Ideais Primos do Anel de Witt
sobre um Anel Local

Rosali Brusamarello

Orientação
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 Matemática.

USP - São Carlos
agosto 1991

À minha família

Inicialmente, agradeço à Ires, pela sua incansável dedicação. Agradeço aos meus pais, pela confiança em mim depositada; aos meus colegas da pós-graduação, pela amizade e apoio; à Míriam, pelo seu exemplar coleguismo e sua grande amizade; ao CNPq, pelo auxílio financeiro recebido; e as demais pessoas que me foram importantes.

Abstract

In this work we study quadratic forms theory on local rings on which we don't have the hypothesis that 2 is invertible. Our aim is to establish a one to one correspondence between the set of the minimal prime ideals of Witt Ring on a local ring and the set of maximal orders of this ring. This correspondence have already been established by Kanzaki and Kitamura when 2 is invertible on the local ring.

Resumo

Neste trabalho estudamos a teoria de formas quadráticas sobre anéis locais, sem a hipótese que 2 é inversível no anel. Nosso objetivo é estabelecer uma correspondência biunívoca entre o conjunto dos ideais primos minimais do Anel de Witt sobre um anel local e o conjunto das ordens maximais deste anel. Esta correspondência já foi estabelecida por Kanzaki e Kitamura quando 2 é inversível no anel local.

Conteúdo

Introdução	iii
1 Espaços Bilineares	1
1.1 Preliminares	1
1.2 Espaços Bilineares	3
1.3 Subespaços	7
1.4 Espaços Metabólicos	10
1.5 Decomposição de Espaços Bilineares	13
2 O Anel de Witt	16
2.1 $\widehat{W}(A)$ e $W(A)$	16
2.2 Geradores de $W(A)$	20
3 Ideais de $W(A)$	24
3.1 Os Ideais Primos de $W(A)$	24

3.2 Os Ideais Primários de $W(A)$	32
4 Correspondências entre Ordens, Assinaturas e Ideais Primos	38
Bibliografia	45

Introdução

A teoria de formas quadráticas teve origem em 1937 através de um artigo escrito por E. Witt, onde foi introduzido pela primeira vez na literatura a noção de Anel de Witt de um corpo. Trinta anos depois, surgiram os trabalhos de A. Pfister, com os primeiros resultados sobre a estrutura do Anel de Witt de um corpo de característica distinta de 2. Em 1973, T. Y. Lam escreveu o livro [12], ainda trabalhando sobre corpos de característica distinta de 2. Posteriormente, surgiram trabalhos importantes na teoria de formas quadráticas sobre domínios mais gerais, dentre eles destacamos os trabalhos de A. Knebusch. Nosso trabalho tem por base a teoria de formas quadráticas sobre anéis locais com 2 inversível ou não. Mais precisamente, estudamos os ideais primos do Anel de Witt sobre um anel local.

Em [12], Lam estabelece uma correspondência biunívoca entre o conjunto dos ideais primos minimais do Anel de Witt de um corpo de característica distinta de 2 e o conjunto das ordens deste corpo. Kanzaki e Kitamura estabeleceram em [8] uma correspondência biunívoca entre o conjunto dos ideais primos minimais do Anel de Witt sobre um anel local em que 2 é inversível e o conjunto das ordens das unidades (ver def. 4.10) deste anel. Nosso objetivo é estabelecer uma correspondência análoga às citadas acima, para o caso de um anel local sem a hipótese de 2 ser inversível. Com isso estaremos generalizando [8].

Baseados no que Baeza apresenta em [2] a respeito da teoria de formas quadráticas sobre anéis semi-locais, introduzimos os conceitos básicos da teoria de formas quadráticas sobre um anel local. Além de definirmos o Anel de Witt sobre um anel local, damos uma caracterização de seus geradores, afim de facilitar

a compreensão da estrutura deste anel.

Damos uma caracterização dos ideais primos do Anel de Witt sobre um anel local, conforme fez M.Knebusch em [11]. Segue desta, uma correspondência biunívoca entre o conjunto dos ideais primos minimais do Anel de Witt sobre um anel local e o conjunto das assinaturas deste anel. Tendo em mãos a caracterização dos ideais primos, obtemos uma caracterização dos ideais primários do Anel de Witt sobre um anel local, análoga à obtida por Fitzgerald em [5] para o caso de corpos de característica distinta de 2.

Baseados nos artigos [9] e [10] de Knebusch estabelecemos uma correspondência biunívoca entre o conjunto das assinaturas de um anel local e o conjunto das suas ordens maximais (ver def.4.1). Com isso, além de atingir o objetivo principal, que é a generalização do Teo (3.1) de [8], estabelecemos outras correspondências interessantes.

Capítulo 1

Espaços Bilineares

1.1 Preliminares

Nesta seção introduzimos alguns conceitos básicos de Álgebra Homológica, bem como enunciamos resultados que serão utilizados no decorrer do trabalho. Nos preocupamos apenas em demonstrar o Teorema 1.8, devido à sua importância. Os demais resultados são elementares e podem ser encontrados em [7].

