SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito... 17/03/99

Assinatura:.....

Unidades em Anéis de Witt

ALEXANDRA YATSUDA FERNANDES BRESCANSIN

Orientadora: PROF^a. DR^a. IRES DIAS

Dissertação apresentada ao Instituto de Ciências Matemáticas de São Carlos-USP, como parte dos requisitos para obtenção do título de "Mestre em Ciências - Área: Matemática".

USP - São Carlos

1999

“À minha família.”

Agradecimentos

À Deus pela vida e pela fé;

À minha orientadora Ires, que acreditou em mim e me apoiou em todos os momentos;

À minha querida filha Lívia, pela compreensão nos momentos de ausência;

Ao meu amado esposo Beto, fonte de alegria, onde sempre renovei minhas esperanças;

À Vilma, minha mãe, e à Dalva e Geraldo, meus sogros, que me apoiaram e proporcionaram a tranquilidade necessária, cuidando de minha filha, durante minha permanência em São Carlos;

Aos meus colegas, novos e antigos, pelo companheirismo, em especial aos meus queridos amigos Adriana, Ana, Nelson, Regilene, Sadao e Simone, com os quais aprendi o verdadeiro sentido da palavra compartilhar;

À Rosali, pela atenção dispensada e sugestões em algumas dúvidas;

Ao CNPQ pelo custeio parcial de meus estudos de pós-graduação;

Aos meus professores da UEM e do ICMC e à todos aqueles que direta ou indiretamente colaboraram na elaboração desta dissertação.

Resumo

Neste trabalho apresentamos um estudo sobre as unidades no anel de Witt dos espaos bilineares sobre um anel local, generalizando os resultados apresentados por Lewis em [7].

Abstract

In this work we give a study about the units in the Witt ring of the bilinear spaces over a local ring, generalizing the results presented by Lewis in [7].

Índice

Introdução	1
1 Espaços Bilineares	3
1.1 Preliminares	3
1.2 $\text{Bil}(A)$	8
1.3 O Teorema do Cancelamento de Witt e o Conjunto de Valores.	17
1.4 Espaços Metabólicos e Hiperbólicos	25
2 O Anel de Witt	35
2.1 Geradores de $W(A)$	35
2.2 Os ideais primos de $W(A)$	40
2.3 $\text{Nil}(W(A))$ e $W_t(A)$	46
3 As unidades no Anel de Witt	53
Referências Bibliográficas	69

Introdução

A teoria algébrica das formas quadráticas sobre corpos, teve origem em 1937 com um trabalho de Ernst Witt, onde ele teve a brilhante idéia de considerar não só o estudo de uma forma quadrática em particular, mas sim o conjunto de todas as formas quadráticas sobre um dado corpo e com este conjunto, construir um anel, o anel de Witt, que é o principal objeto de toda a teoria. A partir daí, todo o estudo de classificação de formas quadráticas se resume ao estudo da estrutura deste anel. Os excelentes livros de W. Scharlau[11] e M. Marshall [8] contém grande parte dos artigos recentes publicados nesta direção.

Em [7], D. W. Lewis apresenta vários resultados sobre as unidades (elementos inversíveis) do anel de Witt dos espaços bilineares sobre um corpo de característica distinta de 2. Nosso propósito, neste trabalho, é apresentar generalizações destes resultados para espaços bilineares sobre um anel local, na medida do possível, não assumindo que 2 é inversível no anel.

Para tanto, no capítulo I, apresentamos as noções básicas sobre espaços bilineares sobre anéis locais necessárias para a compreensão do restante do trabalho.

No capítulo II introduzimos o anel de Witt dos espaços bilineares sobre um anel local A , $W(A)$, e uma descrição completa de seus geradores e ideais primos. Apresentamos também resultados sobre elementos nilpotentes, elementos de torção e espaços de Pfister, importantes para o desenvolvimento do próximo capítulo.

O último capítulo, consiste do que nos propomos a desenvolver no projeto, ou seja, as generalizações dos resultados de Lewis para espaços bilineares sobre anéis locais.

Capítulo 1

Espaços Bilineares

Neste capítulo apresentaremos alguns fatos básicos de álgebra comutativa necessários para a compreensão do restante do trabalho. Algumas demonstrações serão omitidas, as quais podem ser encontradas na literatura, como por exemplo em [1]. Apresentamos também noções básicas sobre espaços bilineares sobre anéis locais, como por exemplo, teoremas de decomposição de espaços bilineares e o teorema do cancelamento de Witt.

Em todo este trabalho os anéis considerados serão comutativos e com elemento identidade 1. Os módulos sobre tais anéis serão unitários. Todo homomorfismo de anéis leva elemento identidade em elemento identidade.

1.1 Preliminares

Sejam A um anel comutativo e $\text{Spec}(A)$ o conjunto de todos os ideais primos de A . Temos então

Proposição 1.1 *O conjunto de todos os elementos nilpotentes em um anel A é igual a intersecção de todos os ideais primos de A .*

Dem.: Ver (1.8) de [1]. ■

Sejam A^* o grupo das unidades de A e $\text{Max}(A)$ o conjunto dos ideais maximais de A . É imediato que $A^* = A - \bigcup_{\mathcal{M} \in \text{Max}(A)} \mathcal{M}$.

Corolário 1.2 *Se a é um elemento nilpotente de A , então $1 + a \in A^*$.*

Dem.: Se $1 + a$ não é uma unidade, temos que $1 + a \in \mathcal{M}$, para algum $\mathcal{M} \in \text{Max}(A)$. Como a é um elemento nilpotente, por (1.1), temos que a está na intersecção de todos os ideais primos de A . Em particular, $a \in \mathcal{M}$. Desta forma $1 = (1 + a) - a \in \mathcal{M}$, o que é um absurdo. Portanto $1 + a \in A^*$. ■

Proposição 1.3 *O conjunto dos divisores de zero de um anel A é uma união de ideais primos.*

Dem.: Ver página 3 de [4]. ■

Seja A um anel. Uma seqüência de A -módulos e A -homomorfismos

$$\dots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \dots$$

é dita ser *exata em M_i* se $\text{Im}(f_i) = \text{Ker}(f_{i+1})$. Se a seqüência é exata em cada M_i , então dizemos que ela é uma *seqüência exata*.

Uma seqüência exata do tipo $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$, é chamada uma *seqüência exata curta*.

Dizemos que uma seqüência exata

$$\dots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \dots$$

cinde em M_i , se o submódulo $X = \text{Im}(f_i) = \text{Ker}(f_{i+1})$ de M_i é um somando direto de M_i . No caso de uma seqüência exata curta $0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$, obviamente temos que ela cinde em X e Z . Se, além disso, a seqüência cinde em Y , dizemos apenas que a seqüência *cinde*.

Proposição 1.4 *Se uma seqüência exata curta de A -módulos*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

cinde, então Y é isomorfo, como A -módulo, à $X \oplus Z$ ($Y \cong X \oplus Z$).

Dem.: Desde que a seqüência exata $0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$ cinde, temos que X é um somando direto de Y , ou seja $Y = X \oplus W$, para algum A -módulo W . Temos, também que $X = \text{Im}(f) = \text{Ker}(g)$. Assim, desde que g é sobrejetor, temos:

$$\frac{Y}{\text{Ker}(g)} \cong \text{Im}(g) = Z.$$

Portanto, Z é isomorfo ao complementar de X em Y , ou seja, $Z \cong W$ como A -módulos. Assim $Y = X \oplus W \cong X \oplus Z$, como queríamos. ■

Seja M um A -módulo. Dizemos que M é um A -módulo *livre* se ele possuir uma base.

Um A -módulo P é dito ser um A -módulo *projetivo* se satisfaz uma das seguintes condições equivalentes:

- (a) P é somando direto de um A -módulo livre.
- (b) Toda seqüência exata curta de A -módulos $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$, cinde.
- (c) Para toda seqüência exata curta de A -módulos $0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$, a seqüência de A -módulos $0 \longrightarrow \text{Hom}(P, X) \longrightarrow \text{Hom}(P, Y) \longrightarrow \text{Hom}(P, Z) \longrightarrow 0$ é exata.

É imediato que todo A -módulo livre é também projetivo.

Um anel comutativo A , com elemento identidade 1, é dito ser um *anel local*, se satisfaz uma das seguintes condições equivalentes:

- (a) A tem um único ideal maximal $\mathcal{M}$.
- (b) As não-unidades de A formam um ideal próprio de A .
- (c) Para cada $a \in A$, a ou $1 - a$ é uma unidade.

Se A é um anel local e $\mathcal{M}$ é seu único ideal maximal, então o corpo $K = \frac{A}{\mathcal{M}}$ é chamado o *corpo das classes residuais de A* . Denotamos a projeção canônica de A em K por $\bar{}$.

Exemplo 1.5 O anel quociente $\frac{\mathbb{Z}}{(p^n)}$, onde p é um número primo, é um anel local com único ideal maximal $\frac{(p)}{(p^n)}$. De fato, os ideais em $\frac{\mathbb{Z}}{(p^n)}$ são da forma $\frac{(m)}{(p^n)}$ com $(m) \supseteq (p^n)$. Então $m = p^k$ com $k \leq n$ e, assim os ideais em $\frac{\mathbb{Z}}{(p^n)}$ são os ideais $\frac{(p^k)}{(p^n)}$ com $k \leq n$. Usando a correspondência entre ideais temos que

$$\frac{(p)}{(p^n)} \supseteq \frac{(p^2)}{(p^n)} \supseteq \dots \supseteq \frac{(p^{n-1})}{(p^n)} \supseteq \frac{(p^n)}{(p^n)}.$$

Portanto $\frac{(p)}{(p^n)}$ é o único ideal maximal de $\frac{\mathbb{Z}}{(p^n)}$.

Agora estamos interessados em mostrar que todo módulo projetivo finitamente gerado sobre um anel local é livre. Para tanto usaremos o seguinte lema auxiliar

Lema 1.6 *Se P é um A -módulo projetivo finitamente gerado, então existe um A -módulo finitamente gerado N tal que $P \oplus N \cong A^n$, para algum $n \in \mathbb{N}$.*

Dem.: Como P é um A -módulo projetivo, existe um A -módulo N_0 , tal que $P \oplus N_0 = L$, onde L é um A -módulo livre, com uma base $\{x_i\}_{i \in I}$. Sendo P finitamente gerado existe um subconjunto finito J de I tal que $P \subseteq L_0 := \sum_{i \in J} Ax_i$. Assim $L_0 = P + (N_0 \cap L_0)$, pois $L_0 = L \cap L_0 = (P + N_0) \cap L$. Tomando $N = N_0 \cap L_0$, temos que $L_0 = P \oplus N$, pois $P \cap N \subseteq P \cap N_0 = \{0\}$. Mas, $N \cong \frac{L_0}{P}$ é finitamente gerado, pois P e L_0 são finitamente gerados. Agora, como A -módulos $L_0 \cong A^n$, pois $L_0 = \sum_{i \in J} Ax_i \cong \sum_{i \in J} A \cong A^n$, onde n é o número de elementos de J . Portanto $P \oplus N \cong A^n$, para algum $n \in \mathbb{N}$. ■

No que segue, exceto menção em contrário, A denotará um anel local, $\mathcal{M}$ seu único ideal maximal, e todos os módulos considerados serão A -módulos.

Teorema 1.7 *Todo módulo projetivo finitamente gerado sobre um anel local é livre.*

Dem.: Sejam A um anel local e P um módulo projetivo finitamente gerado sobre A . Então, pelo lema anterior, existe um módulo finitamente gerado N tal que $P \oplus N \cong A^n$, para algum $n \in \mathbb{N}$. Seja $\{x_1, \dots, x_n\}$ uma base de $P \oplus N$ sobre A . Tensorizando por $K = A/\mathcal{M}$, temos que

$$(P \oplus N) \otimes K \cong (P \otimes K) \oplus (N \otimes K) \cong \overline{P} \oplus \overline{N} \cong (A^n \otimes K) \cong K^n,$$

que é um espaço vetorial de dimensão n sobre o corpo K .

Seja $\{\overline{y}_1, \dots, \overline{y}_m, \overline{y}_{m+1}, \dots, \overline{y}_n\}$ uma base de $\overline{P} \oplus \overline{N}$ sobre K , tal que $\{\overline{y}_1, \dots, \overline{y}_m\}$ é uma base de $\overline{P}$ e $\{\overline{y}_{m+1}, \dots, \overline{y}_n\}$ é uma base de $\overline{N}$ sobre K .

Se $B = (b_{ij})$ com $y_i = \sum_{j=1}^n x_j b_{ij}$, então $\overline{B} = (\overline{b_{ij}}) \in M_n(K)$ e $\overline{y}_i = \sum_{j=1}^n \overline{x}_j \overline{b_{ij}}$. Como $\{\overline{y}_1, \dots, \overline{y}_n\}$ e $\{\overline{x}_1, \dots, \overline{x}_n\}$ são bases de $\overline{P} \oplus \overline{N}$ sobre K , temos que $\overline{B}$ é uma matriz de mudança de base. Assim, $\det \overline{B} \neq 0$ em K o que implica que $\det B \in A - \mathcal{M} = A^*$, ou seja, $\{y_1, \dots, y_n\}$ é também uma base de $P \oplus N$ sobre A . Consequentemente, $\{y_1, \dots, y_m\}$ é uma base de P , ou seja P é um módulo livre. ■

Finalizamos esta seção com um resultado de teoria dos números que nos será útil no último capítulo.

Teorema 1.8 *Sejam i e r inteiros positivos com $2^i \leq r < 2^{i+1}$ e k um inteiro positivo. Então o coeficiente binomial*

$$\binom{2^k}{r}$$

é divisível por 2^{k-i} .

Dem.: Para todo $r > 0$, $r \in \mathbb{N}$, podemos escrever $r = 2^s q$, onde q é um número inteiro ímpar. Se r é ímpar, tomemos $s = 0$. Temos então

$$\binom{2^k}{r} = \frac{2^{k-s}(2^k - 1)(2^k - 2) \cdots (2^k - (r - 1))}{1 \cdot 2 \cdot 3 \cdots (r - 1)q}.$$

Como por hipótese $2^i \leq 2^s q < 2^{i+1}$, onde q é um número inteiro positivo ímpar, temos que $2^s \leq 2^i$, ou seja, $2^{k-s} \geq 2^{k-i}$. Assim, é suficiente mostrarmos que

$$s = \frac{(2^k - 1)(2^k - 2) \cdot \dots \cdot (2^k - (r - 1))}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (r - 1)q}$$

é um número inteiro. Para tanto, mostraremos que todas as potências de 2 que aparecem no denominador são canceladas por fatores do numerador.

Isto segue do fato que se $m < r$ é um inteiro par, então a potência de dois que divide m também divide $(2^k - m)$. De fato, se $m = 2^t n$ com n um inteiro ímpar, então $2^t n < r \leq 2^k$ e, conseqüentemente, $2^t < 2^k$, ou seja $k - t > 0$. Como $2^k - m = 2^t(2^{k-t} - n)$ temos que 2^t divide $(2^k - m)$. Portanto s é um número inteiro e, 2^{k-i} divide $\binom{2^k}{r}$, como queríamos. ■

1.2 Bil(A)

Em geral, a teoria de formas quadráticas sobre anéis é feita na categoria dos módulos projetivos finitamente gerados de posto constante. Como vimos em (1.7), quando A é um anel local, todo A -módulo projetivo finitamente gerado é livre. Assim, no que segue, em toda esta dissertação trabalharemos com a categoria dos A -módulos livres de dimensão finita, onde os morfismos são homomorfismos de A -módulos. Denotamos esta categoria por $L(A)$.

Definição 1.9 O par (M, b) consistindo de um módulo $M \in L(A)$ e uma forma bilinear simétrica $b : M \times M \rightarrow A$ é chamado um *módulo bilinear* sobre A . Um módulo bilinear (M, b) é dito ser *não-singular*, ou simplesmente um *espaço bilinear*, se a função A -linear $d : M \rightarrow M^*$, definida por $d(x) = b(x, \cdot)$, para todo $x \in M$, é um isomorfismo de A -módulos. Se o A -módulo M tem dimensão n , ou seja, M tem uma base com n elementos, dizemos que o módulo bilinear (M, b) tem dimensão n e

indicamos por $\dim b = n$ ou ainda $\dim M = n$. Uma *isometria* entre dois módulos bilineares (M_1, b_1) e (M_2, b_2) é um isomorfismo de A -módulos $\varphi : M_1 \rightarrow M_2$, que preserva a forma bilinear, ou seja, $b_1(x, y) = b_2(\varphi(x), \varphi(y))$, para todo $x, y \in M_1$. Quando existe uma isometria entre (M_1, b_1) e (M_2, b_2) dizemos que os módulos bilineares são *isométricos* e denotamos por $(M_1, b_1) \simeq (M_2, b_2)$, ou simplesmente $b_1 \simeq b_2$, ou ainda $M_1 \simeq M_2$.

Se (M, b) é um módulo bilinear sobre A e $\{x_1, \dots, x_n\}$ é uma base de M , então a forma bilinear b é unicamente determinada pela matriz quadrada $B = (b_{ij}) = (b(x_i, x_j))$, $1 \leq i, j \leq n$, pois para $x = \sum_{i=1}^n \alpha_i x_i$ e $y = \sum_{j=1}^n \beta_j x_j$ em $M = \bigoplus_{i=1}^n A x_i$ temos $b(x, y) = \sum_{i,j=1}^n b_{ij} \alpha_i \beta_j$. Em termos matriciais temos que, se

$$X = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \text{e} \quad Y = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

são os vetores coordenadas de x e y em relação à base dada, então $b(x, y) = X^t B Y$, onde X^t é a matriz transposta de X . Reciprocamente, para cada matriz simétrica $n \times n$ sobre A , (b_{ij}) , obtemos uma forma bilinear simétrica sobre M dada pela mesma fórmula descrita acima e, o módulo bilinear (M, b) é não-singular se, e somente se $\det(b_{ij})$ é uma unidade em A .

O determinante da matriz (b_{ij}) é chamado *determinante* do espaço bilinear b e denotado por $\det b$. No que segue, identificaremos um elemento $x \in M$, com o vetor das coordenadas de x em relação a uma dada base de M . Mais ainda, como um módulo (M, b) é caracterizado por uma matriz quadrada (b_{ij}) , usaremos também a notação $b = (b_{ij})$ para indicarmos a forma bilinear b .

Sejam (M_1, b_1) e (M_2, b_2) , espaços bilineares isométricos com (a_{ij}) e (b_{ij}) suas respectivas matrizes em relação a algum par de bases dado. Se $\varphi : (M_1, b_1) \rightarrow (M_2, b_2)$ é uma isometria, então φ é unicamente determinada por uma matriz inversível C , ou

seja, $\varphi(x) = Cx$, para todo $x \in M_1$. Como $b_1(x, y) = x^t(a_{ij})y$ e

$$b_2(\varphi(x), \varphi(y)) = \varphi(x)^t(b_{ij})\varphi(y) = (Cx)^t(b_{ij})Cy = x^tC^t(b_{ij})Cy$$

para todo $x, y \in M_1$, temos que $(a_{ij}) = C^t(b_{ij})C$, ou seja, as matrizes (a_{ij}) e (b_{ij}) são semelhantes.

Reciprocamente, se existe uma matriz inversível C tal que $(a_{ij}) = C^t(b_{ij})C$, então podemos considerar o isomorfismo $\varphi : M_1 \rightarrow M_2$ tal que $\varphi(x) = Cx$, para todo $x \in M_1$. Assim, para $x, y \in M_1$,

$$b_2(\varphi(x), \varphi(y)) = x^tC^t(b_{ij})Cy = x^t(a_{ij})y = b_1(x, y)$$

e, portanto $(M_1, b_1) \simeq (M_2, b_2)$. Segue imediatamente deste fato que o determinante das matrizes associadas à espaços bilineares isométricos diferem por quadrados.

Denotamos a categoria dos espaços bilineares sobre A por $\mathbf{Bil}(A)$, onde os morfismos são as isometrias. Em $\mathbf{Bil}(A)$ vamos definir duas operações, uma soma e um produto.

Definição 1.10 Definimos a *soma ortogonal* dos espaços $(M_i, b_i) \in \mathbf{Bil}(A)$, $(i = 1, 2)$ como sendo o módulo bilinear:

$$(M_1, b_1) \perp (M_2, b_2) = (M_1 \oplus M_2, b_1 \perp b_2),$$

onde $(b_1 \perp b_2)(x_1 \oplus x_2, y_1 \oplus y_2) = b_1(x_1, y_1) + b_2(x_2, y_2)$, para todo $x_i, y_i \in M_i (i = 1, 2)$.

É fácil ver que $(M_1 \oplus M_2, b_1 \perp b_2)$ é de fato um espaço bilinear sobre A . Denotamos este espaço simplesmente por $b_1 \perp b_2$.

Definimos o *produto tensorial* dos espaços $(M_i, b_i) \in \mathbf{Bil}(A)$ $(i = 1, 2)$, como sendo o módulo bilinear:

$$(M_1, b_1) \otimes (M_2, b_2) = (M_1 \otimes M_2, b_1 \otimes b_2),$$

onde $(b_1 \otimes b_2)(x_1 \otimes x_2, y_1 \otimes y_2) = b_1(x_1, y_1)b_2(x_2, y_2)$, para todo $x_i, y_i \in M_i (i = 1, 2)$. Novamente, pode-se ver que este módulo é não-singular, ou seja, é de fato um espaço bilinear sobre A . Denotamos este espaço por $b_1 \otimes b_2$.

Mostra-se facilmente que essas duas operações são associativas, comutativas e que o produto tensorial é distributivo em relação a soma ortogonal. Além disso, as duas operações são compatíveis com a relação de isometria, ou seja, se $b_1 \simeq b_2$ e $b'_1 \simeq b'_2$, então

$$b_1 \perp b'_1 \simeq b_2 \perp b'_2 \quad \text{e} \quad b_1 \otimes b'_1 \simeq b_2 \otimes b'_2.$$

Exemplo 1.11 Sejam $M = Ax$ e $b : M \times M \rightarrow A$ definida por $b(\beta x, \gamma x) = \beta \gamma b(x, x) = \beta \gamma \alpha$, para todo $\beta, \gamma \in A$, onde $\alpha \in A$. Neste caso temos que b é não-singular se, e somente se $\alpha \in A^*$. Denotaremos esta forma bilinear b , simplesmente por $\langle \alpha \rangle$. Mais geralmente, $b = \langle \alpha_1 \rangle \perp \dots \perp \langle \alpha_n \rangle$ será denotado por $\langle \alpha_1, \dots, \alpha_n \rangle$.

