respeita

i) $\langle \bar{b}\ \bar{c}^2 \rangle = \langle \bar{b} \rangle$

ii) $\langle \bar{a} \rangle + \langle \bar{b} \rangle = \langle \bar{a} + \bar{b} \rangle + \langle \bar{a}\bar{b}(\bar{a} + \bar{b}) \rangle$

iii) $\langle \bar{1} \rangle + \langle -\bar{1} \rangle = 0$, para $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{a} + \bar{b} \in F_p$

Consideremos a, b, c inteiros não-negativos menores que p. Suponhamos que $bc^2 \equiv a \pmod{p}$, isto é, $\overline{bc^2} = \bar{a}$. Então

$$\langle pb \rangle = \langle pbc^2 \rangle \equiv \langle pa \rangle \pmod{L_{p-1}}$$

pelo lema 3.

Assim

$$\langle pb\rangle - \langle pa\rangle \in L_{p-1} \quad e \quad \langle pb\rangle + L_{p-1} = \langle pa\rangle + L_{p-1}$$

isto é,

$$\varphi_p(\langle \bar{b}\rangle) = \langle pa\rangle + L_{p-1}$$

Também $\varphi_p(\langle \bar{b}c^2\rangle) = \varphi_p(\langle \bar{a}\rangle) = \langle pa\rangle + L_{p-1}$.

Logo φ_p respeita i).

Para mostrarmos que φ_p respeita ii), tomemos $ab\ (a + b) \equiv c \pmod p$.

Observamos que sempre podemos tomar a e b tais que $a + b < p$, pois se $a + b = p$ então $\bar{a} + \bar{b} = 0$ e a relação é respeitada.

Temos então que

$$\langle pa\rangle + \langle pb\rangle = \langle p(a+b)\rangle + \langle p(a+b)ab\rangle \equiv \langle p(a+b)\rangle + \langle pc\rangle \pmod{L_{p-1}}$$

pelo lema 3.

Assim

$$\varphi_p\ (\langle \bar{a}\rangle + \langle \bar{b}\rangle) = \langle pa\rangle + \langle pb\rangle + L_{p-1} = \langle p(a+b)\rangle + \langle pc\rangle + L_{p-1}$$

Agora

$$\varphi_p(\langle\bar{a}+\bar{b}\rangle+\langle\overline{a\bar{b}}(\bar{a}+\bar{b})\rangle) = \varphi_p(\langle\overline{a+b}\rangle+\langle\bar{c}\rangle) = \langle p(a+b)\rangle+\langle pc\rangle+L_{p-1}$$

Logo φ_p respeita ii).

Observemos também que

$$\varphi_p(\langle\bar{1}\rangle) = \langle p\rangle + L_{p-1} \text{ e}$$

$$\varphi_p(\langle-\bar{1}\rangle) = \langle -p\rangle + L_{p-1}$$

Então

$$\varphi_p(\langle\bar{1}, -\bar{1}\rangle) = \langle p, -p\rangle + L_{p-1} = \langle 1, -1\rangle + L_{p-1}$$

e assim a terceira condição também é respeitada.

Da primeira parte do lema anterior, concluimos que é sobrejetora. Além disso, o homomorfismo δ_p induz outro homomorfismo $\bar{\delta}_p : L_p|L_{p-1} \longrightarrow W(F_p)$ que satisfaz $\bar{\delta}_p\,\varphi_p(\langle\bar{a}\rangle) = \bar{\delta}_p(\langle pa\rangle) = \langle\bar{a}\rangle$ e $\varphi_p\bar{\delta}_p(\langle pa\rangle) = \varphi_p(\langle\bar{a}\rangle) = \langle pa\rangle$. Logo φ_p e $\bar{\delta}_p$ são isomorfismos inversos.

Na sequência

$$0 \longrightarrow Z \xrightarrow{\ i\ } W(Q) \xrightarrow{\ \oplus\,\delta_p\ } Z/2Z \oplus \sum_{p\neq 2}^{\oplus} W(F_p) \longrightarrow 0$$

vemos que i é injetora, pois se $x \in \ker i$, $x \in Z$ e

$$i(x) = i(1+1+\ldots+1) = i(1) + i(1) + \ldots + i(1) = xi(1) = x\langle 1\rangle$$

Assim $x\langle 1\rangle = 0$ nos leva $x = 0$. Ainda mais $\text{imi} = Z\langle 1\rangle = L_1$, como visto anteriormente.