Esta seção pode ser ignorada pelo leitor com algum conhecimento de Álgebra Homológica.

Definição 1.1 Seja A um anel. Uma seqüência de A -módulos e A -homomorfismos

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

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

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

Dizemos que uma seqüência exata

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

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

Para uma seqüência exata curta o seguinte resultado é imediato.

Proposição 1.2 *Se uma seqüência exata curta de A -módulos $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$ cinde, então $Y \cong X \oplus Z$.*

Definição 1.3 Um A -módulo M é *livre* se ele possui uma base.

Definição 1.4 Um A -módulo P é um módulo *projetivo* se satisfaz uma das seguintes condições equivalentes:

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

$$0 \rightarrow \text{Hom}(P, X) \rightarrow \text{Hom}(P, Y) \rightarrow \text{Hom}(P, Z) \rightarrow 0$$

é exata .

Observação 1.5 Segue diretamente das definições acima que todo módulo livre é projetivo.

Definição 1.6 Dizemos que um anel A é 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 .
- (c) Para cada $a \in A$, a ou $1 - a$ é uma unidade.

O corpo $K = A/\mathcal{M}$ é chamado *corpo das classes residuais de A* . Denotamos a projeção canônica de A em K por $\bar{}$.

Lema 1.7 *Se P é um A -módulo projetivo finitamente gerado, então existe um A -módulo finitamente gerado N tal que $P \oplus N = A^n$, para algum $n \in \mathbb{N}$.*

Dem.: Como P é um A -módulo projetivo, temos que existe um A -módulo N_o , tal que $P \oplus N_o = F$, onde F é um A -módulo livre com base $\{e_i\}_{i \in I}$. Sendo P finitamente gerado existe um subconjunto finito J de I , tal que $P \subseteq F_o := \sum_{i \in J} Ae_i$. Assim, $F_o = P + (N_o \cap F_o)$. Tomando $N = N_o \cap F_o$, temos que $F_o = P \oplus N$, pois $P \cap N = \emptyset$. Claramente $N \cong F_o/P$ é finitamente gerado. Portanto $P \oplus N = A^n$, para algum $n \in \mathbb{N}$. $\square$

Teorema 1.8 *Todo módulo projetivo finitamente gerado sobre um anel local é livre.*

Dem.: Sejam A um anel local e M um A -módulo projetivo finitamente gerado. Então, por (1.7) existe um A -módulo finitamente gerado N tal que $M \oplus N = A^n$, para algum $n \in \mathbb{N}$. Consideremos $\{e_1, \dots, e_n\}$ uma base de $M \oplus N$. Sendo A local podemos considerar o corpo das classes residuais $K = A/\mathcal{M}$ e, pela projeção canônica, temos que $\overline{M} \oplus \overline{N} \cong K^n$. Seja $\overline{f}_1, \dots, \overline{f}_m$ base de $\overline{M}$ e $\overline{f}_{m+1}, \dots, \overline{f}_n$ base de $\overline{N}$ sobre K . Se $B = (b_{ij})$ com $f_i = \sum_{j=1}^n e_j b_{ij}$ então $\overline{B}$ é não singular, pois é uma matriz mudança de base. Assim, o determinante de B é uma unidade, ou seja, B é inversível. Logo, $\{f_1, \dots, f_n\}$ é uma base de $M \oplus N$. Assim, $\{f_1, \dots, f_m\}$ é base de M , ou seja, M é um A -módulo livre. $\square$

1.2 Espaços Bilineares

No que segue e nos demais capítulos A denota sempre um anel local comutativo com elemento identidade 1 e $\mathcal{M}$ seu ideal maximal. Indicamos por A^* o grupo das unidades de A . Assumimos também, a partir de agora, que todo A -módulo é unitário e que todo homomorfismo de anéis leva elemento identidade em elemento identidade.

Em geral, a teoria de formas quadráticas sobre anéis é feita na categoria dos módulos projetivos finitamente gerados de posto constante. Como vimos em

(1.8), para o caso em que A é um anel local, todo A -módulo projetivo finitamente gerado é livre. Assim, em todo este trabalho trabalhamos 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 Sejam $M \in L(A)$ e $b : M \times M \rightarrow A$ uma forma bilinear simétrica. Ao par (M, b) chamamos de *módulo bilinear sobre A* .

Por abuso de notação, para todo $M \in L(A)$ denotamos por M^* o seu A -módulo dual $\text{Hom}_A(M, A) \in L(A)$.

Definição 1.10 Seja (M, b) um módulo bilinear sobre A . Para todo $x \in M$ definimos $d(x) \in M^*$ por $d(x)(y) = b(x, y)$, para todo $y \in M$. Obtemos assim uma aplicação A -linear $d : M \rightarrow M^*$.

O módulo bilinear (M, b) é *não singular*, ou simplesmente um *espaço bilinear sobre A* , se d é um isomorfismo.