Um submódulo U de M é dito ser um *subespaço* de (M, b) , se U é um somando direto de M , ou seja, se existe um submódulo $V \subseteq M$, tal que $M = U \oplus V$. Se x é um elemento de M tal que Ax é um subespaço de M , dizemos que x é um *elemento primitivo* de M .

Seja (M, b) um módulo bilinear. Para todo subconjunto U de M o conjunto

$$U^\perp = \{x \in M; b(x, y) = 0, \text{ para todo } y \in U\},$$

é um submódulo de M , chamado o *complemento ortogonal* de U em relação à b . Dizemos que dois subconjuntos U, V de M são *ortogonais* se $U \subseteq V^\perp$ ou, equivalentemente, $V \subseteq U^\perp$. Com esta terminologia temos o seguinte lema de imediata verificação.

Lema 1.12 (i) Se $V \subseteq U \subseteq M$, então $U^\perp \subseteq V^\perp$.

(ii) $U \subseteq U^{\perp\perp}$.

(iii) $U^\perp = U^{\perp\perp\perp}$.

Dem.: Imediata. ■

Se (M, b) é um módulo bilinear com $M = U \oplus V$ e $U \subseteq V^\perp$, dizemos que M é a soma ortogonal de U e V e denotamos por $M = U \perp V$. Denotaremos por $(U, b|_U)$ a restrição da forma bilinear b ao submódulo $U \subseteq M$. É imediato que se $M = U \perp V$, então $(M, b) \simeq (U, b|_U) \perp (V, b|_V)$.

Um subconjunto $U \subseteq M$ é dito ser *totalmente isotrópico* se $U \subseteq U^\perp$. Dizemos que um elemento $x \in M$ é *isotrópico* se $Ax \subseteq M$ é um subespaço totalmente isotrópico de M , ou seja, se x é um elemento primitivo de M tal que $b(x, x) = 0$. Um elemento $y \in M$ é dito ser *anisotrópico* se $Ay \subseteq M$ é um subespaço de M com $b(y, y) \in A^*$, ou seja, se y é um elemento primitivo de M tal que $b(y, y) \in A^*$. Dizemos também que o espaço bilinear (M, b) é um *espaço bilinear isotrópico* se M contém um elemento isotrópico. Se todos os elementos de M são anisotrópicos dizemos que (M, b) é um *espaço bilinear anisotrópico*.

Em relação à soma de subespaço temos

Proposição 1.13 *Seja (M, b) um módulo bilinear sobre A .*

(i) *Se M é não-singular e $U \subseteq M$ é um subespaço, então $U^\perp$ é também um subespaço de M e $U = U^{\perp\perp}$.*

(ii) *Seja $U \subseteq M$ um submódulo tal que $(U, b|_U)$ é não singular. Então U é um subespaço de M e $M = U \perp U^\perp$.*

Dem.: Desde que U é um somando direto do módulo livre M , temos a seqüência exata $M^* \longrightarrow U^* \longrightarrow 0$. Como (M, b) é não-singular, temos que $d : M \rightarrow M^*$ é um isomorfismo. Compondo este isomorfismo com a seqüência acima obtemos a seqüência exata $M \longrightarrow U^* \longrightarrow 0$. Observemos também que o núcleo da composta $d : M \rightarrow U^*$ é exatamente $U^\perp$. Agora, U^* é projetivo, pois é somando direto do A -módulo livre M^* . Portanto a seqüência exata curta

$$0 \longrightarrow U^\perp \longrightarrow M \longrightarrow U^* \longrightarrow 0$$

cinde, ou seja, $M \cong U^\perp \oplus U^*$. O que mostra que $U^\perp$ é um subespaço de M .

Mostremos agora que $U^\perp = U^{\perp\perp}$. Para simplificar a notação, denotaremos também por b as restrições ou aplicações induzidas da forma bilinear b a subespaços ou quociente de M e por d as restrições ou aplicações induzidas por d a subespaços ou quocientes de M . O isomorfismo $d : \frac{M}{U^\perp} \rightarrow U^*$ induz uma forma bilinear não-singular $b : U \times \frac{M}{U^\perp} \rightarrow A$, para todo subespaço U de M . Em particular, para o subespaço $U^\perp$ temos uma forma bilinear não-singular $b : U^\perp \times \frac{M}{U^{\perp\perp}} \rightarrow A$. Por outro lado, temos o isomorfismo $M \cong (U^\perp)^* \oplus U$ que decorre dos isomorfismos

$$M^* \cong (U^\perp)^* \oplus U^{**}, \quad d : M \rightarrow M^* \quad \text{e} \quad U^{**} \cong U.$$

Assim obtemos o isomorfismo $d : \frac{M}{U} \rightarrow (U^\perp)^*$ que induz a função bilinear não-singular $b : U^\perp \times \frac{M}{U} \rightarrow A$. Destas duas bilineares e do fato que $U \subseteq U^{\perp\perp}$, segue que $U = U^{\perp\perp}$. Pois se $U \neq U^{\perp\perp}$, então existe $y \in U^{\perp\perp} - U$ primitivo. Da primeira forma bilinear obtida segue que $b(x, y) = 0$, para todo $x \in U^\perp$. Da segunda bilinear temos que existe $x \in U^\perp$ tal que $b(x, y) \in A^*$, pois b é não-singular e y é primitivo, o que é uma contradição. Portanto $U = U^{\perp\perp}$, o que mostra (i).

Agora, se $(U, b|_U)$ é um subespaço não-singular de M , então $d : U \rightarrow U^*$ é um isomorfismo. Mas, todo elemento $x \in M$ define um elemento x^* em U^* por $x^*(y) = b(x, y) = d(x)$, para todo $y \in U$.

Como $d : U \rightarrow U^*$ é sobrejetora, temos que existe $z \in U$ tal que $d(z) = d(x)$, ou seja $b(z, y) = b(x, y)$, para todo $y \in U$. Assim $x - z \in U^\perp$ e, como $x = z + (x - z)$, temos que $M = U + U^\perp$. Do fato de $d : U \rightarrow U^*$ ser injetora segue que $\{0\} = \text{Ker}(d|_U) = \text{Ker}(d) \cap U = U^\perp \cap U$. Assim $M = U \oplus U^\perp$ que, junto com o fato de $U \subseteq U^{\perp\perp}$ mostra o item (ii). ■

Proposição 1.14 *Sejam M um espaço bilinear sobre A e U um subespaço totalmente isotrópico maximal de M , isto é, $U = U^\perp$. Então existe um subespaço V de M tal que $U \cong V^*$ e $M = U \oplus V$.*

Dem.: Pela demonstração do item (i) da proposição anterior, temos que

$$M \cong U^\perp \oplus U^*.$$

Tomando $V = U^*$ temos $V^* = U^{**} \cong U$ e, como $U = U^\perp$, obtemos $M \cong U \oplus V$, como queríamos. ■

Finalizaremos esta seção, mostrando que todo espaço bilinear sobre um anel local admite uma decomposição como soma ortogonal de subespaços de dimensão ≤ 2 . Para tanto, iniciaremos com algumas definições e resultados auxiliares.

Dado $(M, b) \in \mathbf{Bil}(A)$, considere o subconjunto $\{b(x, x); x \in M\}$ de A . Se o ideal gerado por este subconjunto é todo o anel A , diremos que o espaço bilinear (M, b) é *próprio*. Caso contrário, dizemos que (M, b) é um espaço bilinear *impróprio*.

Como A é um anel local, dizer que $(M, b) \in \mathbf{Bil}(A)$ é próprio é equivalente a dizer que existe $x \in M$ tal que $b(x, x)$ é uma unidade em A .

Lema 1.15 *Todo espaço bilinear de dimensão ≥ 2 admite um subespaço de dimensão 2 não-singular.*

Dem.: Seja (M, b) um espaço bilinear sobre A , com $\dim M \geq 2$. Separemos a demonstração em dois casos, quando (M, b) é próprio e quando (M, b) é impróprio.

Se (M, b) é próprio, considere $x \in M$ tal que $b(x, x) \in A^*$. Assim, o subespaço (Ax, b) de (M, b) é não-singular e, de (1.13), temos que $M = (Ax, b) \perp (V_1, b)$ onde $(V_1, b) = ((Ax)^\perp, b)$ é também não-singular.

Se (V_1, b) é próprio, usando o argumento acima, temos que

$$(M, b) = (Ax, b) \perp (Ay, b) \perp (V_2, b),$$

onde V_2 é o complemento ortogonal de Ay em V_1 . Assim o subespaço $(Ax, b) \perp (Ay, b)$ é o subespaço não-singular de dimensão 2 de M procurado.

Se (V_1, b) é impróprio, como (V_1, b) é não-singular e A é local, existem $y, z \in V_1$ tais que $b(y, z) \in A^*$, com $y \neq z$. Tomando $w_1 = x + y$ e $w_2 = x + \lambda z$, onde

$\lambda = -\frac{b(x, x)}{b(y, z)}$, temos que $(Aw_1 \perp Aw_2, b)$ é um subespaço não-singular de (M, b) de dimensão 2, pois a matriz de b com relação a base $\{w_1, w_2\}$ é

$$(b_{ij}) = (b(w_i, w_j)) = \begin{pmatrix} b(x, x) + b(y, y) & 0 \\ 0 & b(x, x) + \lambda^2 b(z, z) \end{pmatrix},$$

que é inversível. Logo, se (M, b) é próprio, (M, b) admite um subespaço não-singular de dimensão 2 da forma $(Aw_1, b) \perp (Aw_2, b)$.

Se (M, b) é impróprio, seja $\{x_1, \dots, x_n\}$ uma base de M . Como b é não-singular, temos que $\det(b_{ij}) = \det(b(x_i, x_j)) \in A^*$. Então, existe $i \neq j$, tal que $b(x_i, x_j) \in A^*$, pois A é um anel local. Assim, tomando $w_1 = x_i$ e $w_2 = x_j$, temos que

$$\det(b(w_i, w_j)) = \det \begin{pmatrix} b_{ii} & b_{ij} \\ b_{ji} & b_{jj} \end{pmatrix} \in A^*.$$

Portanto o subespaço gerado por $\{w_1, w_2\}$ é não-singular, o que mostra o lema. ■

Teorema 1.16 *Seja $(M, b) \in \text{Bil}(A)$.*

(i) *Se (M, b) é próprio, então (M, b) admite uma base ortogonal, ou seja, (M, b) é uma soma ortogonal de subespaços de dimensão 1.*

(ii) *Se (M, b) é impróprio, então (M, b) é uma soma ortogonal de subespaços de dimensão 2 da forma $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$, com $\alpha, \beta \in \mathcal{M}$.*

Dem.: A demonstração do teorema será feita por indução sobre a dimensão de M .

Se $\dim M = 1$, nada há a demonstrar. Assumimos então que $\dim M \geq 2$.

Se (M, b) é próprio, da demonstração do lema anterior e de (1.13) temos que

$$(M, b) = (Aw_1, b) \perp (Aw_2, b) \perp (V_2, b).$$

Considerando $(M_1, b) = (Aw_2, b) \perp (V_2, b)$, temos que (M_1, b) é próprio, pois $b(w_2, w_2)$ é uma unidade. Por hipótese de indução, temos que (M_1, b) admite uma base ortogonal que, juntamente com w_1 , formam uma base ortogonal para (M, b) , o que mostra (i).

Se (M, b) é impróprio, de (1.15) e (1.13) temos que

$$(M, b) = (M_1, b) \perp (M_2, b),$$

onde (M_1, b) é um subespaço não-singular de dimensão 2 de (M, b) .

Como todo subespaço de um espaço bilinear impróprio é também impróprio, temos que (M_2, b) é impróprio. Por hipótese de indução, temos que (M, b) é uma soma ortogonal de subespaços de dimensão 2, ou seja

$$(M, b) = (M_1, b) \perp \cdots \perp (M_r, b), \quad \text{com} \quad \dim M_i = 2, \quad i = 1, \dots, r.$$

Resta apenas verificarmos a forma de cada (M_i, b) . Sejam $\{w_1, w_2\}$ uma base de M_i , com $c_{ij} = b(w_i, w_j)$ e

$$(c_{ij}) = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}.$$

Então $\det(c_{ij}) = c_{11}c_{22} - c_{12}c_{21} \in A^*$, o que implica que $c_{12}c_{21} \in A^*$, pois $c_{11}c_{22} \in \mathcal{M}$ o único ideal maximal de A . Tomando $w'_1 = c_{12}^{-1}w_1$ e $w'_2 = w_2$, temos que a matriz da forma bilinear em relação a esta nova base é

$$\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$$

onde $\alpha = c_{12}^{-2}c_{11}$ e $\beta = c_{22}$ estão em $\mathcal{M}$, o que completa a demonstração do teorema. ■

Corolário 1.17 *Todo espaço bilinear próprio sobre um anel local A é da forma $\langle \alpha_1, \dots, \alpha_n \rangle$, com $\alpha_i \in A^*$, $1 \leq i \leq n$.*

Dem.: Imediata. ■

Observação 1.18 Se $2 \in A^*$, então todo espaço bilinear sobre A é próprio e, consequentemente admite uma base ortogonal. De fato, seja $(M, b) \in \text{Bil}(A)$ impróprio. Como (M, b) é não-singular, temos que existem $x, y \in M$ tais que $b(x, y) \in A^*$ e, como $2 \in A^*$, temos $2b(x, y) \in A^*$. Mas $2b(x, y) = b(x+y, x+y) - b(x, x) - b(y, y) \in \mathcal{M}$, o que é uma contradição. Portanto, se $2 \in A^*$, então (M, b) é próprio.

1.3 O Teorema do Cancelamento de Witt e o Conjunto de Valores.

Nesta seção apresentaremos uma coletânea de resultados sobre espaços bilineares sobre um anel local A , onde estaremos assumindo que 2 é uma unidade em A . Alguns destes resultados não valem sem a hipótese que $2 \in A^*$, outros valem com demonstrações mais laborosas. Como, nesta dissertação, estes resultados serão usados somente quando estivermos assumindo que $2 \in A^*$, em toda esta seção, A será um anel local em que 2 é inversível.

Da observação (1.18) podemos assumir, nesta seção, que todo espaço bilinear sobre A admite uma base ortogonal.

Seja $(M, b) \in \text{Bil}(A)$. Para todo elemento anisotrópico $y \in M$, definimos a aplicação $\tau_y : M \rightarrow M$, por

$$\tau_y(x) = x - \frac{2b(x, y)}{b(y, y)}y, \text{ para todo } x \in M.$$

É fácil ver que τ_y é de fato uma isometria de (M, b) , chamada de *reflexão*.

Lema 1.19 *Sejam $(M, b) \in \text{Bil}(A)$ e $x, y \in M$ elementos anisotrópicos tais que $b(x, x) = b(y, y)$. Então existe um elemento anisotrópico $z \in M$ tal que a reflexão τ_z leva x em y , isto é, $\tau_z(x) = y$.*

Dem.: Como $b(x, x) = b(y, y)$, temos que $b(x+y, x+y) + b(x-y, x-y) = 2b(x, x) + 2b(y, y) = 4b(x, x)$ que é uma unidade em A . Como A é um anel local, $b(x+y, x+y)$

ou $b(x - y, x - y)$ é uma unidade. Assim, trocando y por $-y$ se necessário, podemos assumir que $b(x - y, x - y) \in A^*$, ou seja, $z = x - y$ é um elemento anisotrópico de M e, do fato de,

$$\begin{aligned} b(x - y, x - y) &= b(x, x) + b(y, y) - 2b(x, y) \\ &= 2[b(x, x) - b(x, y)] \\ &= 2b(x, x - y), \end{aligned}$$

temos que

$$\tau_z(x) = \tau_{(x-y)}(x) = x - \frac{2b(x, x - y)}{b(x - y, x - y)}(x - y) = x - (x - y) = y,$$

o que mostra o lema. ■

Nosso próximo propósito é apresentar a versão para anel local da Descrição Indutiva de Isometrias do Marshall. Para tanto necessitaremos de dois resultados auxiliares, um destes para espaços bilineares sobre um corpo de característica diferente de 2.

Lema 1.20 *Sejam K um corpo de característica diferente de 2 e (M, b) um espaço bilinear sobre K . Sejam $x \in M$ um elemento anisotrópico e $y \in (Kx)^\perp$ com $b(y, y) \neq -b(x, x)$. Se γ é um elemento não nulo de K , então existem $\alpha, \beta \in K$, com $\beta \neq 0$ tais que $b(\alpha x + \beta y, \alpha x + \beta y) = \gamma^2 b(x, x)$.*

Dem.: Para todo α e β em K , temos $b(\alpha x + \beta y, \alpha x + \beta y) = \alpha^2 b(x, x) + \beta^2 b(y, y)$. Assim queremos encontrar α e β em K tais que $\alpha^2 b(x, x) + \beta^2 b(y, y) = \gamma^2 b(x, x)$, ou seja, $(\frac{\gamma}{\beta})^2 - (\frac{\alpha}{\beta})^2 = \frac{b(y, y)}{b(x, x)}$.

Seja $d = \frac{b(y, y)}{b(x, x)}$. Por hipótese $d \neq -1$ e, do fato que $2 \neq 0$ em K , podemos escrever $d = (\frac{d+1}{2})^2 - (\frac{d-1}{2})^2$. Agora, os elementos α e β de K tais que $\frac{\gamma}{\beta} = \frac{d+1}{2}$ e $\frac{\alpha}{\beta} = \frac{d-1}{2}$, satisfazem o requerido. ■

Lema 1.21 *Sejam $(M, b) \in \text{Bil}(A)$ com $\dim M \geq 3$, e $x, y \in M$ elementos anisotrópicos. Então existe $z \in M$, anisotrópico, tal que $\tau_z(x) = \alpha y + u$, para algum $\alpha \in A$ e $u \in (Ay)^\perp$ anisotrópico.*

Dem.: Primeiro vamos considerar o caso em que A é corpo. Desde que y é um elemento anisotrópico, de (1.13) podemos escrever $x = \gamma y + v$, onde $\gamma \in A$ e $v \in (Ay)^\perp$. Se v é anisotrópico, tomando $z = y$ temos $\tau_z(x) = -\gamma y + v$, ou seja, $\alpha = -\gamma$ e $u = v$. Se v não é anisotrópico, como A é um corpo, temos que $b(v, v) = 0$. Assim, $b(x, x) = b(\gamma y + v, \gamma y + v) + b(v, v) = \gamma^2 b(y, y) \neq 0$.

Agora, desde que $\dim M \geq 3$, temos que $\dim (Ay)^\perp \geq 2$. Então existem dois elementos y_1 e y_2 em $(Ay)^\perp$ tais que $\{y_1, y_2\}$ está contido em alguma base ortogonal de $((Ay)^\perp, b)$. Se $b(y_i, y_i) = -b(y, y)$, para $i = 1, 2$, então $b(y_1 + y_2, y_1 + y_2) = b(y_1, y_1) + b(y_2, y_2) = -2b(y, y) \neq -b(y, y)$. Com estas considerações, mostramos que existe um elemento anisotrópico y' em $(Ay)^\perp$ com $b(y', y') \neq -b(y, y)$.

Como $\gamma \neq 0$ em A , do lema anterior temos que existem α' e β em A , com $\beta \neq 0$, tais que $b(\alpha' y + \beta y', \alpha' y + \beta y') = \gamma^2 b(y, y) = b(x, x)$. Então, do Lema (1.19) segue que existe em elemento anisotrópico $z \in M$ tal que $\tau_z(x) = \alpha' y + \beta y'$, ou seja $\alpha = \alpha'$ e $u = \beta y'$, o que mostra o lema para o caso em que A é corpo.

Consideremos agora A um anel local com $2 \in A^*$, $\{y = y_1, y_2, \dots, y_n\}$ uma base ortogonal de M com $n \geq 3$ e $b(y_i, y_i) = \alpha_i \in A^*$, para $i = 1, \dots, n$. Com relação a esta base, podemos escrever $x = \sum_{i=1}^n x_i y_i$.

Queremos encontrar $z_1, \dots, z_n \in A$, tais que $z = \sum_{i=1}^n z_i y_i$ é um elemento anisotrópico de M satisfazendo o requerido.

Observemos que

$$\begin{aligned} \tau_z(x) &= x - \frac{2b(x, z)}{b(z, z)} z = \\ &= \frac{1}{b(z, z)} [b(z, z)x - 2b(x, z)z] = \\ &= \frac{1}{b(z, z)} \sum_{i=1}^n [b(z, z)x_i - 2b(x, z)z_i] y_i. \end{aligned}$$

Para cada $i = 1, \dots, n$, seja $u_i = u_i(z_1, \dots, z_n) = b(z, z) x_i - 2b(x, z) z_i$. Então $\tau_z(x) = \alpha y + u$ onde $\alpha = \frac{u_i}{b(z, z)} \in A$ e $u = \frac{1}{b(z, z)} \sum_{i=2}^n u_i y_i \in (Ay_1)^\perp$, com $b(u, u) = \frac{1}{b(z, z)^2} \sum_{i=2}^n u_i^2 \alpha_i$ (lembremos que $y = y_1$).

Assim, é suficiente encontrarmos $z_1, \dots, z_n$ tais que $b(z, z)$ e $\sum_{i=2}^n u_i^2 \alpha_i$ sejam unidades em A . Desde que A é um anel local com único ideal maximal $\mathcal{M}$, isto é equivalente a mostrarmos que o polinômio não nulo em n variáveis

$$f(z_1, \dots, z_n) = b(z, z) \sum_{i=2}^n u_i(z_1, \dots, z_n)^2 \alpha_i$$

representa um elemento que não pertence à $\mathcal{M}$, ou seja, $\overline{f(z_1, \dots, z_n)} \neq \bar{0}$ em $\frac{A}{\mathcal{M}}$.