Agora $\text{imi} \subset \ker \oplus \delta_p$ pois

$$\delta_p(m\langle 1\rangle) = \delta_p(\langle 1, 1, \ldots, 1\rangle) = 0 \quad \text{para m positivo e}$$

$$\delta_p(m\langle 1\rangle) = \delta_p(\langle -1, -1, \ldots, -1\rangle) = 0 \quad \text{para m negativo}$$

Para mostrarmos que $\ker \oplus \delta_p \subset \text{imi} = L_1$ verificaremos primeiramente que

$$\oplus_{p\leq q} \bar{\delta}_p : L_q / L_1 \longrightarrow Z_2 \oplus \sum_{2<p\leq q}^{\oplus} W(F_p)$$

é um isomorfismo para todo primo q.

Para $q = 2$ isso já foi observado anteriormente.

Por indução, vamos supor que vale para todo primo menor ou igual a q. Seja então r o próximo primo maior que q. No diagrama comutativo abaixo, vemos que as funções dos flancos são isomorfismos, assim, pelo Lema dos Cinco, a função do centro também é um isomorfismo.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L_{r-1}/L_1 & \longrightarrow & L_r/L_1 & \longrightarrow & L_r/L_{r-1} & \longrightarrow & 0 \\
 & & \downarrow \oplus\bar{\delta}_p & & \downarrow & & \downarrow \delta_r & & \\
0 & \longrightarrow & Z/2Z \oplus \sum_{2<p\leq q} W(F_p) & \longrightarrow & Z/2Z \oplus \sum_{2<p\leq r} W(F_p) & \longrightarrow & W(F_r) & \longrightarrow & 0
\end{array}$$

Supondo que exista uma forma qudrática q em $\ker \oplus \delta_p$ com $q \notin L_1$, teremos que $q \in L_p$, para algum $p \neq 1$, pois $W(Q) = \bigcup_q L_q$, logo $\bar{\delta}_p(q) \neq 0$ e assim $\delta_p(q) \neq 0$. Absurdo, pois $q \in \ker \oplus \delta_p$.

Concluímos então que $\text{im}\, i = \ker \oplus \delta_p$, isto é, a sequência em questão é exata.

Para mostrarmos que a sequência é cindida consideremos:

$$j : W(Q) \longrightarrow W(R) \text{ com } j(\langle a \rangle_Q) = \langle a \rangle_R,$$

$$s : W(R) \longrightarrow Z \quad \text{a função assinatura e}$$

$$t = s \circ j : W(Q) \longrightarrow Z$$

Vemos então que $t \circ i = id$. Portanto a sequência cinde.

A importância do que foi feito acima está no fato de que agora passamos a conhecer a estrutura de W(Q) como grupo aditivo, pois o término da demonstração, conseguimos mostrar que

$$W(Q) \cong Z \oplus Z/_{2Z} \oplus \sum_{p \neq 2} W(F_p)$$

Um resultado importante decorrente do teorema acima é:

Corolário (Princípio Local - Global Fraco) - Seja q uma forma quadrática sobre Q. Se q é hiperbólica sobre todo completamento de Q

então q é hiperbólica sobre Q.

Demonstração: Tomando q hiperbólica sobre Q_p teremos:

i) para $p \neq 2$, $\delta_p(p) = 0$ para todo p, ou seja,

$$q \in \ker \oplus \delta_p = L_1$$

ii) para $p = 2$, q é equivalente a uma forma hiperbólica q' sobre Q_2, logo existe uma matriz inversível M tal que $M_q = M^t M_{q'} M$. Assim $\det M_q = (\det M)^2 \det M_{q'}$. Como $\det M_{q'} = (-1)^r$, r inteiro positivo, vem que

$$\delta_2(q) = v_2(\det M_q)(\mathrm{mod}\ 2) = 2v_2(\det M)(\mathrm{mod}\ 2) = 0$$

De i) e ii) segue que $q \in \ker \oplus \delta_p = L_1$, para todo p.

Do fato da sequência apresentada no teorema 3 cindir, temos que $(i \circ s) = id_{WQ}$, onde s é a assinatura. Agora q é hiperbólica sobre R, logo $s(q) = 0$ e consequentemente $q = (i \circ s)(q) = i(0) = 0$, provando assim o corolário.

BIBLIOGRAFIA

H - Harrison, D. K. *Witt Rings (Notes by Joel Cunninghan).* University of Kentucky, 1970.

L - Lam, T. Y. *The Algebraic Theory of Quadratic Forms.* Mathemathics Lecture Notes Serie, Benjamin, U.S.A., 1973.

R - Ribenboin, P. *L'Arithmétique Des Corps*, Paris, Hermann, 1972.

S - Scharlaw, W. *Quadratic Forms.* Queen's Paper on Pure an Applied Mathematics, nº 22, Queen's University, Kingston, 1969.

Z - Zariski, O. & Samuel P. *Commutative Algebra.* New York, Springer, 1979.