Como já provamos o lema para o caso em que A é um corpo, temos que existe $\bar{z} = \sum_{i=1}^n \bar{z}_i \bar{y}_i \in \bar{M} = M \otimes \frac{A}{\mathcal{M}}$, com $b(\bar{z}, \bar{z}) \neq \bar{0}$, tal que $\tau_{\bar{z}}(\bar{x}) = \bar{\alpha} \bar{y}_1 + \bar{u}$, onde $\alpha \in A$ e $u \in (Ay)^\perp$ é tal que $b(\bar{u}, \bar{u}) \neq \bar{0}$. Para tais elementos temos $\bar{f}(\bar{z}_1, \dots, \bar{z}_n) \neq \bar{0}$, como queríamos. ■

Teorema 1.22 (Descrição Indutiva de Isometrias) Para $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ em A^* , $n \geq 3$, as seguintes afirmações são equivalentes

- (a) $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$;
- (b) Existem $\alpha, \beta, \gamma_3, \dots, \gamma_n \in A^*$ tais que $\langle \alpha_1, \alpha \rangle \simeq \langle \beta_1, \beta \rangle$, $\langle \alpha_2, \dots, \alpha_n \rangle \simeq \langle \alpha, \gamma_3, \dots, \gamma_n \rangle$ e $\langle \beta_2, \dots, \beta_n \rangle \simeq \langle \beta, \gamma_3, \dots, \gamma_n \rangle$.

Dem.: Para mostrarmos que (b) implica em (a) é suficiente observarmos que

$$\begin{aligned} \langle \alpha_1, \dots, \alpha_n \rangle &\simeq \langle \alpha_1, \alpha, \gamma_3, \dots, \gamma_n \rangle \simeq \\ &\simeq \langle \beta_1, \beta, \gamma_3, \dots, \gamma_n \rangle \simeq \\ &\simeq \langle \beta_1, \dots, \beta_n \rangle. \end{aligned}$$

Para a recíproca, consideremos $(M, b) \in \text{Bil}(A)$ tal que

$$b \simeq \langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle.$$

Destas decomposições, temos que existem bases ortogonais $\{x_1, \dots, x_n\}$ e $\{y_1, \dots, y_n\}$ de (M, b) com $b(x_i, x_i) = \alpha_i$ e $b(y_i, y_i) = \beta_i$, para cada $i = 1, \dots, n$.

Do lema anterior temos que existe $z \in M$, anisotrópico, tal que $\tau_z(y_1) = \alpha'x_1 + x$, com $\alpha' \in A$ e $x \in (Ax_1)^\perp$ anisotrópico. Desde que τ_z é uma isometria, temos que $\{\tau_z(y_1), \dots, \tau_z(y_n)\}$ é também uma base ortogonal de (M, b) com a propriedade que $b(\tau_z(y_i), \tau_z(y_i)) = \beta_i$, para cada $i = 1, \dots, n$. Assim, trocando $\{y_1, \dots, y_n\}$ por $\{\tau_z(y_1), \dots, \tau_z(y_n)\}$, podemos assumir, sem perda de generalidade, que $y_1 = \alpha'x_1 + x$. Desde que $x \in (Ax_1)^\perp = Ax_2 \oplus \dots \oplus Ax_n$ é anisotrópico, podemos obter uma base ortogonal de $Ax_2 \oplus \dots \oplus Ax_n$ da forma $\{x, z_3, \dots, z_n\}$. Do mesmo modo, desde que $y_1 \in Ax_1 \oplus Ax$ é anisotrópico, podemos obter uma base ortogonal de $(Ax_1 \oplus Ax, b)$ da forma $\{y_1, y\}$. Consequentemente $\{y_1, y, z_3, \dots, z_n\}$ é uma base ortogonal de (M, b) e $\{y, z_3, \dots, z_n\}$ é uma base ortogonal de $Ay_2 \oplus \dots \oplus Ay_n$.

Agora o resultado do item (b) segue tomando $\alpha = b(x, x)$, $\beta = b(y, y)$ e $\gamma_i = b(z_i, z_i)$ para $i = 3, \dots, n$. ■

Vejamos agora o teorema do cancelamento de Witt para espaços bilineares sobre um anel local em que 2 é inversível. Este é um dos resultados desta seção que não vale sem assumirmos que 2 é inversível no anel de base, veremos um contra-exemplo logo após o teorema.

Teorema 1.23 (Teorema do Cancelamento de Witt) *Se (M_i, b_i) , $1 \leq i \leq 3$, são espaços bilineares sobre A tais que $b_1 \perp b_2 \simeq b_1 \perp b_3$, então $b_2 \simeq b_3$.*

Dem.: Usando indução sobre a dimensão de b_1 , é suficiente mostrarmos o resultado para o caso em que $\dim(b_1) = 1$. Usando que $b_1 \perp b_2 \simeq b_1 \perp b_3$ e comparando as dimensões, podemos escrever $b_1 = \langle \gamma \rangle$, $b_2 = \langle \alpha_2, \dots, \alpha_n \rangle$ e $b_3 = \langle \beta_2, \dots, \beta_n \rangle$ e, por hipótese temos

$$\langle \gamma, \alpha_2, \dots, \alpha_n \rangle \simeq \langle \gamma, \beta_2, \dots, \beta_n \rangle.$$

Se $n = 2$, então $\gamma\alpha_2 \equiv \gamma\beta_2 \pmod{(A^*)^2}$, ou seja, $\alpha_2 \equiv \beta_2 \pmod{(A^*)^2}$ e, portanto $b_2 \simeq b_3$.

Agora, se $n \geq 3$ então da Descrição Indutiva de Isometrias, podemos encontrar $\alpha, \beta, \gamma_3, \dots, \gamma_n \in A^*$ tais que $\langle \gamma, \alpha \rangle \simeq \langle \gamma, \beta \rangle$, $\langle \alpha_2, \dots, \alpha_n \rangle \simeq \langle \alpha, \gamma_3, \dots, \gamma_n \rangle$ e $\langle \beta_2, \dots, \beta_n \rangle \simeq \langle \beta, \gamma_3, \dots, \gamma_n \rangle$. Do caso $n = 2$ obtemos $\langle \alpha \rangle \simeq \langle \beta \rangle$ e, consequentemente $\langle \alpha_2, \dots, \alpha_n \rangle \simeq \langle \alpha, \gamma_3, \dots, \gamma_n \rangle \simeq \langle \beta, \gamma_3, \dots, \gamma_n \rangle \simeq \langle \beta_2, \dots, \beta_n \rangle$, ou seja $b_2 \simeq b_3$, como queríamos. ■

Exemplo 1.24 Sejam (M, b) o espaço bilinear sobre um corpo A de característica 2, onde $b = \langle 1, 1, 1, 1 \rangle$ e $\{x_1, x_2, x_3, x_4\}$ a base de M correspondente à esta decomposição. Tomando $x = x_1 + x_2$ e $y = x_1 + x_3$, temos que a matriz de b restrita ao subespaço $M_1 = Ax \oplus Ay$ de M é

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

Logo (M_1, b) é um subespaço não-singular de (M, b) e, por (1.13),

$$(M, b) \simeq (M_1, b) \perp (M_2, b),$$

onde $(M_2, b) = (M_1, b)^\perp$.

É fácil verificar que $x' = x_1 + x_2 + x_3$ e $y' = x_4$ é uma base para $M_1^\perp$ e que a matriz de b em relação a esta base é

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

ou seja,

$$\langle 1, 1, 1, 1 \rangle \simeq \langle 1, 1 \rangle \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Agora, $(M_1, \langle 1, 1 \rangle)$ não é isométrico a $(M_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix})$ pois para todo $z \in M_2$, temos que $b(z, z) = 0$ e se $\varphi : M_1 \rightarrow M_2$ é uma isometria, então $1 = b(x, x) = b(\varphi(x), \varphi(x)) = 0$, o que é um absurdo. Portanto o teorema do cancelamento de Witt não vale em geral se 2 não é uma unidade no anel.

Finalizaremos esta seção apresentando alguns resultados sobre o comportamento do conjunto de valores de um espaço bilinear, com relação a decomposição ortogonal de subespaços.

Seja (M, b) um espaço bilinear sobre A . O subconjunto de A^*

$$\mathcal{D}(b) = \{\alpha \in A^*; \alpha = b(x, x), \text{ para algum } x \in M\}$$

é dito ser o *conjunto de valores* de (M, b) , ou ainda o conjunto dos elementos representados pela forma bilinear b .

É fácil verificar que se $\alpha \in \mathcal{D}(b)$ e $\beta \in A^*$, então $\beta^2 \alpha \in \mathcal{D}(b)$; se $b' \in \text{Bil}(A)$ e b é um somando ortogonal de b' , então $\mathcal{D}(b) \subseteq \mathcal{D}(b')$ e se $b \simeq b'$, então $\mathcal{D}(b) = \mathcal{D}(b')$.

Em particular se $b \simeq \langle \alpha_1, \dots, \alpha_n \rangle$, então

$$\mathcal{D}(b) = \{\alpha \in A^*; \alpha = \alpha_1 \beta_1^2 + \dots + \alpha_n \beta_n^2, \text{ com } \beta_1, \dots, \beta_n \in A\}.$$

É fácil verificar que se $b \in \text{Bil}(A)$ e $\alpha \in A^*$, então $\mathcal{D}(\langle \alpha \rangle \otimes b) = \alpha \mathcal{D}(b)$.

Com esta terminologia, decorre imediatamente de (1.13) o seguinte resultado

Lema 1.25 *Se $b \in \text{Bil}(A)$ e $\alpha \in \mathcal{D}(b)$, então $b \simeq \langle \alpha \rangle \perp b'$, para algum $b' \in \text{Bil}(A)$.*

Dem.: Imediata. ■

Teorema 1.26 *Sejam b_1 e b_2 espaços bilineares sobre A com dimensão ≥ 1 . Então*

$$\mathcal{D}(b_1 \perp b_2) = \bigcup \{\mathcal{D}(\langle \alpha, \beta \rangle); \alpha \in \mathcal{D}(b_1), \beta \in \mathcal{D}(b_2)\}.$$

Dem.: Se $\dim(b_1 \perp b_2) = 2$, temos $b_1 = \langle \alpha' \rangle$ e $b_2 = \langle \beta' \rangle$, então $b_1 \perp b_2 = \langle \alpha', \beta' \rangle$ onde $\alpha' \in \mathcal{D}(b_1)$ e $\beta' \in \mathcal{D}(b_2)$, o que mostra que

$$\mathcal{D}(b_1 \perp b_2) \subseteq \bigcup \{ \mathcal{D}(\langle \alpha, \beta \rangle); \alpha \in \mathcal{D}(b_1), \beta \in \mathcal{D}(b_2) \}.$$

Por outro lado, se $\alpha \in \mathcal{D}(b_1)$ e $\beta \in \mathcal{D}(b_2)$, como $\dim(b_1) = \dim(b_2) = 1$, temos que $\langle \alpha \rangle \simeq b_1$ e $\langle \beta \rangle \simeq b_2$ o que implica que $\mathcal{D}(\langle \alpha, \beta \rangle) = \mathcal{D}(b_1 \perp b_2)$.

Podemos então assumir que $\dim(b_1 \perp b_2) \geq 3$. Dado $\alpha \in \mathcal{D}(b_1)$ e $\beta \in \mathcal{D}(b_2)$, do lema anterior temos que existem $\alpha_i, \beta_j \in A^*$, $2 \leq i \leq k$ e $2 \leq j \leq m$, tais que $b_1 \simeq \langle \alpha, \alpha_2, \dots, \alpha_k \rangle$ e $b_2 \simeq \langle \beta, \beta_2, \dots, \beta_m \rangle$. Assim $\mathcal{D}(b_1 \perp b_2) = \mathcal{D}(\langle \alpha, \alpha_2, \dots, \alpha_k, \beta, \beta_2, \dots, \beta_m \rangle) = \mathcal{D}(\langle \alpha, \beta \rangle \perp \langle \alpha_2, \dots, \alpha_k, \beta_2, \dots, \beta_m \rangle)$. Portanto, $\mathcal{D}(\langle \alpha, \beta \rangle) \subseteq \mathcal{D}(b_1 \perp b_2)$.

Reciprocamente, seja $\rho \in \mathcal{D}(b_1 \perp b_2)$. Suponhamos que $b_1 \simeq \langle \alpha_1, \dots, \alpha_k \rangle$ e $b_2 \simeq \langle \alpha_{k+1}, \dots, \alpha_n \rangle$, onde $1 < k < n$. Temos então que $\rho \in \mathcal{D}(\langle \alpha_1, \dots, \alpha_n \rangle)$ e, podemos escrever $\rho = \sum_{i=1}^n \alpha_i \gamma_i^2$. Se $\alpha = \sum_{i=1}^k \alpha_i \gamma_i^2$ e $\beta = \sum_{i=k+1}^n \alpha_i \gamma_i^2$ são unidades em A , então $\rho \in \mathcal{D}(\langle \alpha, \beta \rangle)$ o que mostra que

$$\mathcal{D}(b_1 \perp b_2) \subseteq \bigcup \{ \mathcal{D}(\langle \alpha, \beta \rangle); \alpha \in \mathcal{D}(b_1), \beta \in \mathcal{D}(b_2) \}.$$

Se α e β não são unidades, a demonstração desta inclusão é um pouco mais complicada e faremos por indução sobre k .

Como $\rho \in \mathcal{D}(\langle \alpha_1, \dots, \alpha_n \rangle)$, do lema anterior temos que existem $\gamma_2, \dots, \gamma_n \in A^*$ tais que $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \rho, \gamma_2, \dots, \gamma_n \rangle$. Então, por (1.22) existem $\alpha, \gamma, \beta_3, \dots, \beta_n$ em A^* , tais que $\rho \in \mathcal{D}(\langle \rho, \gamma \rangle) = \mathcal{D}(\langle \alpha_1, \alpha \rangle)$ e $\alpha \in \mathcal{D}(\langle \alpha, \beta_3, \dots, \beta_n \rangle) = \mathcal{D}(\langle \alpha_2, \dots, \alpha_n \rangle)$, o que completa a demonstração para o caso em que $k = 1$.

Consideremos agora que $k \geq 2$. Como $\alpha \in \mathcal{D}(\langle \alpha_2, \dots, \alpha_n \rangle)$, por hipótese de indução, existem $\alpha' \in \mathcal{D}(\langle \alpha_2, \dots, \alpha_k \rangle)$ e $\beta \in \mathcal{D}(\langle \alpha_{k+1}, \dots, \alpha_n \rangle)$, tais que $\alpha \in \mathcal{D}(\langle \alpha', \beta \rangle)$. Novamente do lema anterior obtemos $\langle \alpha, \gamma' \rangle \simeq \langle \alpha', \beta \rangle$, para algum $\gamma' \in A^*$. Isto implica que $\langle \alpha, \rho, \gamma' \rangle \simeq \langle \rho, \alpha', \beta \rangle$. Assim $\mathcal{D}(\langle \alpha, \rho \rangle) \subseteq \mathcal{D}(\langle \rho, \alpha', \beta \rangle)$.

Agora, $\rho \in \mathcal{D}(\langle \alpha, \rho \rangle) \subseteq \mathcal{D}(\langle \beta \rangle \perp \langle \rho, \alpha' \rangle)$. Desta forma, usando o caso em que $k = 1$, temos que existe $\omega \in \mathcal{D}(\langle \rho, \alpha' \rangle)$ tal que $\rho \in \mathcal{D}(\langle \beta, \omega \rangle)$, o que completa a demonstração, pois $\mathcal{D}(\langle \rho, \alpha' \rangle) \subseteq \mathcal{D}(\langle \alpha_1, \dots, \alpha_k \rangle)$. ■

Corolário 1.27 *Se $b_1, \dots, b_n \in \mathbf{Bil}(A)$ são tais que $\dim(b_i) \geq 1$, para todo $i = 1, \dots, n$, então*

$$\mathcal{D}(b_1 \perp \dots \perp b_n) = \bigcup \{ \mathcal{D}(\langle \alpha_1, \dots, \alpha_n \rangle); \alpha_i \in \mathcal{D}(b_i) \text{ para todo } i = 1, \dots, n \}.$$

Dem.: Segue facilmente usando indução sobre n e o teorema anterior. ■

1.4 Espaços Metabólicos e Hiperbólicos

Encerramos este capítulo com a definição e a caracterização dos espaços metabólicos e hiperbólicos, os quais são essenciais para a definição dos anéis de Witt que apresentaremos no próximo capítulo.

Seja (U, b) um módulo bilinear sobre A . Definimos em $U \oplus U^*$ uma forma bilinear simétrica b_U por:

$$b_U(u \oplus u^*, v \oplus v^*) = b(u, v) + u^*(v) + v^*(u),$$

para todo $u, v \in U$ e $u^*, v^* \in U^*$. Ao módulo bilinear $(U \oplus U^*, b_U)$ damos o nome de *espaço metabólico* e denotamos por $\mathbf{M}(U, b)$, ou simplesmente por $\mathbf{M}(U)$, ou ainda $\mathbf{M}(b)$. Provamos a seguir que este módulo é de fato não-singular.

Proposição 1.28 *Para todo módulo bilinear (U, b) sobre A , $\mathbf{M}(U)$ é um espaço bilinear.*

Dem.: Consideremos $\{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$ uma base de $\mathbb{M}(U) = U \oplus U^*$, onde $\{x_1, \dots, x_n\}$ é uma base de U e $\{x_1^*, \dots, x_n^*\}$ é a base dual de U^* . A matriz de b_U com relação a esta base é a matriz em blocos

$$(b_U(x_i, x_j^*)) = \begin{pmatrix} b & I \\ I & 0 \end{pmatrix},$$

onde o bloco b é a matriz associada ao módulo bilinear (U, b) , I é a matriz identidade $n \times n$ e 0 é a matriz nula $n \times n$. O determinante desta matriz é $-\det(b) \det(I)$, isto é, a matriz associada a forma bilinear simétrica b_U é inversível e, portanto $\mathbb{M}(U)$ é um espaço bilinear não-singular, como queríamos. ■

Em $\mathbb{M}(U)$ o subespaço U^* é sempre totalmente isotrópico, o mesmo pode não ocorrer com U . Se $b = 0$, então U também é um subespaço totalmente isotrópico de $\mathbb{M}(U)$. Neste caso, dizemos que $\mathbb{M}(U, 0)$ é um *espaço bilinear hiperbólico* que denotaremos também por $\mathbb{H}(U)$.

Se $U = Ax$, então $\mathbb{H}(U) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, será chamado de *plano hiperbólico* e denotado simplesmente por $\mathbb{H}$. Todo espaço bilinear hiperbólico é uma soma ortogonal de planos hiperbólicos. De fato consideremos $(U, 0)$ tal que $\dim U = n$. Sejam $\{x_1, \dots, x_n\}$ e $\{x_1^*, \dots, x_n^*\}$ bases de U e U^* respectivamente. Podemos considerar $\{x_1, x_1^*, x_2, x_2^*, \dots, x_n, x_n^*\}$ como base de $U \oplus U^*$ e com relação a esta base

$$\mathbb{H}(U) \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \dots \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

com n parcelas. Portanto, $\mathbb{H}(U) \simeq \mathbb{H} \perp \dots \perp \mathbb{H} \simeq n\mathbb{H}$, onde $n = \dim U$.

Consideremos agora, $(U, b) = (Ax, \langle \alpha \rangle)$, então:

$$\mathbb{M}(\langle \alpha \rangle) = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}.$$

Mais geralmente,

$$\mathbb{M}(\langle \alpha_1, \dots, \alpha_n \rangle) \simeq \begin{pmatrix} \alpha_1 & 1 \\ 1 & 0 \end{pmatrix} \perp \dots \perp \begin{pmatrix} \alpha_n & 1 \\ 1 & 0 \end{pmatrix}.$$

As noções de espaço metabólico e espaço hiperbólico coincidem quando 2 é uma unidade no anel de base. Mais precisamente, quando A é um anel local com $2 \in A^*$, temos

Proposição 1.29 *Se 2 é uma unidade em A , então todo espaço metabólico é hiperbólico. Além disso, $\mathbb{H} \simeq \langle 1, -1 \rangle$.*

Dem.: Das decomposições ortogonais de $\mathbb{H}(U)$ e de $\mathbb{M}(U)$ listadas acima, é suficiente mostrarmos que para todo $\alpha \in A$

$$\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Seja $(Ax \oplus Ay, b) = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$, ou seja, $b(x, x) = \alpha, b(x, y) = 1$ e $b(y, y) = 0$.

Os elementos $x' = x - \frac{\alpha}{2}y$ e $y' = y \in Ax \oplus Ay$ são tais que $b(x', x') = 0 = b(y', y')$ e $b(x', y') = 1$. Assim $(Ax' \oplus Ay', b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ é um subespaço não-singular de $\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$. Agora, de (1.13) e do fato que ambos são espaços bilineares de dimensão 2, temos que

$$\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Além disso, se $\mathbb{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, com base $\{x', y'\}$ como acima, então $Ax'' \oplus Ay''$,

onde $x'' = \frac{x' + y'}{2}$ e $y'' = \frac{x' - y'}{2}$, é um subespaço não singular de $\mathbb{H}$ da forma $\langle 1, -1 \rangle$ e, como acima, obtemos que $\mathbb{H} \simeq \langle 1, -1 \rangle$. ■

Como consequência desta proposição temos

Corolário 1.30 *Se (M, b) é um espaço bilinear isotrópico sobre o anel local A com $2 \in A^*$, então $b \simeq \langle 1, -1 \rangle \perp b'$, para algum $b' \in \text{Bil}(A)$.*

Dem.: Desde que b é um espaço bilinear isotrópico, então existe $x \in M$, primitivo com $b(x, x) = 0$, isto é, um elemento isotrópico de M . Além disso, como b é não-singular, existe $y \in M$ tal que $b(x, y) = 1$. Consequentemente, a matriz da forma bilinear b restrita ao subespaço $Ay \oplus Ax$ de M é

$$\begin{pmatrix} b(y, y) & 1 \\ 1 & 0 \end{pmatrix},$$

ou seja, $(Ay \oplus Ax, b) = \mathbb{M}(\langle b(y, y) \rangle)$ que é metabólico e, da proposição anterior temos que este subespaço é isométrico à $\langle 1, -1 \rangle$. Agora o resultado segue de (1.13). ■

O próximo teorema caracteriza os espaços metabólicos.

Teorema 1.31 *Seja (M, b) um espaço bilinear sobre A . Então (M, b) é um espaço metabólico se, e somente se M contém um subespaço totalmente isotrópico maximal.*

Dem.: Seja (M, b) um espaço metabólico. Então $M = V \oplus V^*$ para algum módulo bilinear (V, b') . Como V^* é um subespaço totalmente isotrópico, temos que $V^* \subseteq (V^*)^\perp$. Vamos agora mostrar que $(V^*)^\perp \subseteq V^*$, ou seja que V^* é um subespaço totalmente isotrópico maximal de M . Consideremos $\{x_1, \dots, x_n\}$ uma base de V e $\{x_1^*, \dots, x_n^*\}$ a base dual de V^* . Seja $v + v^* \in (V^*)^\perp$. Então $b_V(v + v^*, v_1^*) = 0$ para todo $v_1^* \in V^*$, em particular $b_V(v + v^*, x_i^*) = 0$ para todo $i = 1, \dots, n$. Mas

$$b_V(v + v^*, x_i^*) = b(v, 0) + v^*(0) + x_i^*(v),$$

ou seja, $x_i^*(v) = 0$, para todo $i = 1, \dots, r$. Escrevendo $v = u_1x_1 + \dots + u_nx_n$, temos que $x_i^*(v) = u_i$, para todo $i = 1, \dots, n$. Logo $v = 0$ e, assim $(V^*)^\perp \subseteq V^*$. Portanto, $V^* = (V^*)^\perp$.

Reciprocamente, se U é um subespaço totalmente isotrópico de M , então $U = U^\perp$ e de (1.14), existe um subespaço V de M tal que $U \cong V^*$ e $M = U \oplus V$. Consideremos a aplicação $d : U \rightarrow V^*$, onde $d(u)(v) = b(u, v)$ para todo $u \in U$ e $v \in V$. Seja $\{x_1, \dots, x_n, y_1, \dots, y_m\}$ é uma base de M , onde $\{x_1, \dots, x_n\}$ é uma base de U e $\{y_1, \dots, y_m\}$ é uma base de V . Como $U = U^\perp$, a matriz de b com relação a esta base é a matriz em blocos

$$\begin{pmatrix} 0 & B_{12} \\ B_{12} & B_{22} \end{pmatrix},$$

onde (B_{12}) é a matriz de $b|_{U \times V}$ e (B_{22}) é a matriz de $b|_{V \times V}$. Do fato de b ser não-singular, temos que $\det(B_{12}) \in A^*$, ou seja, $b : U \times V \rightarrow A$ é não singular, o que mostra que a aplicação d definida acima, é um isomorfismo.

Seja $f : M \rightarrow \mathbb{M}(V) = V \oplus V^*$ tal que $f(u + v) = v + d(u)$. Temos que f é um isomorfismo, pois é a soma da identidade com o isomorfismo d . Mostremos que de fato f é uma isometria. Para todo $u + v, u' + v' \in M = U \oplus V$, temos

$$\begin{aligned} b_V(f(u + v), f(u' + v')) &= b_V(v + d(u), v' + d(u')) = \\ &= b(v, v') + d(u)(v') + d(u')(v) = b(u + v, u' + v'). \end{aligned}$$

Sendo que a última igualdade decorre do fato que $b(u, u') = 0$. Assim, $M \simeq \mathbb{M}(U)$ que é metabólico. ■

Corolário 1.32 (i) Para $(V, b) \in \text{Bil}(A)$ e (U, b') um módulo bilinear sobre A , temos que $\mathbb{M}(U) \otimes (V, b) \simeq \mathbb{M}(U \otimes V)$.

(ii) Para $(U, b) \in \text{Bil}(A)$, temos que $(U, b)^\perp(U, -b) \simeq \mathbb{M}(U)$, onde $-b(x, y) = (-1)b(x, y)$, para todo $x, y \in U$.

Dem.: Desde que $\mathbb{M}(U) \otimes V = (U \oplus U^*) \otimes V \cong (U \otimes V) \oplus (U^* \otimes V)$ e U^* é um subespaço totalmente isotrópico de $\mathbb{M}(U)$, temos que $U^* \otimes V$ é um subespaço totalmente isotrópico de $\mathbb{M}(U) \otimes V$, ou seja, $U^* \otimes V \subseteq (U^* \otimes V)^\perp$. Para provarmos (i), do teorema anterior é suficiente mostrarmos que $(U^* \otimes V)^\perp \subseteq U^* \otimes V$, ou seja, que $U^* \otimes V$ é um subespaço totalmente isotrópico maximal de $\mathbb{M}(U) \otimes V$. Desde que $\mathbb{M}(U) \otimes V$ é gerado pelos elementos da forma $(u \oplus u^*) \otimes v$, com $u \in U$ e $v \in V$, é suficiente considerarmos os elementos de $(U^* \otimes V)^\perp$ da forma $(u_1 \oplus u_1^*) \otimes v_1$, com $u_1 \in U$ e $v_1 \in V$ primitivo. Assim

$$(b_U \otimes b)((u_1 + u_1^*) \otimes v_1, u^* \otimes v) = 0,$$

para todo $u^* \in U^*$ e $v \in V$. Como v_1 é primitivo e (V, b) é não-singular, temos que existe $v \in V$ tal que $b(v_1, v) \in A^*$. Assim $0 = b_U(u_i + u_i^*, u^*) \cdot b(v_1, v)$, para todo $u^* \in U^*$, o que implica que para todo $u^* \in U$, $0 = b_U(u_i + u_i^*, u^*) = b(u_i, 0) + u_i^*(0) + u^*(u_i)$ ou seja $u^*(u_i) = 0$ para todo $u^* \in U^*$. Logo $u_i = 0$, o que mostra (i).

Para o item (ii) basta observarmos que $V = \{(x, x); x \in U\}$ é um subespaço totalmente isotrópico maximal de $(U, b) \perp (U, -b)$. ■

De (1.32), temos que mesmo quando 2 não é inversível em A , o espaço bilinear $b = \langle 1, -1 \rangle$ é metabólico.

Proposição 1.33 *Seja (U, b) um módulo bilinear. Então:*

$$\mathbb{M}(U, b) \perp \mathbb{M}(U, -b) \simeq \mathbb{H}(U) \perp \mathbb{M}(U, -b).$$

Dem.: Seja $\{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$ uma base de $U \oplus U^*$, onde $\{x_1, \dots, x_n\}$ é uma base de U e $\{x_1^*, \dots, x_n^*\}$ é a base dual de U^* . Nesta base temos que

$$\mathbb{M}(U, b) = \begin{pmatrix} 0 & I \\ I & b \end{pmatrix},$$

onde I é a matriz identidade $n \times n$, 0 é a matriz nula $n \times n$ e b é a matriz de (U, b) em relação a base de U dada acima. Note que em relação a esta mesma base

$$\mathbb{M}(U, -b) = \begin{pmatrix} 0 & -I \\ -I & -b \end{pmatrix},$$

pois $-b_U(x, y) = -b(x, y) - u^*(v) - v^*(u)$.

Considerando a matriz em blocos inversível $C = \begin{pmatrix} I & 0 & I & b \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & I & 0 & I \end{pmatrix}$, obtemos

$$\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & I \\ I & 0 & I & 0 \\ b & 0 & 0 & I \end{pmatrix} \begin{pmatrix} 0 & I & 0 & 0 \\ I & b & 0 & 0 \\ 0 & 0 & 0 & -I \\ 0 & 0 & -I & -b \end{pmatrix} \begin{pmatrix} I & 0 & I & b \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & I & 0 & I \end{pmatrix} = \begin{pmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & -I \\ 0 & 0 & -I & -b \end{pmatrix},$$

o que mostra que $\mathbb{M}(U, b) \perp \mathbb{M}(U, -b) \simeq \mathbb{H}(U) \perp \mathbb{M}(U, -b)$, como queríamos. ■

Em geral, um espaço bilinear isotrópico não necessariamente é metabólico e/ou hiperbólico. Mas quando 2 é inversível no anel de base, existem certos tipos de espaços bilineares que são isotrópicos se, e somente se são hiperbólicos. No restante desta seção, definiremos tais espaços e mostraremos a equivalência acima. Para tanto, no que segue nesta seção, 2 será uma unidade no anel local A .

A forma bilinear não-singular $b = \langle 1, \alpha_1 \rangle \otimes \cdots \otimes \langle 1, \alpha_n \rangle$, com $\alpha_i \in A^*$, $1 \leq i \leq n$, é dita ser uma *forma (ou n -forma) de Pfister*. Por convenção, a única 0 -forma de Pfister é $\langle 1 \rangle$. O espaço bilinear (M, b) , onde b é uma n -forma de Pfister, é dito ser um *espaço (ou n -espaço) de Pfister*. Usaremos também a notação $\ll \alpha_1, \dots, \alpha_n \gg$ para denotar a n -forma de Pfister $\langle 1, \alpha_1 \rangle \otimes \cdots \otimes \langle 1, \alpha_n \rangle$.

Proposição 1.34 *Seja $b \in \text{Bil}(A)$ uma n -forma de Pfister. Então*

$$\mathcal{D}(b) = \{\alpha \in A^*; \langle \alpha \rangle \otimes b \simeq b\}.$$

Mais ainda, $\mathcal{D}(b)$ é um subgrupo do grupo multiplicativo A^* .

Dem.: Se $\alpha \in A^*$ é tal que $\langle \alpha \rangle \otimes b \simeq b$, então desde que $\mathcal{D}(\langle \alpha \rangle \otimes b) = \alpha \mathcal{D}(b)$ e $1 \in \mathcal{D}(b)$, temos que $\alpha \in \alpha \mathcal{D}(b) = \mathcal{D}(b)$.

Mostraremos a inclusão contrária por indução sobre n . Considere $\alpha \in \mathcal{D}(b)$. Se $n = 0$, então $b = \langle 1 \rangle$ e α é um quadrado em A^* . Logo $\langle \alpha \rangle \otimes b = \langle \alpha \rangle \simeq b$.

Podemos então considerar que $n \geq 1$ e escrever $b = \langle 1, \alpha_1 \rangle \otimes b'$ onde $b' = \langle 1, \alpha_2 \rangle \otimes \cdots \otimes \langle 1, \alpha_n \rangle$. Neste caso $b \simeq b' \perp \langle \alpha_1 \rangle \otimes b'$ e de (1.26),

$$\alpha \in \mathcal{D}(b) = \bigcup \{ \mathcal{D}(\langle \gamma, \beta' \rangle); \gamma \in \mathcal{D}(b'), \beta' \in \mathcal{D}(\langle \alpha_1 \rangle \otimes b') \}$$

ou seja, $\alpha \in \mathcal{D}(\langle \gamma, \alpha_1 \beta \rangle)$, onde γ e β são elementos de $\mathcal{D}(b')$.

Como α é uma unidade de A e $\alpha \in \mathcal{D}(\langle \gamma, \alpha_1 \beta \rangle)$, de (1.25) e comparando os determinantes, obtemos que $\langle \gamma, \alpha_1 \beta \rangle \simeq \langle \alpha, \alpha \gamma \alpha_1 \beta \rangle$.

Como b' é uma $(n-1)$ -forma de Pfister e $\gamma, \beta \in \mathcal{D}(b')$, por hipótese de indução, temos que $\langle \gamma \rangle \otimes b' \simeq b'$, $\langle \beta \rangle \otimes b' \simeq b'$ e, conseqüentemente,

$$\langle \gamma \rangle \otimes \langle \beta \rangle \otimes b' \simeq \langle \gamma \rangle \otimes b' \simeq b'.$$

Assim

$$\begin{aligned} \langle \alpha \rangle \otimes b &\simeq \langle \alpha \rangle \otimes (b' \perp \langle \alpha_1 \rangle \otimes b') \simeq \langle \alpha \rangle \otimes b' \perp \langle \alpha \rangle \otimes \langle \alpha_1 \rangle \otimes b' \simeq \\ &\simeq \langle \alpha \rangle \otimes b' \perp \langle \alpha \rangle \otimes \langle \alpha_1 \rangle \otimes \langle \gamma \rangle \otimes \langle \beta \rangle \otimes b' \simeq \\ &\simeq \langle \alpha, \alpha \alpha_1 \gamma \beta \rangle \otimes b' \simeq \langle \gamma, \alpha_1 \beta \rangle \otimes b' \simeq \\ &\simeq \langle \gamma \rangle \otimes b' \perp \langle \alpha_1 \beta \rangle \otimes b' \simeq \\ &\simeq b' \perp \langle \alpha_1 \rangle \otimes b' \simeq b, \end{aligned}$$

ou seja $\langle \alpha \rangle \otimes b \simeq b$, o que prova a requerida inclusão.

Mais ainda, se $\alpha, \beta \in \mathcal{D}(b)$, então $\langle \alpha \rangle \otimes b \simeq b$ e $\langle \beta \rangle \otimes b \simeq b$. Logo $\langle \alpha \rangle \otimes \langle \beta \rangle \otimes b \simeq b$, ou seja, $\alpha \beta \in \mathcal{D}(b)$.

Desde que $\langle 1 \rangle \otimes b \simeq b$, temos que $\langle 1 \rangle \in \mathcal{D}(b)$. Agora, se $\alpha \in A^*$ e $\langle \alpha \rangle \otimes b \simeq b$, então

$$b \simeq \langle 1 \rangle \otimes b \simeq \langle \alpha^{-1} \rangle \otimes \langle \alpha \rangle \otimes b \simeq \langle \alpha^{-1} \rangle \otimes b,$$

ou seja, $\alpha^{-1} \in \mathcal{D}(b)$. Portanto, $\mathcal{D}(b)$ é um subgrupo de A^* . ■

Proposição 1.35 *Sejam b uma n -forma de Pfister e b' um espaço bilinear sobre A com $b \simeq \langle 1 \rangle \perp b'$. Se $\gamma = \gamma_1 \in \mathcal{D}(b')$, então existem $\gamma_2, \dots, \gamma_n \in A^*$ tais que*

$$b \simeq \langle 1, \gamma_1 \rangle \otimes \dots \otimes \langle 1, \gamma_n \rangle .$$

Dem.: Desde que b é uma n -forma de Pfister, podemos escrever

$$b = \langle 1, \alpha_1 \rangle \otimes \dots \otimes \langle 1, \alpha_n \rangle .$$

Provaremos agora a proposição por indução sobre n . Se $n = 1$ então $b' \simeq \langle \alpha_1 \rangle$, pois $b = \langle 1 \rangle \perp \langle \alpha_1 \rangle$. Se $\gamma \in \mathcal{D}(b') = \mathcal{D}(\langle \alpha_1 \rangle)$, então $\langle \gamma \rangle \simeq \langle \alpha_1 \rangle$ e, portanto, $b \simeq \langle 1, \gamma \rangle$. Se $n \geq 2$, considerando $b_1 = \langle 1, \alpha_2 \rangle \otimes \dots \otimes \langle 1, \alpha_n \rangle$, temos que $b \simeq b_1 \perp \langle \alpha_1 \rangle \otimes b_1$.

Seja $b'_1 \in \mathbf{Bil}(A)$ tal que $b_1 \simeq \langle 1 \rangle \perp b'_1$. Temos então $\langle 1 \rangle \perp b' \simeq b \simeq b_1 \perp \langle \alpha_1 \rangle \otimes b_1 \simeq \langle 1 \rangle \perp b'_1 \perp \langle \alpha_1 \rangle \otimes b_1$. Do teorema do Cancelamento de Witt, obtemos $b' \simeq b'_1 \perp \langle \alpha_1 \rangle \otimes b_1$. Se $\gamma \in \mathcal{D}(b')$, então de (1.26), temos que existem $\alpha \in \mathcal{D}(b'_1)$ e $\beta \in \mathcal{D}(b_1)$ tais que $\gamma \in \mathcal{D}(\langle \alpha, \alpha_1 \beta \rangle)$. Como na proposição anterior, obtemos que $\langle \alpha, \alpha_1 \beta \rangle \simeq \langle \gamma, \gamma \alpha \alpha_1 \beta \rangle$.

Como $b_1 \simeq \langle 1 \rangle \perp b'_1$ e $\alpha \in \mathcal{D}(b'_1)$, por hipótese de indução temos que $b_1 \simeq \langle 1, \alpha \rangle \otimes b_2$, para alguma forma de Pfister b_2 .

Agora, $\beta \in \mathcal{D}(b_1)$ e de (1.34), obtemos

$$\begin{aligned} b &\simeq b_1 \perp \langle \alpha_1 \rangle \otimes b_1 \simeq b_1 \perp \langle \beta \alpha_1 \rangle \otimes b_1 \simeq \langle 1, \alpha_1 \beta \rangle \otimes b_1 \simeq \\ &\simeq \langle 1, \alpha_1 \beta \rangle \otimes \langle 1, \alpha \rangle \otimes b_2 \simeq \\ &\simeq \langle 1, \alpha, \alpha_1 \beta, \alpha \alpha_1 \beta \rangle \otimes b_2 \simeq \\ &\simeq \langle 1, \gamma, \gamma \alpha \alpha_1 \beta, \alpha \alpha_1 \beta \rangle \otimes b_2 \simeq \\ &\simeq \langle 1, \gamma \rangle \otimes \langle 1, \alpha \alpha_1 \beta \rangle \otimes b_2, \end{aligned}$$

o que mostra a proposição. ■

Corolário 1.36 *Todo espaço bilinear de Pfister isotrópico é hiperbólico.*

Dem.: Se b é um espaço bilinear de Pfister isotrópico então, de (1.30), temos que $b \simeq \langle 1, -1 \rangle \perp b_1$ para algum $b_1 \in \text{Bil}(A)$. Escrevendo $b' = \langle -1 \rangle \perp b_1$, temos que $-1 \in \mathcal{D}(b')$ e, do teorema anterior obtemos $b \simeq \langle 1, -1 \rangle \otimes b_2$, para alguma forma de Pfister b_2 . Assim, $b \simeq b_2 \perp (-b_2)$ que, de (1.32) é metabólico. Como $2 \in A^*$, temos de (1.29) que b é hiperbólico, como queríamos. ■

Capítulo 2

O Anel de Witt

Neste capítulo apresentaremos um estudo da estrutura do anel $W(A)$, o anel de Witt dos espaços bilineares sobre um anel local A . Mais especificamente, daremos uma descrição dos ideais primos e dos geradores de $W(A)$. Apresentaremos também alguns resultados sobre os elementos nilpotentes e de torção de $W(A)$ que serão de extrema importância para o desenvolvimento do próximo capítulo.

2.1 Geradores de $W(A)$

À categoria $\mathbf{Bil}(A)$ associamos seu correspondente *Anel de Grothendieck*, o qual é chamado, *Anel de Witt-Grothendieck* dos espaços bilineares sobre A . Tal anel será denotado por $\widehat{W}(A)$.

Se $[b]$ denota a classe de isometrias do espaço bilinear b , então os elementos de $\widehat{W}(A)$ são as diferenças formais $[b_1] - [b_2]$, de classes $[b_1]$ e $[b_2]$, onde por definição $[b_1] - [b_2] = [b'_1] - [b'_2]$ se, e somente se existe $b \in \mathbf{Bil}(A)$ tal que $b_1 \perp b'_2 \perp b \simeq b_2 \perp b'_1 \perp b$.

As operações que fornecem uma estrutura de anel comutativo em $\widehat{W}(A)$ são as operações induzidas pelas operações soma ortogonal e produto tensorial de $\mathbf{Bil}(A)$.

Seja $\widehat{\mathbf{M}}(A) = \{[b] - [b'] \in \widehat{W}(A); b \text{ e } b' \text{ são metabólicos}\}$. De (1.32), decorre que

$\widehat{\mathbb{M}}(A)$ é um ideal de $\widehat{W}(A)$. Assim, definimos o *anel de Witt dos espaços bilineares sobre A* como sendo o anel quociente $W(A) = \frac{\widehat{W}(A)}{\widehat{\mathbb{M}}(A)}$.

Com a mesma notação de $\widehat{W}(A)$, seja $[b_1] - [b_2]$ um elemento genérico de $W(A)$. Então

$$[b_1] - [b_2] = [b_1] - [b_2] + [(-b_2)] - [(-b_2)] = [b_1 \perp (-b_2)] - [b_2 \perp (-b_2)].$$

De (1.32) temos que $b_2 \perp (-b_2)$ é metabólico; logo $[b_2 \perp (-b_2)] = [0]$ em $W(A)$. Assim, $[b_1] - [b_2] = [b_1 \perp (-b_2)]$, ou seja, todo elemento de $W(A)$ é da forma $[b]$ com $b \in \text{Bil}(A)$.

Da definição de $W(A)$, segue que $[b_1] = [b_2]$ se, e somente se existem U, V módulos bilineares tais que $b_1 \perp \mathbb{M}(U) \simeq b_2 \perp \mathbb{M}(V)$.

Vemos facilmente que $W(A)$, com as operações induzidas por $\perp$ e $\otimes$, é de fato um anel comutativo com elemento identidade, onde $-[b] = [(-b)]$ e $1_{W(A)} = [<1>]$.

Quando não houver perigo de confusão denotaremos simplesmente por b o elemento $[b]$ de $W(A)$, dentro do contexto se tornará claro quando consideramos b como um elemento de $W(A)$ ou como um elemento de $\text{Bil}(A)$.

Decorre de (1.33) que, para todo módulo bilinear (U, b) , $\mathbb{M}(U) = \mathbb{H}(U)$ em $\widehat{W}(A)$. Desta forma se considerarmos o subconjunto de $\widehat{W}(A)$

$$\widehat{\mathbb{H}}(A) = \{[\mathbb{H}(U)] - [\mathbb{H}(V)]; U, V \text{ são módulos bilineares}\},$$

temos que $\widehat{\mathbb{H}}(A) = \widehat{\mathbb{M}}(A)$ em $\widehat{W}(A)$. Agora se $\dim U = m$ e $\dim V = n$ temos que $\mathbb{H}(U) \simeq m\mathbb{H}$ e $\mathbb{H}(V) \simeq n\mathbb{H}$, ou seja em $\widehat{W}(A)$ temos

$$[\mathbb{H}(U)] - [\mathbb{H}(V)] = [m\mathbb{H}] - [n\mathbb{H}] = [(m - n)\mathbb{H}],$$

com $m - n \in \mathbb{Z}$. Portanto, podemos identificar $\widehat{\mathbb{H}}(A)$ com $\mathbb{Z}\mathbb{H} = \{n\mathbb{H}; n \in \mathbb{Z}\}$ e escrever $W(A) = \frac{\widehat{W}(A)}{\mathbb{Z}\mathbb{H}}$.

Proposição 2.1 *Dois espaços bilineares são iguais em $\widehat{W}(A)$ se, e somente se são iguais em $W(A)$ e tem a mesma dimensão.*

Dem.: Se $[b_1] = [b_2]$ em $\widehat{W}(A)$, então existe $(V, b) \in \text{Bil}(A)$ tal que $b_1 \perp b \simeq b_2 \perp b$ e, consequentemente, $\dim b_1 = \dim b_2$. Além disso temos $b_1 \perp b \perp (-b) \simeq b_2 \perp b \perp (-b)$ o que implica, de (1.32), que $b_1 \perp \mathbb{M}(V) \simeq b_2 \perp \mathbb{M}(V)$, ou seja, $[b_1] = [b_2]$ em $W(A)$. Reciprocamente sejam $b_1, b_2 \in \text{Bil}(A)$ espaços de mesma dimensão tais que $[b_1] = [b_2]$ em $W(A)$. Então existem $m, n \in \mathbb{Z}$ tais que $b_1 \perp m\mathbb{H} \simeq b_2 \perp n\mathbb{H}$. Como $\dim b_1 = \dim b_2$, igualando as dimensões temos que $m = n$. Portanto, $[b_1] = [b_2]$ em $\widehat{W}(A)$. ■

Sejam $G = A^*/(A^*)^2$ o grupo das classes quadradas de A e $f : G \rightarrow W(A)$ a aplicação que leva cada classe $(\alpha) \in G$ no elemento $\langle \alpha \rangle \in W(A)$. Escrevemos $f(\alpha)$ para indicar a imagem de (α) pela aplicação f .

Como um primeiro resultado sobre a geração do anel de Witt temos

Proposição 2.2 *O anel $W(A)$ é aditivamente gerado por $f(G)$, a imagem de f .*

Dem.: Seja $b \in \text{Bil}(A)$. O espaço $b \perp \langle 1 \rangle$ é próprio e, de (1,17), $b \perp \langle 1 \rangle$ admite uma base ortogonal, ou seja, existem $\beta_1, \dots, \beta_n \in A^*$ tais que:

$$b \perp \langle 1 \rangle \simeq \langle \beta_1 \rangle \perp \dots \perp \langle \beta_n \rangle.$$

Desde que $\langle 1, -1 \rangle$ é metabólico, em $W(A)$ temos

$$b = b \perp \langle 1, -1 \rangle = \langle \beta_1 \rangle \perp \dots \perp \langle \beta_n \rangle \perp \langle -1 \rangle = f(\beta_1) + \dots + f(\beta_n) + f(-1).$$

Assim, todo elemento de $W(A)$ se escreve como uma soma finita de elementos de $f(G)$. ■

A proposição acima mostra, em particular, que todo elemento de $W(A)$ pode ser representado pela classe de um espaço bilinear próprio sobre A , independentemente de 2 ser ou não inversível no anel A .

Seja $\mathbb{Z}[G]$ o anel de grupos de G . Também da proposição anterior, podemos afirmar que existe um homomorfismo de anéis sobrejetor $\varphi : \mathbb{Z}[G] \rightarrow W(A)$, que é

a extensão por linearidade de f . O próximo resultado caracteriza o núcleo $\mathcal{K}$ deste homomorfismo.

Proposição 2.3 *O ideal $\mathcal{K}$ de $\mathbb{Z}[G]$ é aditivamente gerado por $(1) + (-1)$ e por todos os elementos da forma $\sum_{i=1}^n (\alpha_i) - \sum_{i=1}^n (\beta_i) \in \mathbb{Z}[G]$, com $n \in \mathbb{N}$, tais que*

$$\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle .$$

Dem.: Claramente os elementos deste tipo estão em $\mathcal{K}$. Por outro lado, seja $z = \sum_{i=1}^r (\alpha_i) - \sum_{i=1}^s (\beta_i)$ um elemento de $\mathcal{K}$. Trocando z por $-z$ se necessário, podemos assumir que $r \geq s$. Desde que $\varphi(z) = 0$, temos que $\langle \alpha_1, \dots, \alpha_r \rangle = \langle \beta_1, \dots, \beta_s \rangle$ em $W(A)$, ou seja, existem $U_1, U_2 \in \mathbf{Bil}(A)$, tais que

$$\langle \alpha_1, \dots, \alpha_r \rangle \perp \mathbb{M}(U_1) \simeq \langle \beta_1, \dots, \beta_s \rangle \perp \mathbb{M}(U_2).$$

Como, $\dim \mathbb{M}(U_1)$ e $\dim \mathbb{M}(U_2)$ são números pares, temos que $r - s$ é um número par, digamos $2t$, com $t \geq 0$.

Sejam $b_1 = \langle \alpha_1, \dots, \alpha_r \rangle$ e $b_2 = \langle \beta_1, \dots, \beta_s \rangle \perp t \langle 1, -1 \rangle$. Desde que $b_1 = b_2$ em $W(A)$ e $\dim b_1 = \dim b_2$, temos por (2.1) que eles representam o mesmo elemento em $\widehat{W}(A)$. Assim, existe $b_3 \in \mathbf{Bil}(A)$ tal que

$$\langle \alpha_1, \dots, \alpha_r \rangle \perp b_3 \simeq \langle \beta_1, \dots, \beta_s \rangle \perp t \langle 1, -1 \rangle \perp b_3.$$

Somando $\langle 1 \rangle$ em ambos os lados, se necessário, podemos assumir que b_3 é próprio, ou seja $b_3 \simeq \langle \alpha_{r+1}, \dots, \alpha_n \rangle$. Tomando $\beta_i = \pm 1$, para $s < i \leq r$, e $\beta_i = \alpha_i$, para $r < i \leq n$, obtemos $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$ e

$$z = t((1) + (-1)) + \sum_{i=1}^n (\alpha_i) - \sum_{i=1}^n (\beta_i),$$

como queríamos. ■

Teorema 2.4 *O anel $W(A)$ é aditivamente gerado por $\{<\alpha>; \alpha \in A^*\}$ com as seguintes relações*

- (i) $<\alpha\beta^2> = <\alpha>$ para todo $\beta \in A^*$.
- (ii) $<\alpha_1> + \dots + <\alpha_n> = <\beta_1> + \dots + <\beta_n> \Leftrightarrow <\alpha, \dots, \alpha_n> \simeq <\beta_1, \dots, \beta_n>$.
- (iii) $<\alpha> + <-\alpha> = 0$.
- (iv) $<\alpha> + <\beta> = <\alpha + \beta> + <\alpha\beta(\alpha + \beta)>$, se $\alpha + \beta \in A^*$.
- (v) $<\alpha> \cdot <\beta> = <\alpha\beta>$.

Dem.: De (2.2) temos que $W(A)$ é aditivamente gerado por $\{<\alpha>; (\alpha) \in G\}$. Usando que $G = A^*/(A^*)^2$, podemos dizer que $W(A)$ é aditivamente gerado por $\{<\alpha>; \alpha \in A^*\}$ e vale (i). Para mostrarmos que (ii), (iii) e (v) valem para $W(A)$, basta observarmos que $W(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$ e usarmos a caracterização dos elementos de $\mathcal{K}$ apresentada na proposição anterior.

Mostremos então o item (iv). Consideremos o espaço bilinear $(M, b) = <\alpha, \beta>$ com uma base $\{x, y\}$ tal que, $b(x, y) = 0$, $b(x, x) = \alpha$ e $b(y, y) = \beta$. Então, $b(x + y, x + y) = \alpha + \beta \in A^*$. Como $\alpha + \beta \in A^*$ temos que $A(x + y)$ é um subespaço não-singular de M e de (1.13), $M = A(x + y) \perp (A(x + y))^\perp$. Como $(A(x + y))^\perp$ é um subespaço não-singular de M unidimensional, existe $z \in M$ com $b(z, z) = \gamma \in A^*$ e $b(x + y, z) = 0$, ou seja $(A(x + y))^\perp = Az$. Assim,

$$<\alpha> \perp <\beta> \simeq <\alpha + \beta> \perp <\gamma>.$$

Comparando os determinantes, temos $\alpha\beta \equiv (\alpha + \beta)\gamma \pmod{(A^*)^2}$. Isto implica que $\alpha\beta(\alpha + \beta)^{-1} \equiv \gamma \pmod{(A^*)^2}$, ou seja, $\gamma \equiv \alpha\beta(\alpha + \beta) \pmod{(A^*)^2}$. Logo, de (i) $<\gamma> = <\alpha\beta(\alpha + \beta)>$. Consequentemente,

$$<\alpha> \perp <\beta> \simeq <\alpha + \beta> \perp <\alpha\beta(\alpha + \beta)>.$$

Portanto, $<\alpha> + <\beta> = <\alpha + \beta> + <\alpha\beta(\alpha + \beta)>$, em $W(A)$, por (ii). ■

2.2 Os ideais primos de $W(A)$.

Nesta seção caracterizaremos os ideais primos de $W(A)$ usando o isomorfismo de anéis $W(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$, onde $G = A^*/A^{*2}$ e $\mathcal{K}$ é bem determinado em (2.3), ou seja, usaremos o fato que os ideais primos de $W(A)$ estão em correspondência biunívoca com os ideais primos de $\mathbb{Z}[G]$ que contém $\mathcal{K}$.

Para tanto começaremos determinando todos os ideais primos de $\mathbb{Z}[G]$ e, a seguir aqueles que contém $\mathcal{K}$.

Lema 2.5 (i) *Para cada ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, com $\mathbb{Z} \cap \mathcal{P} = \{0\}$, existe um único homomorfismo de anéis ϕ de $\mathbb{Z}[G]$ em $\mathbb{Z}$ com núcleo $\mathcal{P}$.*

(ii) *Para cada ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, com $\mathbb{Z} \cap \mathcal{P} = p\mathbb{Z}$, onde p é um número inteiro primo, existe um único homomorfismo de anéis ψ de $\mathbb{Z}[G]$ em $\mathbb{F}_p$, com núcleo $\mathcal{P}$, onde $\mathbb{F}_p$ denota o corpo finito com p elementos.*

Dem.: Consideramos o homomorfismo de anéis sobrejetor $h : \mathbb{Z} \rightarrow \frac{\mathbb{Z}[G]}{\mathcal{P}}$, que é a composição da inclusão $i : \mathbb{Z} \rightarrow \mathbb{Z}[G]$ com a sobrejeção $\pi : \mathbb{Z}[G] \rightarrow \frac{\mathbb{Z}[G]}{\mathcal{P}}$. Logo o núcleo de h , $\text{Ker}(h)$, é $\mathbb{Z} \cap \mathcal{P}$. Como $\mathbb{Z} \cap \mathcal{P}$ é ideal primo de $\mathbb{Z}$, temos que $\mathbb{Z} \cap \mathcal{P} = \{0\}$ ou $\mathbb{Z} \cap \mathcal{P} = p\mathbb{Z}$, para algum inteiro primo p de $\mathbb{Z}$.

Se $\mathbb{Z} \cap \mathcal{P} = \{0\}$, então $\mathbb{Z} \cong \frac{\mathbb{Z}[G]}{\mathcal{P}}$ e se $\mathbb{Z} \cap \mathcal{P} = p\mathbb{Z}$, então $\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \frac{\mathbb{Z}[G]}{\mathcal{P}}$. Assim estes isomorfismos induzem os homomorfismos ϕ e ψ requeridos e, desde que os anéis $\mathbb{Z}$ e $\mathbb{F}_p$ não admitem automorfismos não triviais, estes homomorfismos são únicos. ■

Como $g^2 = 1$ para todo $g \in G$, temos que para todo homomorfismo de anéis $\varphi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$, $\phi(g)^2 = \phi(g^2) = \phi(1) = 1$. Como $\phi(g) \in \mathbb{Z}$, temos que $\phi(g) = \pm 1$. Logo, todo homomorfismo de anéis de $\mathbb{Z}[G]$ em $\mathbb{Z}$ leva G em $\{\pm 1\}$, ou seja, a restrição $\phi|_G$, de ϕ em G é um *caracter do grupo* G , isto é, um homomorfismo de grupos χ de G em $\{\pm 1\}$. Reciprocamente, dado um caracter $\chi : G \rightarrow \{\pm 1\}$, ele se estende, de maneira única, a um homomorfismo de anéis $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$, devido a propriedade

universal de $\mathbb{Z}[G]$. Assim, para cada homomorfismo ϕ existe um único caracter χ tal que $\phi = \phi_\chi$.

Agora, seja p um número primo ímpar. O grupo $\{\pm 1\} \subseteq \mathbb{F}_p^*$, é o subgrupo de todos os elementos de $(\mathbb{F}_p)^*$ de ordem 2. Logo, a restrição de um homomorfismo de anéis $\psi : \mathbb{Z}[G] \rightarrow \mathbb{F}_p$ ao grupo G , é também um caracter $\chi : G \rightarrow \{\pm 1\}$. Assim, existe uma única extensão $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$ que faz o diagrama abaixo comutar

$$\begin{array}{ccc} \mathbb{Z}[G] & \xrightarrow{\phi_\chi} & \mathbb{Z} \\ & \searrow \psi & \swarrow \pi \\ & \mathbb{F}_p & \end{array}$$

onde π é a sobrejeção canônica de $\mathbb{Z}$ em $\mathbb{F}_p$.

Consideremos $p = 2$. Cada homomorfismo de $\mathbb{Z}[G]$ em $\mathbb{F}_2$, leva todo elemento de G em 1. Logo, existe um único homomorfismo de anéis $\psi_o : \mathbb{Z}[G] \rightarrow \mathbb{F}_2$, que é obtido da composição de $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$ com a projeção canônica sobre $\mathbb{F}_2$, onde ϕ_χ é a extensão de qualquer caracter $\chi : G \rightarrow \{\pm 1\}$.

Destas observações e do lema (2.5), temos

Proposição 2.6 (i) Para cada ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, com $\mathbb{Z} \cap \mathcal{P} = \{0\}$, existe um único caracter χ de G , tal que $\mathcal{P} = \mathcal{P}_\chi$ é o núcleo do homomorfismo $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$.
(ii) Para cada ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, com $\mathbb{Z} \cap \mathcal{P} = p\mathbb{Z}$, p um número primo ímpar, existe um único caracter χ de G , tal que $\mathcal{P}$ coincide com o conjunto

$$\mathcal{P}_{\chi,p} := \{z \in \mathbb{Z}[G]; \phi_\chi(z) \equiv 0 \pmod{p}\}.$$

(iii) Existe um único ideal $\mathcal{P}_0$ de $\mathbb{Z}[G]$ com $\mathbb{Z} \cap \mathcal{P}_0 = 2\mathbb{Z}$ e

$$\mathcal{P}_0 = \{z \in \mathbb{Z}[G]; \phi_\chi(z) \equiv 0 \pmod{2}\},$$

para cada caracter χ de G .

Dem.: Imediata. ■

Observação 2.7 É claro que os ideais $\mathcal{P}_\chi$, com χ percorrendo o conjunto dos caracteres de G , são todos os ideais primos minimais de $\mathbb{Z}[G]$. Os ideais $\mathcal{P}_{\chi,p}$ com χ percorrendo o conjunto dos caracteres de G , p o conjunto dos números primos ímpares e $\mathcal{P}_0$ são todos os ideais maximais de $\mathbb{Z}[G]$.

Consideremos agora, os ideais primos de $W(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$. Denotemos por $I(A)$ o núcleo do homomorfismo de anéis $d_0 : W(A) \rightarrow \mathbb{F}_2$, definido por $d_0([b]) = \dim b \pmod{2}$. Desde que $\frac{W(A)}{I(A)} \cong \mathbb{F}_2$ que é um corpo, temos que $I(A)$ é um ideal maximal de $W(A)$.

Proposição 2.8 $I(A)$ é o único ideal primo de $W(A)$ que contém $2 < 1 > = 2.1_{W(A)}$.

Dem.: Resta mostrarmos apenas a unicidade. O item (iii) da proposição anterior garante que $\mathcal{P}_0$ é o único ideal primo de $\mathbb{Z}[G]$ que contém (2). Como $\varphi(2) = 2 < 1 >$, temos que $I(A)$ corresponde ao ideal $\mathcal{P}_0$ de $\mathbb{Z}[G]$, na correspondência entre os ideais de $W(A)$ e os ideais de $\mathbb{Z}[G]$ que contém $\mathcal{K}$. Portanto, a unicidade de $I(A)$ decorre da unicidade de $\mathcal{P}_0$. ■

Para uma melhor caracterização dos ideais primos de $W(A)$, usaremos a noção de assinatura como definida abaixo.

Definição 2.9 Uma *assinatura* de A é um homomorfismo de anéis de $W(A)$ em $\mathbb{Z}$. Denotamos por $Ass(A)$ o conjunto de todas as assinaturas de A e, por $\mathcal{P}_\sigma$ o núcleo da assinatura σ . Dizemos que A é um anel *formalmente real* se A admite pelo menos uma assinatura, ou seja, se $Ass(A) \neq \emptyset$. Caso contrário, A é dito ser um anel *não formalmente real*.

Assumiremos primeiro, que A é um anel formalmente real, ou seja, que $Ass(A) \neq \emptyset$. Do Teorema do Isomorfismo para anéis, segue imediatamente que $\frac{W(A)}{\mathcal{P}_\sigma} \cong \mathbb{Z}$, para toda $\sigma \in Ass(A)$.

Proposição 2.10 Para cada ideal primo $\mathcal{P}$ de $W(A)$ que não contém $p < 1 >$ para todo número primo p , existe uma única assinatura σ de A tal que $\mathcal{P} = \mathcal{P}_\sigma$.

Dem.: Seja $\mathcal{P}$ um ideal primo de $W(A)$ que não contém $p < 1 >$ para todo número primo p . Desde que $W(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$, temos que existe $\mathcal{P}' = \varphi^{-1}(\mathcal{P})$, ideal primo de $\mathbb{Z}[G]$ tal que $\mathcal{K} \subseteq \mathcal{P}'$.

Como $p < 1 > \notin \mathcal{P}$ para todo número primo p , o ideal $\mathcal{P}'$ é tal que $\mathbb{Z} \cap \mathcal{P}' = \{0\}$. Pelo item (i) da proposição (2.6) existe um único homomorfismo de anéis $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$, tal que $\text{Ker } \phi_\chi = \mathcal{P}'$. Mas $\mathcal{K} \subseteq \text{Ker } \phi_\chi = \mathcal{P}'$. Logo, existe uma única $\sigma \in \text{Ass}(A)$ que faz o seguinte diagrama comutar

$$\begin{array}{ccc} \mathbb{Z}[G] & \xrightarrow{\phi_\chi} & \mathbb{Z} \\ & \searrow \varphi & \nearrow \sigma \\ & W(A) & \end{array}$$

Resta mostrarmos que $\mathcal{P} = \mathcal{P}_\sigma$. Desde que $\sigma(\mathcal{P}) = \sigma \circ \varphi(\mathcal{P}') = \phi_\chi(\mathcal{P}') = 0$, temos que $\mathcal{P} \subseteq \mathcal{P}_\sigma$. Por outro lado, dado $b \in \mathcal{P}_\sigma$, o fato de φ ser sobrejetora implica que existe $x \in \mathbb{Z}[G]$ tal que $\varphi(x) = b$. Assim, $\phi_\chi(x) = \sigma \circ \varphi(x) = \sigma(b) = 0$, ou seja $x \in \text{Ker } \phi_\chi = \mathcal{P}'$. Logo, $\varphi(x) = b \in \mathcal{P}$. Portanto $\mathcal{P}_\sigma \subseteq \mathcal{P}$, como queríamos. ■

Para analisarmos os ideais primos de $W(A)$ que contém $p < 1 >$, para algum primo ímpar p , necessitamos das informações sobre o ideal $\mathcal{K}$ contidas no seguinte lema.

Lema 2.11 *Para cada caracter χ de G , temos que $\phi_\chi(\mathcal{K}) = 0$ ou $\phi_\chi(\mathcal{K}) \subseteq 2^n \mathbb{Z}$, para algum $n \geq 1$.*

Dem.: Para cada caracter χ de G , basta analisarmos a ação de ϕ_χ nos geradores de $\mathcal{K}$. Como $\phi_\chi(1) = 1$, temos que ϕ_χ leva $(1) + (-1)$ em 0 ou 2.

Seja $z = \sum_{i=1}^n (\alpha_i) - \sum_{i=1}^n (\beta_i) \in \mathbb{Z}[G]$, tal que $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$. Sejam s o número de elementos $(\alpha_i) \in G$, $1 \leq i \leq n$, com $\phi_\chi(\alpha_i) = -1$ e t o número de elementos $(\beta_i) \in G$, $1 \leq i \leq n$, com $\phi_\chi(\beta_i) = 1$. Assim, $\phi_\chi(z) = -s + (n - s) + t - (n - t) = 2(t - s)$. Mas $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$, o que implica que seus

determinantes diferem por quadrados, ou seja,

$$\prod_{i=1}^n \alpha_i \equiv \prod_{i=1}^n \beta_i \pmod{(A^*)^2}, \quad \text{ou} \quad \prod_{i=1}^n (\alpha_i) = \prod_{i=1}^n (\beta_i) \quad \text{em } G.$$

Aplicando ϕ_χ nesta igualdade e usando que $\phi_\chi(\alpha^2) = 1$, para todo $\alpha \in A^*$, obtemos $(-1)^s = (-1)^t$, isto é, $t - s$ é um número par. Consequentemente, $\phi_\chi(z) \equiv 0 \pmod{4}$. Portanto, $\phi_\chi(\mathcal{K}) = 0$ ou $\phi_\chi(\mathcal{K}) \subseteq 2^n \mathbb{Z}$, para algum $n \geq 1$. ■

Corolário 2.12 *Se $\phi_\chi(\mathcal{K}) \subseteq p\mathbb{Z}$, para algum primo ímpar p , então $\phi_\chi(\mathcal{K}) = 0$.*

Dem.: Imediata. ■

Proposição 2.13 *Seja p um número primo ímpar. Para cada ideal primo $\mathcal{P}$ de $W(A)$ com $p < 1 > \in \mathcal{P}$, existe uma única assinatura σ de A tal que $\mathcal{P}$ coincide com o conjunto*

$$\mathcal{P}_{\sigma,p} = \{b \in W(A); \sigma(b) \equiv 0 \pmod{p}\}.$$

Dem.: Seja $\mathcal{P}$ um ideal primo de $W(A)$ com $p < 1 > \in \mathcal{P}$. Novamente pelo isomorfismo $W(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$ temos que existe $\mathcal{P}' \subseteq \mathbb{Z}[G]$ tal que $\mathcal{K} \subseteq \mathcal{P}'$ e $\varphi(\mathcal{P}') = \mathcal{P}$. Como $p < 1 > \in \mathcal{P}$, temos que $\mathbb{Z} \cap \mathcal{P}' = p\mathbb{Z}$. Por (2.6), temos que existe um único caracter χ de G , tal que $\mathcal{P}' = \mathcal{P}_{\chi,p} = \{z \in \mathbb{Z}[G]; \phi_\chi(z) \equiv 0 \pmod{p}\}$.

Do fato que $\mathcal{K} \subseteq \mathcal{P}' = \mathcal{P}_{\chi,p}$, segue que $\phi_\chi(\mathcal{K}) \subseteq p\mathbb{Z}$. Assim, de (2.12), temos que $\phi_\chi(\mathcal{K}) = 0$. Logo $\mathcal{K} \subseteq \text{Ker } \phi_\chi$ e, consequentemente, existe uma única $\sigma \in \text{Ass}(A)$ que faz o diagrama abaixo comutar

$$\begin{array}{ccc} \mathbb{Z}[G] & \xrightarrow{\phi_\chi} & \mathbb{Z} \\ & \searrow \varphi & \nearrow \sigma \\ & W(A) & \end{array}$$

Mostremos agora que $\mathcal{P} = \mathcal{P}_{\sigma,p}$. Dado $b \in \mathcal{P}$, existe $x \in \mathcal{P}'$ tal que $\varphi(x) = b$, pois $\mathcal{P}' = \varphi^{-1}(\mathcal{P})$. Da definição de $\mathcal{P}'$, temos que $\phi_x(x) \equiv 0 \pmod{p}$. Assim, $\sigma(b) = \sigma \circ \varphi(x) = \phi_x(x) \equiv 0 \pmod{p}$, ou seja, $b \in \mathcal{P}_{\sigma,p}$, o que mostra que $\mathcal{P} \subseteq \mathcal{P}_{\sigma,p}$. Seja agora $b \in \mathcal{P}_{\sigma,p}$. Segue da sobrejetividade de φ que existe $x \in \mathbb{Z}[G]$ tal que $\varphi(x) = b$. Assim, $\phi_x(x) = \sigma \circ \varphi(x) = \sigma(b) \equiv 0 \pmod{p}$, ou seja, $x \in \mathcal{P}'$. Logo, $b = \varphi(x) \in \mathcal{P}$. Portanto, $\mathcal{P}_{\sigma,p} = \mathcal{P}$, como queríamos. ■

De (2.6) e da correspondência entre os ideais de $W(A)$ com os ideais de $\mathbb{Z}[G]$, que contém $\mathcal{K}$, concluímos que se $\text{Ass}(A) \neq \emptyset$ então $\mathcal{P}_\sigma$, $\mathcal{P}_{\sigma,p}$, para cada $\sigma \in \text{Ass}(A)$ e todo número primo ímpar p , e $I(A)$ são todos os ideais primos de $W(A)$.

Teorema 2.14 *Se A é um anel local formalmente real, então*

- (i) *Os $\mathcal{P}_\sigma$, com $\sigma \in \text{Ass}(A)$, são todos os ideais primos minimais de $W(A)$.*
- (ii) *Os $\mathcal{P}_{\sigma,p}$ com $\sigma \in \text{Ass}(A)$ e p um número primo ímpar, e $I(A)$ são todos os ideais primos maximais de $W(A)$.*
- (iii) *Cada $\mathcal{P}_{\sigma,p}$ contém um único ideal primo minimal, a saber $\mathcal{P}_\sigma$.*
- (iv) *$I(A)$ contém todos os ideais primos minimais.*

Dem.: Resta apenas mostrarmos (iii) e (iv). Em $\mathbb{Z}$ existe um único ideal maximal que contém p . Então, devido ao isomorfismo $W(A)/\mathcal{P}_\sigma \cong \mathbb{Z}$, existe um único ideal maximal de $W(A)$ que contém $p < 1 >$ e $\mathcal{P}_\sigma$, que é claramente $\mathcal{P}_{\sigma,p}$. Suponhamos que exista um ideal primo minimal $\mathcal{P}_\psi$ de $W(A)$, tal que $\mathcal{P}_\psi$ também está contido em $\mathcal{P}_{\sigma,p}$. Como $\mathcal{P}_{\sigma,p}$ contém $\mathcal{P}_\psi$ e $p < 1 >$ temos que $\mathcal{P}_{\sigma,p} = \mathcal{P}_{\psi,p}$. Segue então de (2.13) que $\sigma = \psi$. Portanto $\mathcal{P}_\sigma = \mathcal{P}_\psi$, o que mostra (iii).

Agora, queremos mostrar que $\mathcal{P}_\sigma \subseteq I(A)$, para cada $\sigma \in \text{Ass}(A)$. Para tanto, seja $b = \langle \alpha_1, \dots, \alpha_n \rangle \in \mathcal{P}_\sigma$. Como $\sigma(\langle \alpha_i \rangle) = \pm 1$, para $1 \leq i \leq n$ e, $\sigma(b) = 0$, temos que para metade dos índices $i = 1, \dots, n$, $\sigma(\langle \alpha_i \rangle) = 1$, e para a outra metade $\sigma(\langle \alpha_i \rangle) = -1$. Logo, $\dim b = n = 2m$, o que mostra que $b \in I(A)$. Portanto $\mathcal{P}_\sigma \subseteq I(A)$, como queríamos. ■

Para o caso em que A é um anel local não formalmente real temos

Teorema 2.15 *O anel local A é não formalmente real se, e somente se $I(A)$ é o único ideal primo de $W(A)$.*

Dem.: Da descrição dos ideais de $\mathbb{Z}[G]$, temos claramente que se $\text{Ass}(A) = \emptyset$, então $I(A)$ é o único ideal primo de $W(A)$. Reciprocamente se $I(A)$ é o único ideal primo de $W(A)$, então $I(A)$ é o nilradical de $W(A)$, isto é, o conjunto de todos os elementos nilpotentes de $W(A)$. Em particular, $2\langle 1 \rangle \in I(A)$ é nilpotente. Assim existe $n \geq 1$ tal que $2^n \langle 1 \rangle = (2\langle 1 \rangle)^n = 0$ em $W(A)$, o que implica que $\langle 1 \rangle \in W(A)$ é um elemento de torção. Como $\mathbb{Z}$ é um anel livre de torção e assumimos que todo homomorfismo de anéis leva elemento identidade em elemento identidade, temos que não existe homomorfismo de anéis de $W(A)$ em $\mathbb{Z}$, ou seja, A é não formalmente real. ■

Como uma consequência imediata deste teorema temos

Corolário 2.16 *Se A é um anel local não formalmente real, então os divisores de zero de $W(A)$ tem dimensão par.*

Dem.: Imediata. ■

2.3 $\text{Nil}(W(A))$ e $W_t(A)$.

Nesta seção apresentamos alguns resultados sobre os elementos de torção, os elementos nilpotentes e os divisores de zero do anel de Witt de A .

Desde que $W(A)$ é um anel comutativo com elemento identidade $\langle 1 \rangle$, o conjunto dos elementos nilpotentes de $W(A)$ formam um subgrupo aditivo que denotaremos

por $\text{Nil}(W(A))$. O subgrupo dos elementos de torção de $W(A)$ será denotado por $W_t(A)$.

Em um anel R , um elemento de torção $x \in R$ é dito ter p -torção, $p \in \mathbb{Z}$, um número primo, se x é anulado por uma potência de p . Dentre os resultados apresentados nesta seção, mostraremos que o anel $W(A)$ tem somente 2-torção.

Ao contrário da seção anterior, assumiremos primeiramente que A é um anel local não formalmente real. Neste caso, como consequência imediata do teorema (2.15) e sua demonstração, temos

Teorema 2.17 *Se A é um anel local não formalmente real, então*

- (i) $\text{Nil}(W(A)) = I(A)$.
- (ii) $W_t(A) = W(A)$.
- (iii) $W(A)$ tem somente 2-torção.

Dem.: Imediata. ■

Agora seja A um anel local formalmente real. Desde que os $\mathcal{P}_\sigma$ com $\sigma \in \text{Ass}(A)$, são todos os ideais primos minimais de $W(A)$, temos

Proposição 2.18 *Se $\text{Ass}(A) \neq \emptyset$, então um elemento $b \in W(A)$ é nilpotente se, e somente se $\sigma(b) = 0$ para toda $\sigma \in \text{Ass}(A)$, isto é, $\text{Nil}(W(A)) = \bigcap_{\sigma \in \text{Ass}(A)} \text{Ker } \sigma$.*

Dem.: Imediata. ■

Para o subgrupo de torção temos

Proposição 2.19 *Se A é um anel local formalmente real, então $W_t(A) = \text{Nil}(W(A))$.*

Dem.: Sejam $b \in W_t(A)$ e $n \in \mathbb{N}$, $n \geq 1$, tal que $nb = 0$. Então, para cada $\sigma \in \text{Ass}(A)$, temos $\sigma(nb) = n\sigma(b) = 0$, o que implica que $\sigma(b) = 0$. Assim, b

pertence a $\bigcap_{\sigma \in \text{Ass}(A)} \text{Ker} \sigma = \text{Nil}(W(A))$, o que mostra que $W_t(A) \subseteq \text{Nil}(W(A))$.

Reciprocamente, dado $b = \langle \alpha_1, \dots, \alpha_n \rangle \in \text{Nil}(W(A))$; consideremos H o subgrupo de G gerado por $\{(\alpha_1), \dots, (\alpha_n)\}$. Então, desde que todo elemento de G tem ordem 2, temos que H é um subgrupo finito de G e z está no subanel R de $W(A)$ isomorfo à $\frac{\mathbb{Z}[H]}{(\mathcal{K} \cap \mathbb{Z}[H])}$. Usando o teorema de Maschke (ver (3.6) em [9]) temos que o anel de grupo $\mathbb{Q}[H] \cong \mathbb{Q} \otimes \mathbb{Z}[H]$ é semi-simples, isto é, $\text{Nil}(\mathbb{Q}[H]) = \{0\}$.

Considerando que $R \cong \mathbb{Z}[H]$, implica que $\mathbb{Q} \otimes \mathbb{Z}[H] \cong \mathbb{Q} \otimes R$, temos por (3.1.b) de [9], que $\text{Nil}(\mathbb{Q} \otimes R) = \{0\}$.

Mas, $1 \otimes b \in \mathbb{Q} \otimes \text{Nil}(R) \subseteq \text{Nil}(\mathbb{Q} \otimes R) = \{0\}$. Também identificando $\mathbb{Q} \otimes R$ com $T^{-1}(\mathbb{Z}) \otimes R \cong T^{-1}(R)$, onde $T = \mathbb{Z} - \{0\}$, temos $0 = 1 \otimes b = \frac{b}{1} \in T^{-1}(R)$, o que é equivalente a existir $n \in T$, $n \geq 1$, tal que $nb = 0$ em R . Assim, $b \in R_t \subseteq W_t(A)$, o que mostra a proposição. ■

Das duas últimas proposições, deduzimos imediatamente o Princípio Local-Global de Pfister para espaços bilineares sobre um anel local formalmente real.

Teorema 2.20 (Princípio Local-Global de Pfister) *Seja A um anel local formalmente real. Então uma forma bilinear b representa um elemento de torção em $W(A)$ se, e somente se $\sigma(b) = 0$, para toda $\sigma \in \text{Ass}(A)$.*

Dem.: Imediata. ■

Mostremos agora que também no caso em que A é formalmente real $W(A)$ tem somente 2-torção.

Teorema 2.21 *Se A é um anel local formalmente real, então $W(A)$ tem somente 2-torção.*

Dem.: Seja $b = \langle \alpha_1, \dots, \alpha_n \rangle \in W_t(A)$. Desde que $W_t(A) = \text{Nil}(W(A))$, temos que $b \in \text{Nil}(W(A))$ e, como na demonstração da proposição anterior, b está no

subanel R de $W(A)$ isomorfo à $\frac{\mathbb{Z}[H]}{(\mathcal{K} \cap \mathbb{Z}[H])}$, onde H é o subgrupo de G gerado por $\{(\alpha_1), \dots, (\alpha_n)\}$. Agora, para mostrarmos que b é 2-torção em $W(A)$, é suficiente mostrarmos que o anel R não tem p -torção, para todo número primo ímpar p .

Seja p um número primo ímpar qualquer. Desde que $R \cong \frac{\mathbb{Z}[H]}{(\mathcal{K} \cap \mathbb{Z}[H])}$, temos que $\frac{R}{pR} \cong \frac{\mathbb{F}_p[H]}{K'}$, para algum subgrupo K' de $\mathbb{F}_p[H]$.

Como $H \subseteq G$, temos que os elementos de H tem ordem 2. Desde que $\mathbb{F}_p$ tem característica p um primo ímpar, novamente pelo teorema de Maschke, obtemos que R/pR é um anel semi-simples, ou seja, $\text{Nil}(R/pR) = \{0\}$.

Se $b_0 \in R$ é nilpotente, então $\overline{b_0} \in \text{Nil}(R/pR) = \{0\}$, ou seja, existe $b_1 \in R$ tal que $b_0 = pb_1$. Isto, e o fato que $W_t(A) = \text{Nil}(W(A))$, mostra que o subgrupo de torção R_t de R é divisível por cada número primo ímpar, isto é, $R_t = pR_t$ para cada número primo ímpar p .

Se $b_0 \in R$ tem p -torção, então $b_0 \in R_t = pR_t$, ou seja, $b_0 = pb_1$, com b_1 em R_t que também tem p -torção, o que implica que $b_1 = pb_2$, para algum $b_2 \in R_t$ e consequentemente, $b_0 = p^2b_2$. Assim, para cada inteiro $n \geq 0$, existe $b_n \in R_t$, onde b_n tem p -torção e $b_0 = p^n b_n$.

Mas R é um grupo abeliano finitamente gerado, então pela decomposição dos $\mathbb{Z}$ -módulos finitamente gerado, temos que R_t é um grupo finito. Logo, existe $N > 0$ tal que $p^N b' = 0$, para todo $b' \in R_t$ com p -torção. Logo $b_0 = p^N b_N = 0$ em R . Como p é um número primo ímpar qualquer, temos que R não tem p -torção, para todo número primo ímpar p , como queríamos. ■

Como consequência do teorema anterior deduzimos que também no caso em que A é formalmente real, os divisores de zero de $W(A)$ tem dimensão par.

Corolário 2.22 *Os divisores de zero de $W(A)$ tem dimensão par.*

Dem.: De (1.3), temos que o conjunto dos divisores de zero de $W(A)$ é uma união de ideais primos. Suponhamos que $p < 1 >$ é um divisor de zero, para algum número

primo ímpar p . Então existe $b \in W(A)$, $b \neq 0$, tal que $p \langle 1 \rangle \otimes b = 0$ em $W(A)$, o que implica que b tem p -torção em $W(A)$. Mas, do teorema anterior temos que $W(A)$ tem somente 2-torção. Assim, $p \langle 1 \rangle$ não é divisor de zero para nenhum primo ímpar p . Assim na união dos divisores de zero, não aparece os ideais primos da forma $P_{\sigma,p}$, com $\sigma \in \text{Ass}(A)$ e p um número primo ímpar, ou seja de (2.14) temos que cada ideal primo que aparece na união é minimal ou $I(A)$. Desde que $P_\sigma \subseteq I(A)$, para todo $\sigma \in \text{Ass}(A)$, o resultado segue. ■

No restante deste trabalho, para simplificar a notação, denotaremos as operações $\perp$ e $\otimes$ em $W(A)$ por $+$ e $\cdot$ respectivamente. Também denotaremos por b^n o elemento $b \otimes b \otimes \dots \otimes b$ (n -vezes) em $W(A)$. Mais ainda, salvo menção em contrário, todas as igualdades envolvendo espaços bilineares são igualdades de elementos de $W(A)$.

Apesar de termos provado que em $W(A)$, todo elemento de torção tem ordem uma potência de 2, não temos uma descrição mais detalhada de como é a forma de tais elementos. Para o caso em que 2 é uma unidade em A , como consequência do próximo teorema, apresentamos uma tal descrição.

Teorema 2.23 *Seja A um anel local com $2 \in A^*$. Se b_1 e $b_2 \in \text{Bil}(A)$, com b_1 uma forma de Pfister anisotrópica, são tais que $b_1 \cdot b_2 = 0$ em $W(A)$, então*

$$b_2 = \langle \gamma_1 \rangle \cdot \langle 1, -\beta_1 \rangle + \dots + \langle \gamma_n \rangle \cdot \langle 1, -\beta_n \rangle,$$

para algum inteiro $n \geq 0$, $\gamma_1, \dots, \gamma_n \in A^*$ e $\beta_1, \dots, \beta_n \in \mathcal{D}(b_1)$.

Dem.: Como $2 \in A^*$, temos que b_2 admite uma decomposição da forma $\langle \alpha_1, \dots, \alpha_m \rangle$, com $\alpha_1, \dots, \alpha_m \in A^*$. Além disso, por hipótese $b_1 \cdot b_2 = 0$ em $W(A)$. Então

$$b_1 \cdot b_2 = \langle \alpha_1 \rangle \cdot b_1 + \dots + \langle \alpha_m \rangle \cdot b_1 = 0,$$

ou seja, $\langle -\alpha_1 \rangle \cdot b_1 = \langle \alpha_2 \rangle \cdot b_1 + \dots + \langle \alpha_m \rangle \cdot b_1$ em $W(A)$.

Como $1 \in \mathcal{D}(b_1)$, temos

$$-\alpha_1 \cdot 1 \in (-\alpha_1) \mathcal{D}(b_1) = \mathcal{D}(\langle -\alpha_1 \rangle \otimes b_1) \subseteq \mathcal{D}(\langle \alpha_2 \rangle \otimes b_1 \perp \cdots \perp \langle \alpha_m \rangle \otimes b_1).$$

Assim, de (1.27), segue que $-\alpha_1 \in \mathcal{D}(\langle \alpha_2 \alpha'_2, \dots, \alpha_m \alpha'_m \rangle)$ onde $\alpha'_i \in \mathcal{D}(b_1)$, para cada $i = 2, \dots, m$. Agora, do lema (1.25), temos que $\langle \alpha_2 \alpha'_2, \dots, \alpha_m \alpha'_m \rangle \simeq \langle -\alpha_1 \rangle \perp b'$, para algum $b' \in \text{Bil}(A)$. Adicionando $\langle -\alpha_1 \rangle$ a ambos os lados, obtemos $\langle \alpha_1, -\alpha_1 \rangle \perp b' \simeq \langle \alpha_1, \alpha_2 \alpha'_2, \dots, \alpha_m \alpha'_m \rangle$, ou seja, $b' = \langle \alpha_1, \alpha_2 \alpha'_2, \dots, \alpha_m \alpha'_m \rangle$ em $W(A)$.

Agora, em $W(A)$ temos as seguintes identidades

$$\begin{aligned} b_2 &= \langle \alpha_1, \dots, \alpha_m \rangle = \\ &= \langle \alpha_1, \dots, \alpha_m \rangle + \langle \alpha_2 \alpha'_2, \dots, \alpha_m \alpha'_m \rangle + \langle -\alpha_2 \alpha'_2, \dots, -\alpha_m \alpha'_m \rangle = \\ &= \langle \alpha_1, \alpha_2 \alpha'_2, \dots, \alpha_m \alpha'_m \rangle + \langle \alpha_2 \rangle \cdot \langle 1, -\alpha'_2 \rangle + \cdots + \langle \alpha_m \rangle \cdot \langle 1, -\alpha'_m \rangle = \\ &= b' + \langle \alpha_2 \rangle \cdot \langle 1, -\alpha'_2 \rangle + \cdots + \langle \alpha_m \rangle \cdot \langle 1, -\alpha'_m \rangle. \end{aligned}$$

Desde que b_1 é uma forma de Pfister e $\alpha'_i \in \mathcal{D}(b_1)$, para $2 \leq i \leq m$, de (1.34) temos que $\langle 1, -\alpha'_i \rangle \otimes b_1 \simeq b_1 \perp \langle -\alpha'_i \rangle \otimes b_1 \simeq b_1 \perp (-b_1)$. Consequentemente, $\langle 1, -\alpha'_i \rangle \otimes b_1 = 0$ em $W(A)$, para cada $i = 2, \dots, m$. Portanto $b' \cdot b_1 = b_2 \cdot b_1 = 0$ em $W(A)$.

Agora o resultado segue por indução sobre a dimensão de b_2 , pois $\dim b' = \dim b_2 - 2$. ■

Para todo $k \geq 0$, é fácil ver que $2 \langle 1 \rangle$ é uma k -forma de Pfister e, de (1.34) temos que $\mathcal{D}(2^k \langle 1 \rangle)$ é um subgrupo de A^* . Com isso, temos em particular que o produto de duas somas de 2^k quadrados é ainda uma soma de 2^k quadrados.

Corolário 2.24 *Se $2^k \langle 1 \rangle$ é anisotrópico, então o ideal de $W(A)$,*

$$\text{Ann}(2^k \langle 1 \rangle) = \{b \in W(A); 2^k b = 0\},$$

é gerado pelos elementos da forma $\langle 1, -\alpha \rangle$, onde $\alpha \in A^$ é uma soma de 2^k quadrados.*

Dem.: Observando que o conjunto dos elementos de A^* , que são somas de 2^k quadrados, é igual a $\mathcal{D}(2^k < 1 >)$ e aplicando o teorema anterior para a k -forma de Pfister $2^k < 1 >$, o resultado segue. ■

Capítulo 3

As unidades no Anel de Witt

Neste capítulo apresentamos alguns resultados sobre as unidades do anel de Witt dos espaços bilineares sobre um anel local A . Estes resultados são generalizações para anéis locais dos apresentados por Lewis em [7] para corpos de característica distinta de 2. Denotaremos o grupo das unidades de $W(A)$ por $W(A)^*$. Como uma consequência imediata de (2.15) temos

Proposição 3.1 *Se A é um anel local não formalmente real, então $b \in W(A)$ é uma unidade se, e somente se $\dim b$ é um número ímpar.*

Dem.: Se A é não formalmente real, de (2.15), temos que $W(A)$ é um anel comutativo local com único ideal maximal $I(A)$. Assim $W(A)^* = W(A) - I(A)$, que é exatamente o conjunto dos elementos de $W(A)$ que são representados por formas bilineares de dimensão ímpar. ■

Para o caso em que A é formalmente real temos

Proposição 3.2 *Se A é um anel local formalmente real, então $b \in W(A)$ é uma unidade se, e somente se $\sigma(b) = \pm 1$, para cada $\sigma \in \text{Ass}(A)$.*

Dem.: Seja $b \in W(A)$ uma unidade. Então existe $b_1 \in W(A)$ tal que $b \cdot b_1 = \langle 1 \rangle$. Assim, para cada $\sigma \in \text{Ass}(A)$, temos $\sigma(b \cdot b_1) = \sigma(b)\sigma(b_1) = \sigma(\langle 1 \rangle) = 1$, ou seja, $\sigma(b) = \pm 1$.

Reciprocamente, se $\sigma(b) = \pm 1$ para cada $\sigma \in \text{Ass}(A)$, então $\sigma(b^2 + \langle -1 \rangle) = \sigma((b + \langle 1 \rangle) \cdot (b + \langle -1 \rangle)) = 0$, para cada $\sigma \in \text{Ass}(A)$. Assim, do Princípio Local-Global de Pfister, temos que $b_1 = b^2 + \langle -1 \rangle \in \text{Nil}(W(A))$. Portanto, de (1.2) segue que $b^2 = \langle 1 \rangle + b_1$ é invertível e, conseqüentemente $b \in W(A)^*$, como queríamos. ■

Nos próximos três resultados, analisamos as unidades de $W(A)$ com relação à sua ordem no grupo multiplicativo $W(A)^*$, ou seja, a *ordem* de uma unidade $b \in W(A)$ é a ordem de b como elemento no grupo $W(A)^*$.

Proposição 3.3 *Se b é uma unidade de ordem finita em $W(A)$, então sua ordem é uma potência de 2.*

Dem.: Seja $b \in W(A)$ uma unidade de ordem finita $k > 0$, isto é, $b^k = \langle 1 \rangle$ e $b^i \neq \langle 1 \rangle$ para $1 \leq i < k$. De $b^k = \langle 1 \rangle$, temos que b é necessariamente de dimensão ímpar. Em $W(A)$, podemos escrever

$$b^k + \langle -1 \rangle = (b + \langle -1 \rangle) \cdot (b^{k-1} + b^{k-2} + \dots + b + \langle 1 \rangle) = 0.$$

Se k é um inteiro ímpar, então o elemento $b^{k-1} + b^{k-2} + \dots + b$ de $W(A)$ tem dimensão par e, conseqüentemente $b^{k-1} + \dots + b + \langle 1 \rangle$ tem dimensão ímpar. Como, de (2.16) e (2.22), os divisores de zero de $W(A)$ tem dimensão par, a equação $b^k = \langle 1 \rangle$ não é possível para k ímpar. Logo, a ordem da unidade b é par, ou seja, $k = mn$ onde m é um número inteiro ímpar e n é uma potência de 2. Se $m \neq 1$, então o argumento acima pode ser aplicado para b^n , ou seja,

$$0 = (b^n)^m + \langle -1 \rangle = (b^n + \langle -1 \rangle) \cdot ((b^n)^{m-1} + \dots + b^n + \langle 1 \rangle),$$

o que nos leva a uma contradição novamente. Portanto, $m = 1$ e $k = n$ é uma potência de 2, como queríamos. ■

Proposição 3.4 *Todos os elementos de $W(A)$ da forma $\langle 1 \rangle + b$ com b em $Nil(W(A))$, são unidades de ordem potência de 2.*

Dem.: Se $b \in Nil(W(A))$, então de (2.19) e (2.21), temos que existem inteiros l e k tais que $b^l = 2^k b = 0$. Agora, se $2^i \leq m < 2^{i+1}$ então, de (1.8), 2^{r-i} divide o coeficiente binomial

$$\binom{2^r}{m}$$

e, conseqüentemente, 2 também divide o coeficiente binomial.

Assim, podemos escrever

$$(\langle 1 \rangle + b)^{2^r} = \langle 1 \rangle + 2n_1 b + 2n_2 b \cdot b + 2n_3 b^2 \cdot b + \dots + 2n_{2^r-1} b^{2^r-2} \cdot b + b^{2^r} = \langle 1 \rangle + 2b_r \cdot b + b^{2^r},$$

para algum $b_r \in W(A)$. Logo, se $2^r > l$, temos a igualdade

$$(\langle 1 \rangle + b)^{2^r} = 1 + 2b_r \cdot b. \quad (1)$$

Mostremos agora que para todo $b_1 \in W(A)$, existe $b'_1 \in W(A)$ tal que

$$(\langle 1 \rangle + 2b_1)^{2^k} = \langle 1 \rangle + 2^{k+1} b'_1 \cdot b_1. \quad (2)$$

Mostremos esta igualdade por indução sobre k . Para $k = 1$, basta tomar $b'_1 = \langle 1 \rangle + b_1$. Suponhamos que a igualdade é válida para $n \leq k$. Assim

$$\begin{aligned} (\langle 1 \rangle + 2b_1)^{2^{k+1}} &= ((\langle 1 \rangle + 2b_1)^{2^k})^2 = \\ &= (\langle 1 \rangle + 2^{k+1} b'_1 \cdot b_1)^2 = \\ &= (\langle 1 \rangle + 22^k b'_1 \cdot b_1)^2 = \\ &= (\langle 1 \rangle + 2^{k+2} b_1'' \cdot b_1), \end{aligned}$$

para algum $b_1'' \in W(A)$.

Agora, se $2^r > l$ temos que as igualdades de (1) e (2) são verificadas e, consequentemente

$$(<1> + b)^{2^{r+k-1}} = ((<1> + b)^{2^r})^{2^{k-1}} = (<1> + 2b_r \cdot b)^{2^{k-1}},$$

para algum $b_r \in W(A)$. Ou seja, $(<1> + b)^{2^{r+k-1}} = <1> + 2^k b_1 \cdot b$, para algum $b_1 \in W(A)$.

Mas $2^k b = 0$, então $(<1> + b)^{2^{r+k-1}} = <1>$, ou seja a ordem da unidade $<1> + b$ é uma potência de 2. ■

Proposição 3.5 *Toda unidade em $W(A)$ tem ordem finita.*

Dem.: Seja $b \in W(A)^*$. Podemos escrever $b^2 = <1> + b_1$, com $b_1 = b^2 + <-1>$. Da proposição anterior, é suficiente mostrarmos que $b_1 \in Nil(W(A))$.

Se $Ass(A) = \emptyset$, então de (3.1), temos que $\dim b$ é ímpar e, neste caso, basta observarmos que $b_1 = (b + <1>) \cdot (b + <-1>) \in I^2(A) \subseteq Nil(W(A)) = I(A)$. Se $Ass(A) \neq \emptyset$ e b é uma unidade, então pela proposição (3.2), $\sigma(b) = \pm 1$, para cada $\sigma \in Ass(A)$. Assim, $\sigma(b_1) = \sigma(b^2 + <-1>) = 0$, para toda $\sigma \in Ass(A)$, o que implica que b_1 é um elemento torção e, neste caso, o resultado segue da proposição (2.19). ■

Juntando as proposições (3.3) e (3.5) obtemos

Teorema 3.6 *Todo elemento de $W(A)^*$ tem ordem potência de 2.*

Dem.: Imediata. ■

Exemplo 3.7 Se A é um corpo finito de característica distinta de 2 ou o anel dos inteiros p -ádicos, então $b^2 = <1>$ para toda unidade b em $W(A)$. De fato, seja

$(M, b) \in \text{Bil}(A)$ com $\dim b \geq 5$, onde A é um corpo finito com $\text{car } A \neq 2$, ou o anel dos inteiros p -ádicos. Então b é uma forma bilinear isotrópica (ver[11]).

Temos também que, se (M, b) é um espaço bilinear isotrópico, então existe $w_1 \in M$ primitivo tal que $b(w_1, w_1) = 0$. Por outro lado, (M, b) não singular implica que existe $w_2 \in M$ tal que $b(w_1, w_2) \in A^*$. Assim $(Aw_1 \oplus Aw_2, b)$ é um subespaço metabólico não singular de (M, b) . Logo de (1.13)

$$(M, b) \simeq (Aw_1 \oplus Aw_2, b) \perp (V, b)$$

ou seja, $(M, b) = (V, b)$ em $W(A)$ e $\dim V = \dim M - 2$.

Repetindo esse raciocínio, concluímos que $(M, b) = (N, b)$ em $W(A)$, onde (N, b) é um espaço bilinear anisotrópico, com $\dim N < 5$.

Assim, as únicas possíveis unidades de $W(A)$ neste caso, são as representadas por formas anisotrópicas b com $\dim b = 1$ ou $\dim b = 3$. Se $b = \langle \alpha \rangle$, com $\alpha \in A^*$, claramente $b^2 = \langle 1 \rangle$. Se $b = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$, é fácil verificar que

$$b^2 = \langle \alpha_1, \alpha_2, \alpha_3 \rangle^2 = \langle 1 \rangle \perp 2 \langle 1, \alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_2\alpha_3 \rangle.$$

Agora,

$$2 \langle 1, \alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_2\alpha_3 \rangle = \langle 1, \alpha_1\alpha_2 \rangle \otimes \langle 1, \alpha_1\alpha_3 \rangle \otimes \langle 1, 1 \rangle = \ll 1, \alpha_1\alpha_2, \alpha_1\alpha_3 \gg,$$

que é isotrópica, pois $\dim (2 \langle 1, \alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_2\alpha_3 \rangle) > 5$.

Como $(2 \langle 1, \alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_2\alpha_3 \rangle)$ é uma forma de Pfister e 2 é uma unidade em A , de (1.36), temos que esta forma é hiperbólica. Consequentemente, $b^2 = \langle 1 \rangle$ em $W(A)$.

No próximo teorema daremos uma caracterização das unidades de $W(A)$ em termos dos elementos de torção e/ou nilpotentes de $W(A)$. Para tanto necessitaremos da caracterização dos geradores do ideal fundamental $I(A)$ que veremos no próximo lema.

Lema 3.8 O ideal $I(A)$ de $W(A)$ é aditivamente gerado pelas formas do tipo $\langle 1, \alpha \rangle$, com $\alpha \in A^*$.

Dem.: Obviamente as formas do tipo $\langle 1, \alpha \rangle$ pertencem a $I(A)$. Seja $b = \langle \alpha_1, \dots, \alpha_n \rangle \in I(A)$, onde $n = 2m$ para algum m . Temos então

$$\langle \alpha_1, \dots, \alpha_n \rangle = \sum_{i=1}^m \langle 1, \alpha_i \rangle - \sum_{i=m+1}^n \langle 1, -\alpha_i \rangle$$

em $W(A)$, o que mostra o lema. ■

No que segue, identificaremos o grupo $G = A^*/A^{*2}$ com sua imagem $\{\langle \alpha \rangle; (\alpha) \in G\}$ em $W(A)$.

Teorema 3.9 (i) Se $\text{Ass}(A) = \emptyset$ então, $W(A)^* = \langle 1 \rangle + I(A)$.

(ii) Se $\text{Ass}(A) \neq \emptyset$ então, $W(A)^* = G \cdot (\langle 1 \rangle + W_t(A))$.

Dem.: (i) Desde que $\text{Ass}(A) = \emptyset$, temos de (2.15) que $I(A)$ é o único ideal maximal do anel local $W(A)$. Assim $W(A)^* = W(A) - I(A)$. Se $b \in W(A) - I(A)$, então $b = \langle \alpha \rangle + b_1$, para algum $\alpha \in A^*$ e $b_1 \in I(A)$. Assim, de (3.8), existem $\alpha_1, \dots, \alpha_n \in A^*$ tais que

$$\begin{aligned} b &= \langle \alpha \rangle + \sum_{i=1}^n \langle 1, \alpha_i \rangle = \\ &= \langle \alpha \rangle + \langle 1 \rangle + \langle \alpha_1 \rangle + \langle 1 \rangle + \langle \alpha_2 \rangle + \dots + \langle 1 \rangle + \langle \alpha_n \rangle = \\ &= \langle 1 \rangle + \langle \alpha \rangle + \langle \alpha_1 \rangle + \langle 1 \rangle + \langle \alpha_2 \rangle + \dots + \langle 1 \rangle + \langle \alpha_n \rangle = \\ &= \langle 1 \rangle + b', \end{aligned}$$

para algum $b' \in I(A)$, o que mostra que $b \in \langle 1 \rangle + I(A)$, ou seja, $W(A)^* \subseteq \langle 1 \rangle + I(A)$. A outra inclusão é imediata.

(ii) Se $\text{Ass}(A) \neq \emptyset$, usando o Princípio Local-Global de Pfister, para cada $b \in W_t(A)$ e $\sigma \in \text{Ass}(A)$, temos $\sigma(\langle 1 \rangle + b) = \sigma(\langle 1 \rangle) + \sigma(b) = 1$. Portanto, de (3.2), temos que $1 + W_t(A) \subseteq W(A)^*$. Como $\langle \alpha \rangle^2 = \langle 1 \rangle$, para todo $\langle \alpha \rangle \in G = A^*/A^{*2}$, temos que $G \subseteq W(A)^*$. Assim, $G \cdot (1 + W_t(A)) \subseteq W(A)^*$.

Reciprocamente, se $b = \langle \alpha_1, \dots, \alpha_n \rangle \in W(A)^*$, considere,

$$s = (-1)^{\frac{n(n-1)}{2}} \alpha_1 \cdot \dots \cdot \alpha_n \in A^*.$$

Para cada $\sigma \in \text{Ass}(A)$, seja k o número de índices i 's com $\sigma(\langle \alpha_i \rangle) = -1$. Temos então $\sigma(b) = (n - k) - k = n - 2k$, ou seja, $n = 2k + \sigma(b)$. Mas, como $b \in W(A)^*$, de (3.2) temos que $\sigma(b) \in \{1, -1\}$. Se $\sigma(b) = 1$, temos que $(-1)^{\frac{n(n-1)}{2}} = ((-1)^{2k+1})^{\frac{2k}{2}} = (-1)^k = (-1)^k \sigma(b)$. Usando o mesmo argumento para o caso em que $\sigma(b) = -1$, temos que $(-1)^{\frac{n(n-1)}{2}} = (-1)^k \sigma(b)$. Assim,

$$\sigma(\langle s \rangle) = (-1)^k \sigma(b) \sigma(\langle \alpha_1 \rangle) \dots \sigma(\langle \alpha_n \rangle) = \sigma(b) (-1)^k (-1)^k = \sigma(b).$$

Desde que σ é uma assinatura arbitrária de A , temos que $b = \langle s \rangle + b'$, para algum $b' \in W_t(A)$. Assim, $b = \langle s \rangle + b' = \langle s \rangle \cdot (\langle 1 \rangle + \langle s \rangle \cdot b') \in G \cdot (\langle 1 \rangle + W_t(A))$ o que mostra (ii). ■

Nosso próximo interesse é mostrarmos que se $2 \in A^*$, então a ordem de uma unidade da forma $\langle 1 \rangle + b$, para certos elementos de torção b , é uma potência de 2 menor ou igual a potência de 2 que é a ordem aditiva do elemento de torção b . Para tanto usaremos o seguinte lema

Lema 3.10 *Seja A um anel local com $2 \in A^*$. Se $\alpha \in A^*$ é uma soma de 2^k quadrados, então $2^k \langle 1, -\alpha \rangle = 0$ em $W(A)$.*

Dem.: Desde que $b = 2^k \langle 1, -\alpha \rangle$ é uma k -forma de Pfister, de (1.36) é suficiente mostrarmos que b é isotrópico.

Consideremos uma base ortogonal $\{x_1, \dots, x_{2^k}, y_1, \dots, y_{2^k}\}$ de b , tal que $b(x_i, x_i) = 1$ e $b(y_i, y_i) = -\alpha$, para todo $i = 1, \dots, 2^k$. Como α é uma soma de 2^k quadrados, podemos escrever $\alpha = \beta_1^2 + \dots + \beta_{2^k}^2$, com $\beta_1, \dots, \beta_{2^k} \in A$.

Para $x = \beta_1 x_1 + \dots + \beta_{2^k} x_{2^k} + y_1$, temos que $b(x, x) = \beta_1^2 + \dots + \beta_{2^k}^2 + (-\alpha) = 0$, o que mostra que b é isotrópico, pois x é primitivo e $b(x, x) = 0$. ■

Teorema 3.11 *Seja A um anel local com $2 \in A^*$. Se $b \in I(A)$ é tal que $2^k b = 0$ para algum número natural k tal que $2^k \langle 1 \rangle$ é anisotrópica, então*

$$(\langle 1 \rangle + b)^{2^k} = \langle 1 \rangle.$$

Dem.: Desde que $2^k \langle 1 \rangle$ é uma k -forma de Pfister anisotrópica, de (2.24) podemos escrever $b = \sum_{i=1}^m \langle \gamma_i \rangle \cdot b_i$, com $\gamma_i \in A^*$ e, cada b_i da forma $\langle 1, -\alpha_i \rangle$, onde α_i é uma soma de 2^k quadrados. Do lema anterior temos que $2^k b_i = 0$, para cada $i = 1, \dots, m$. Mais ainda, é fácil verificar que em $W(A)$, $b_i^2 = 2b_i$ para cada $i = 1, \dots, m$.

Agora, em $W(A)$ temos

$$b^2 = \sum_{i=1}^m b_i^2 + 2 \sum_{i \neq j} \langle \gamma_i \rangle \cdot \langle \gamma_j \rangle \cdot b_i \cdot b_j = 2 \sum_{i=1}^m b_i + 2 \sum_{i \neq j} \langle \gamma_i \rangle \cdot \langle \gamma_j \rangle \cdot b_i \cdot b_j.$$

Assim,

$$2^{k-1} b^2 = 2^{k-1} 2 \sum_{i=1}^m b_i + 2^{k-1} 2 \sum_{i \neq j} \langle \gamma_i \rangle \cdot \langle \gamma_j \rangle \cdot b_i \cdot b_j = 0,$$

pois $2^k b_i = 0$, para todo $i = 1, \dots, m$. Em particular $b^2 = 2b'$, onde $b' = \sum_{i=1}^m b_i + \sum_{i \neq j} \langle \gamma_i \rangle \cdot \langle \gamma_j \rangle \cdot b_i \cdot b_j \in W(A)$ satisfaz $2^k b' = 0$. Como $(b^2)^2 = (2b')^2 = 2^2 (b')^2$, temos que $2^{k-2} b^4 = 2^{k-2} 2^2 (b')^2 = 0$ e, assim sucessivamente, obtemos

$$2^{k-i} b^{2^i} = 0, \text{ para cada } i = 1, 2, \dots, k.$$

Mas se $2^i \leq r < 2^{i+1}$, então de (1.8), temos que 2^{k-i} divide o coeficiente binomial

$$\binom{2^k}{r}.$$

Então, $2^{k-i} b^{2^i} = 0$, implica que $\binom{2^k}{r} b^r = \binom{2^k}{r} b^{2^i} b^{r-2^i} = 0$, para todo $r = 1, \dots, 2^k$, ou seja, cada termo após o $\langle 1 \rangle$ na expansão binomial de $(\langle 1 \rangle + b)^{2^k}$ é nulo, ou seja, $(\langle 1 \rangle + b)^{2^k} = \langle 1 \rangle$. ■

Observamos que a hipótese $2^* < 1 >$ anisotrópico do teorema acima é sempre verificada quando A é um anel formalmente real, ou seja, neste caso o elemento de torção b é genérico. Quando A é um anel não formalmente real, o teorema é válido somente para os elementos b cuja ordem de torção é diferente da ordem de torção do elemento $< 1 >$.

Se $b = < \alpha, \dots, \alpha_n >$ é um espaço bilinear sobre A , definimos o *discriminante assinalado de b* por $disc_{\pm}(b) = (-1)^{\frac{n(n-1)}{2}} (\alpha_1) \dots (\alpha_n) \in A^*/A^{*2}$.

Para cada número natural $n > 1$, denotaremos por $I^n(A)$ o produto de n -vezes o ideal $I(A)$, ou seja

$$I^n(A) = \left\{ \sum_{fin} b_1 \dots b_n; b_i \in I(A), \text{ para cada } i = 1, \dots, n \right\}.$$

Denotaremos por $I_t^n(A)$ o conjunto $I^n(A) \cap W_t(A)$.

Com esta terminologia temos

Lema 3.12 *Sejam A um anel local e $b \in W(A)$. Se $b \in I(A)$ e $disc_{\pm} b = 1$, então $b \in I^2(A)$.*

Dem.: Para todo $\alpha, \beta \in A^*$, em $W(A)$ temos

$$\begin{aligned} < 1, -\alpha\beta > + < 1, \alpha > \cdot < 1, \beta > &= < 1, -\alpha\beta > + < 1, \alpha, \beta, \alpha\beta > = \\ &= < 1, \alpha > + < 1, \beta > + < -\alpha\beta, \alpha\beta > = \\ &= < 1, \alpha > + < 1, \beta > . \end{aligned}$$

Desde que $b \in I(A)$, de (3.8), podemos escrever $b = \sum_{i=1}^n < 1, \alpha_i >$, com α_i em A^* , $1 \leq i \leq n$.

Afirmamos agora que se $\dim b > 2$, então

$$b = < 1, -disc_{\pm}(b) > + b', \text{ para algum } b' \in I^2(A).$$

Mostraremos a afirmação por indução sobre n . O caso $n = 2$ segue diretamente da igualdade acima. Suponhamos que $b_1 = \sum_{i=1}^n < 1, \alpha_i >$ é um elemento de $I^2(A)$ e

seja $b = \sum_{i=1}^{n+1} \langle 1, \alpha_i \rangle$. Então, usando a identidade acima, temos

$$\begin{aligned} b &= \sum_{i=1}^n \langle 1, \alpha_i \rangle + \langle 1, \alpha_{n+1} \rangle = \\ &= \langle 1, -\text{disc}_{\pm}(b_1) \rangle + b' + \langle 1, \alpha_{n+1} \rangle = \\ &= \langle 1, +\text{disc}_{\pm}(b_1) \alpha_{n+1} \rangle + b'', \end{aligned}$$

para algum $b'' \in I^2(A)$. Mas $\text{disc}_{\pm}(b) = -\text{disc}_{\pm}(b_1)(\alpha_{n+1})$. Portanto $b = \langle 1, -\text{disc}_{\pm}(b) \rangle + b''$, com b'' em $I^2(A)$.

Se $b \in I(A)$, $\dim b = 2$ e $\text{disc}_{\pm}(b) = 1$, temos que $b = \langle 1, \alpha \rangle = 0$ em $W(A)$, ou seja, $b \in I^2(A)$. ■

No próximo resultado apresentaremos uma descrição mais detalhada da forma das unidades de $W(A)$ do que a apresentada em (3.9).

Teorema 3.13 *Cada unidade b em $W(A)$ pode ser expressa na forma $\langle s \rangle \cdot (\langle 1 \rangle + b_1)$, onde $s \in G$ e $b_1 \in I_t^2(A)$. Esta expressão é única e s é o discriminante assinalado de b .*

Dem.: Desde que, de (2.2), todo elemento de $W(A)$ pode ser representado por um espaço bilinear próprio, podemos considerar que uma unidade b de $W(A)$, é da forma $b = \langle \alpha_1, \dots, \alpha_n \rangle$. Sejam $s = (-1)^{\frac{n(n-1)}{2}}(\alpha_1) \dots (\alpha_n) \in G$ e $b_1 = \langle -1 \rangle + \langle s \rangle \cdot b$.

Em G temos

$$\begin{aligned} \text{disc}_{\pm}(b_1) &= \text{disc}_{\pm}(\langle -1 \rangle + \langle s \rangle \cdot b) = \\ &= (-1)^{\frac{(n+1)(n+1-1)}{2}}(s)(\alpha_1) \dots (\alpha_n)(-1) = \\ &= (-1)^{\frac{n(n+1)}{2}}(-1)^{\frac{n(n-1)}{2}}(-1)(\alpha_1^2) \dots (\alpha_n^2) = \\ &= (-1)^{\frac{n(n+1)}{2}}(-1)^{\frac{n(n-1)}{2}}(-1). \end{aligned}$$

Mas, $\frac{n(n+1)}{2} + \frac{n(n-1)}{2} + 1 = (n^2 + 1)$, que é um número par. Então

$$\text{disc}_{\pm}(b_1) = (-1)^{\frac{n(n+1)}{2}}(-1)^{\frac{n(n-1)}{2}}(-1) = 1.$$

Como b é uma unidade, temos que n é ímpar e, conseqüentemente, $\dim(b_1) = n+1$ é par. Assim, do lema (3.8), temos que $b_1 \in I^2(A)$ e, $b = \langle s \rangle \cdot (\langle 1 \rangle + b_1)$. Resta mostrarmos que b_1 é um elemento de torção. Observemos que, para cada $\sigma \in \text{Ass}(A)$,

$$\sigma(b_1) = \sigma(\langle -1 \rangle + \langle s \rangle \cdot b) = -1 + \sigma(\langle s \rangle)\sigma(b).$$

Agora, como na demonstração do teorema (3.9), temos que $\sigma(\langle s \rangle) = \sigma(b)$. Portanto, $\sigma(b_1) = 0$, para todo $\sigma \in \text{Ass}(A)$ e, do Princípio Local-Global de Pfister, temos que b_1 é um elemento de torção de A , como queríamos. ■

Observação 3.14 Se b é uma unidade em $W(A)$ da forma $b = \langle 1 \rangle + b'$ com $b' = \sum_{i=1}^n \ll -\alpha_i, -\beta_i \gg \in I^2(A)$, então b' é necessariamente um elemento de torção de $W(A)$, ou seja $b' \in I_t^2(A)$. De fato, se $\sigma \in \text{Ass}(A)$, então $\sigma(b) = \pm 1$, pois b é uma unidade. Mas, para cada $i = 1, \dots, n$, $\sigma(\ll -\alpha_i, -\beta_i \gg) = 0$ ou 4 , pois se $\sigma(\langle \alpha_i \rangle) = \sigma(\langle \beta_i \rangle) = 1$ ou $\sigma(\langle \alpha_i \rangle) = -\sigma(\langle \beta_i \rangle)$, temos que $\sigma(\ll -\alpha_i, -\beta_i \gg) = 0$ e, se $\sigma(\langle \alpha_i \rangle) = \sigma(\langle \beta_i \rangle) = -1$, obtemos $\sigma(\ll -\alpha_i, -\beta_i \gg) = 4$. Portanto $\sigma(b) = \sigma(\langle 1 \rangle + b') \neq -1$, ou seja, $\sigma(b) = 1$. Conseqüentemente $\sigma(b') = 0$. Como σ é um elemento genérico de $\text{Ass}(A)$, de (2.20), temos que $b' \in W_t(A)$.

Contudo é possível ter unidades da forma $\langle 1 \rangle + b'$ com $b' \notin W_t(A)$, como veremos no exemplo seguinte.

Exemplo 3.15 Sejam $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ e $b' = \langle -2, \sqrt{2} \rangle$ um elemento de $\text{Bil}(K)$. É fácil verificar que $P = \{a + b\sqrt{2} \in K; a - b\sqrt{2} > 0\}$ determina uma ordem em K , o que mostra em particular que K é formalmente real. Observe que, em relação a esta ordem, $\sqrt{2}$ é negativo, ou seja, $\sqrt{2} \in -P$.

Agora a aplicação $\sigma : W(K) \rightarrow \mathbb{Z}$, definida por

$$\sigma(\langle \alpha \rangle) = \begin{cases} 1 & \text{se } \alpha \in P \\ -1 & \text{se } \alpha \in -P \end{cases}$$

para cada $\alpha \in K^*$, é claramente uma assinatura de K . Mais ainda, $\sigma(b') = \sigma(\langle -2, \sqrt{2} \rangle) = \sigma(\langle -2 \rangle) + \sigma(\langle \sqrt{2} \rangle) = -2$ o que mostra, pelo Princípio Local-Global de Pfister, que b' não é um elemento de torção em $W(K)$.

Por outro lado, para $b = \langle 1 \rangle \perp b' = \langle 1, -2, -\sqrt{2} \rangle$, temos

$$b^2 = \langle 1, -2, \sqrt{2} \rangle \otimes \langle 1, -2, \sqrt{2} \rangle = \langle 1 \rangle \perp 2 \langle 1, -2, \sqrt{2}, -2\sqrt{2} \rangle = \langle 1 \rangle \perp b_1.$$

Se $\{x_1, x_2, x_3, x_4\}$ é uma base ortogonal para o espaço $\langle 1, -2, \sqrt{2}, -2\sqrt{2} \rangle$, então $x = \sqrt{2}x_1 + x_2$ é um elemento isotrópico deste espaço. Assim $b_1 = 2 \langle 1, -2, \sqrt{2}, -2\sqrt{2} \rangle = \ll 1, -2, \sqrt{2} \gg$ é um espaço de Pfister isotrópico e, de (1.36), segue que $b_1 = 0$ em $W(K)$. Consequentemente $b^2 = \langle 1 \rangle$ em $W(K)$, ou seja b é uma unidade da forma $\langle 1 \rangle + b'$, com $b' \notin W_t(K)$.

Para cada unidade b de $W(A)$ e $k \geq 1$, temos que os elementos b^{2^k} são também unidades de $W(A)$. Para estas unidades temos

Proposição 3.16 *Seja b uma unidade em $W(A)$. Então, para cada $k \geq 1$ temos $b^{2^k} = \langle 1 \rangle + b'$, com $b' \in I_t^{k+2}(A)$.*

Dem.: Faremos a demonstração por indução sobre k . Do teorema anterior temos que $b = \langle s \rangle \cdot (\langle 1 \rangle + b_1)$, com $b_1 \in I_t^2(A)$. Logo, $b^2 = \langle 1 \rangle + 2b_1 + b_1^2 = \langle 1 \rangle + b_1 \cdot (b_1 + 2 \langle 1 \rangle)$, ou seja $b^2 = \langle 1 \rangle + b'$ onde $b' = b_1 \cdot (b_1 + 2 \langle 1 \rangle) \in I_t^3(A)$, o que mostra que o resultado é válido para $k = 1$.

Agora assumamos que o resultado vale para $k - 1$, isto é, que $b^{2^{k-1}} = \langle 1 \rangle + b'$ com $b' \in I_t^{k+1}(A)$. Então

$$b^{2^k} = (b^{2^{k-1}})^2 = (\langle 1 \rangle + b')^2 = \langle 1 \rangle + 2b' + b'^2 = \langle 1 \rangle + b'',$$

onde $b'' = b' \cdot (b' + 2 \langle 1 \rangle) \in I_t^{k+2}(A)$, como queríamos. ■

Como consequência desta proposição temos

Corolário 3.17 Para $k \geq 3$, se $I^k(A)$ é livre de torção, então cada unidade b de $W(A)$ satisfaz $b^{2^{k-2}} = \langle 1 \rangle$ em $W(A)$.

Dem.: Da proposição anterior segue que $b^{2^{k-2}} = \langle 1 \rangle + b'$, onde $b' \in I_t^k(A) = \{0\}$, ou seja $b^{2^{k-2}} = \langle 1 \rangle$. ■

Do teorema (3.13) temos que toda unidade $b \in W(A)$ e da forma $\langle s \rangle \cdot (\langle 1 \rangle + b')$, com $b' \in I_t^2(A)$. No próximo resultado apresentamos uma descrição mais detalhada dos elementos de $I_t^2(A)$.

Lema 3.18 Sejam A um anel local com $2 \in A^*$ e k um inteiro positivo tal que $2^k \langle 1 \rangle \neq 0$ em $W(A)$. Se $b \in I_t^2(A)$ é tal que $2^k b = 0$, então $b = \sum_{i=1}^n \ll \alpha_i, -\gamma_i \gg$, para algum $n \geq 1$ e $\alpha_i, \gamma_i \in A^*$, onde cada γ_i é uma soma de 2^k quadrados.

Dem.: Desde que $2^k \langle 1 \rangle \neq 0$ e $2^k b = 0$, ou seja $b \in \text{Ann}(2^k \langle 1 \rangle)$, de (2.24), temos que $b = \sum_{i=1}^s \langle \alpha_i \rangle \cdot \langle 1, -\gamma_i \rangle$ onde, para cada $i = 1, \dots, s$, γ_i é uma soma de 2^k quadrados.

Seja $b' = \sum_{i=1}^s \langle 1, -\gamma_i \rangle$, então

$$b = \sum_{i=1}^s \langle \alpha_i \rangle \cdot \langle 1, -\gamma_i \rangle + b' + (-b') = \sum_{i=1}^s \ll \alpha_i, -\gamma_i \gg + (-b')$$

e, $\text{disc}_{\pm}(b') = (\gamma_1)(\gamma_2) \dots (\gamma_n) = 1$ em G , pois $b' \in I^2(A)$. Assim, é suficiente mostrarmos o resultado para $-b'$.

Usando que em $W(A)$ vale a igualdade

$$\langle 1, -\gamma \rangle + \langle 1, -\gamma' \rangle = \ll -\gamma, -\gamma' \gg + \langle 1, -\gamma\gamma' \rangle,$$

e que n é par, obtemos

$$\begin{aligned} b' &= \langle 1, -\gamma_1 \rangle + \langle 1, -\gamma_2 \rangle + \dots + \langle 1, -\gamma_{n-1} \rangle + \langle 1, -\gamma_n \rangle = \\ &= \ll -\gamma_1, -\gamma_2 \gg + \langle 1, -\gamma_1\gamma_2 \rangle + \dots + \ll \gamma_{n-1}, \gamma_n \gg + \langle 1, -\gamma_{n-1}\gamma_n \rangle = \end{aligned}$$

$$= \ll -\gamma_1, -\gamma_2 \gg + \cdots + \ll -\gamma_{n-1}, -\gamma_n \gg + \ll -\gamma_1\gamma_2, -\gamma_3\gamma_4 \gg + \langle 1, -\gamma_1\gamma_2\gamma_3\gamma_4 \rangle \\ + \cdots + \ll -\gamma_{n-3}\gamma_{n-2}, \gamma_{n-1}\gamma_n \gg + \langle 1, -\gamma_{n-3}\gamma_{n-2}\gamma_{n-1}\gamma_n \rangle .$$

Aplicando este raciocínio repetidamente, obtemos

$$b' = \sum_{i=1}^m \ll \alpha'_i, -\gamma'_i \gg + \langle 1, -disc_{\pm}(b') \rangle ,$$

onde cada γ'_i é uma soma de 2^k quadrados, pois $\mathcal{D}(2^k \langle 1 \rangle)$ é um grupo. Desde que $disc_{\pm}(b') = 1$ temos que $\langle 1, -disc_{\pm}(b') \rangle = 0$ e, portanto o resultado vale para b' .

Agora, como cada γ_i , $1 \leq i \leq s$, é uma soma de 2^k quadrados, de (3.10) temos que $2^k b' = 0$. Consequentemente $-b' = (2^k - 1)b'$ também satisfaz o resultado, o que mostra o lema. ■

Observemos que na expressão $b = \sum_{i=1}^n \ll \alpha_i, -\gamma_i \gg$, do lema anterior, temos também que, para cada $i = 1, \dots, n$,

$$2^k \ll \alpha_i, \gamma_i \gg = 2^k (\langle 1, \alpha_i \rangle \cdot \langle 1, -\gamma_i \rangle) = 0,$$

pois cada γ_i é uma soma de 2^k quadrados. Observemos também que, quando A é formalmente real, o resultado do lema anterior vale para todo $k \geq 1$, pois o elemento $\langle 1 \rangle$ não é de torção.

Vejamos agora que, sob certas condições, vale a volta do teorema (3.11).

Teorema 3.19 *Seja A um anel local formalmente real, com $2 \in A^*$. Se $b \in I_t^2(A)$ é tal que $(\langle 1 \rangle + b)^{2^k} = \langle 1 \rangle$, então $2^k b = 0$.*

Dem.: Do lema anterior temos que existe um número natural n e espaços bilineares de Pfister $b_i = \ll \alpha_i, -\beta_i \gg$, tais que $b = \sum_{i=1}^n b_i$ com $2^r b_i = 0$ para algum $r \geq 1$ e todo $i = 1, \dots, n$.

Temos também que $b_i^2 = 4b_i$, $1 \leq i \leq n$, pois

$$\begin{aligned} (\langle 1, \alpha_i \rangle \otimes \langle 1, -\beta_i \rangle)^2 &\simeq \langle 1, \alpha_i \rangle^2 \otimes \langle 1, -\beta_i \rangle^2 \simeq \\ &\simeq 2 \langle 1, \alpha_i \rangle \otimes 2 \langle 1, -\beta_i \rangle \simeq \\ &\simeq 4 \langle 1, \alpha_i \rangle \otimes \langle 1, -\beta_i \rangle . \end{aligned}$$

Agora,

$$b^2 = \sum_{i=1}^m b_i^2 + 2 \sum_{i \neq j} b_i \cdot b_j = 4 \sum_{i=1}^m b_i + 2 \sum_{i \neq j} b_i \cdot b_j.$$

Assim, $b^2 = 2c_1$, onde $c_1 = 2 \sum_{i=1}^m b_i + \sum_{i \neq j} b_i \cdot b_j \in W(A)$.

De maneira análoga obtemos, $c_1^2 = 2c_2$, onde c_2 é uma soma de termos envolvendo produtos dos $(b_i)'s$. Podemos repetir este processo sucessivamente e obter uma sequência de elementos de $W(A)$, $\{c_n\}$, satisfazendo $c_n^2 = 2c_{n+1}$ para cada n . Como $b_i^2 = 4b_i$, $2^r b_i = 0$ para cada i e temos somente um número finito de $(b_i)'s$ distintos, segue que para n suficientemente grande, cada termo em $\{c_n\}$ se anula, pois potências grandes de pelo menos 2^r , aparecerão como coeficientes. Logo, para n suficientemente grande, $c_n = 0$.

Mostraremos agora o teorema por indução sobre k . Quando $k = 0$ o teorema é trivial.

Vamos assumir que o resultado vale para $k - 1$ e supor que

$$(<1> + b)^{2^k} = (<1> + 2b + b^2)^{2^{k-1}} = <1>.$$

Assim, por hipótese de indução, temos que

$$2^{k-1}(2b + b^2) = 0, \text{ isto é } 2^k b = -2^{k-1} b^2.$$

Desde que $b^2 = 2c_1$, para algum $c_1 \in W(A)$, temos $2^k b = -2^{k-1} 2c_1$ e, isto implica que $2^k(c_1 + b) = 0$.

Agora, do teorema (3.11), cada termo após o $<1>$ na expansão binomial de $(<1> + c_1 + b)^{2^k}$ é nulo em $W(A)$. Em particular

$$\binom{2^k}{2} (c_1 + b)^2 = 0.$$

Mas

$$\binom{2^k}{2} = \frac{2^k}{(2^k - 2)!2!} = 2^{k-1}(2^k - 1);$$

assim $2^{k-1}(2^k - 1)(c_1 + b)^2 = -2^{k-1}(c_1 + b)^2 = 0$, pois $2^k(c_1 + b) = 0$. Logo $2^{k-1}c_1^2 + 2^k c_1 \cdot b + 2^{k-1}b^2 = 2^{k-1}c_1^2 - 2^k b^2 + 2^{k-1}b^2 = 0$. Consequentemente

$$\begin{aligned} 2^{k-1}c_1^2 &= 2^k b^2 - 2^{k-1} \cdot b^2 = \\ &= 2^{k-1}(2b^2 - b^2) = \\ &= 2^{k-1}b^2. \end{aligned}$$

Substituindo $2^{k-1}b^2 = -2^k b$ e $c_1^2 = 2c_2$ na igualdade acima, para algum $c_2 \in W(A)$, temos $2^{k-1}2c_2 = -2^k b$, ou seja, $2^k c_2 + 2^k b = 2^k(c_2 + b) = 0$. Repetindo este raciocínio, obtemos

$$2^k(c_n + b) = 0,$$

para cada número natural n . Mas, como vimos no início da demonstração, $c_n = 0$ para n suficientemente grande. Portanto $2^k b = 0$, como queríamos. ■

Dos teoremas (3.11) e (3.19), para o caso em que A é um anel local formalmente real com $2 \in A^*$ temos

Corolário 3.20 *Seja b uma unidade em $W(A)$. Expressando b na forma $\langle s \rangle \cdot (\langle 1 \rangle + b_1)$ onde $b_1 \in I_t^2(A)$, a ordem de b no grupo das unidades de $W(A)$ é igual a ordem aditiva do elemento b_1 em $W_t(A)$.*

Dem.: Imediata. ■

Referências Bibliográficas

- [1] ATIYAH, M.F. e MACDONALD, I.G.; *Introduction to Commutative Algebra*, University of Oxford, 1969.
- [2] BAEZA, R.; *Quadratic Forms over Semilocal Ring*, Lecture Notes in Mathematics 655, 1978.
- [3] DIAS, I.; *Formas quadráticas sobre LG-Anéis*, Tese de Doutorado, IMECC-UNICAMP, 1988.
- [4] KAPLANSKY, I.; *Commutative Rings*, Allyn an Bacon, Boston, 1970.
- [5] KNEBUSCH, M.; ROSENBERG, A.; WARE, R.; *Struture of Witt Ring and Quotients of Abelian Group Rings*, Am. J. of Math. 94, 119-155, (1972).
- [6] LAM, T. Y.; *The Algebric Theory of Quadratic Forms*, University of California, 1973.
- [7] LEWIS, D. W.; *Units in Witt Rings*, Communication in Algebra, 18(10), 3295-3306, (1990).
- [8] MARSHALL, M.; *Abstract Witt Rings*, Queen's Papers in Pure and Applied Mathematics - 57, 1980.
- [9] PIERCE, R.; *Associative Algebras*, G. T. M. 88, Springer Verlag, 1982.

- [10] BRUSAMARELLO, R.; *Ideais Primos do Anel de Witt sobre um Anel Local*, Tese de Mestrado, ICMSC-USP, 1991.
- [11] SCHARLAU, W.; *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin-Heidelberg-New York-Tokio, 1985.