Se o A -módulo M tem dimensão n , dizemos que o espaço bilinear (M, b) tem dimensão n e indicamos por $\dim_A M = n$, ou simplesmente $\dim b = n$.

Observação 1.11 Seja (M, b) um módulo bilinear sobre A e $\{e_1, \dots, e_n\}$ uma base de M . A forma bilinear simétrica b é determinada pela matriz simétrica (b_{ij}) onde $b_{ij} = b(e_i, e_j)$, pois para $x = \sum_{i=1}^n x_i e_i$ e $y = \sum_{i=1}^n y_i e_i$ temos que:

$$b(x, y) = \sum_{i,j=1}^n b_{ij} x_i y_j$$

Reciprocamente, dada uma matriz simétrica $(b_{ij})_{n \times n}$ obtemos, pela fórmula acima uma forma bilinear simétrica.

Podemos considerar as coordenadas de x e y , em relação a base $\{e_1, \dots, e_n\}$, como um vetor coluna, assim obtemos $b(x, y) = x^t(b_{ij})y$, onde (b_{ij}) é a matriz que determina b .

O módulo bilinear (M, b) é não singular se, e somente se, $\det(b_{ij}) \in A^*$. Para ver isto, basta observarmos que a matriz (b_{ij}) é a matriz da aplicação

$d : M \rightarrow M^*$.

Como um módulo bilinear (M, b) é caracterizado por uma matriz quadrada (b_{ij}) , usamos também a notação $b = (b_{ij})$ para indicarmos a forma bilinear b . O determinante da matriz (b_{ij}) é chamado *determinante do espaço bilinear* b .

Exemplo 1.12 Seja (M, b) um módulo bilinear tal que $M = Ae_1 \oplus Ae_2$, com $b(e_1, e_1) = \alpha$, $b(e_2, e_2) = \beta$ e $b(e_1, e_2) = 1$. Assim:

$$(b_{ij}) = (b(e_i, e_j)) = \begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix},$$

ou seja, (M, b) é um espaço bilinear se, e somente se, $1 - \alpha\beta \in A^*$.

A menos que se diga em contrário, no que segue, (M, b) denotará um espaço bilinear sobre A .

Definição 1.13 Uma *isometria* entre dois espaços bilineares (M_1, b_1) e (M_2, b_2) é um isomorfismo linear $\varphi : M_1 \rightarrow M_2$, tal que $b_1(x, y) = b_2(\varphi(x), \varphi(y))$, para todo $x, y \in M_1$. Se existir uma isometria entre (M_1, b_1) e (M_2, b_2) dizemos que os espaços são *isométricos* e denotamos por $(M_1, b_1) \simeq (M_2, b_2)$, ou simplesmente $b_1 \simeq b_2$.

Proposição 1.14 Sejam (M_1, b_1) e (M_2, b_2) espaços bilineares sobre A e (a_{ij}) , (b_{ij}) suas respectivas matrizes. Então $b_1 \simeq b_2$ se, e somente se, (a_{ij}) e (b_{ij}) são matrizes semelhantes.

Dem.: Se $b_1 \simeq b_2$, então existe um isomorfismo $\varphi : M_1 \rightarrow M_2$, tal que $b_1(x, y) = b_2(\varphi(x), \varphi(y))$. Todo isomorfismo entre módulos livres é determinado por uma matriz inversível C , ou seja, $\varphi(x) = Cx$, para todo $x \in M_1$. Como

$$b_1(x, y) = x^t(a_{ij})y \quad \text{e} \quad b_2(\varphi(x), \varphi(y)) = \varphi(x)^t(b_{ij})\varphi(y) = x^t C^t(b_{ij})Cy$$

temos $(a_{ij}) = C^t(b_{ij})C$. Portanto (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 $x, y \in M_1$,

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

Portanto $b_1 \simeq b_2$. $\square$

Como consequência desta proposição temos:

Corolário 1.15 *Os determinantes de dois espaços bilineares isométricos diferem por quadrados.*

Dem.: Imediata. $\square$

Consideremos agora a categoria dos espaços bilineares sobre A , que denotamos por $Bil(A)$, onde os morfismos são as isometrias. Em $Bil(A)$ vamos definir uma soma e um produto.

Definição 1.16 Definamos a *soma ortogonal* dos espaços $(M_i, b_i) \in Bil(A)$ ($i = 1, 2$) como sendo o espaço 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 $x_i, y_i \in M_i$ ($i = 1, 2$). Denotamos este espaço simplesmente por $b_1 \perp b_2$.

Definamos o *produto tensorial* dos espaços $(M_i, b_i) \in Bil(A)$ ($i = 1, 2$), como sendo o espaço 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 $x_i, y_i \in M_i$ ($i = 1, 2$). Denotamos por $b_1 \otimes b_2$ este espaço.

As duas operações são associativas, comutativas e 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

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

De fato, se $\varphi : (M_1, b_1) \rightarrow (M_2, b_2)$ e $\varphi' : (M'_1, b'_1) \rightarrow (M'_2, b'_2)$ são isometrias, então é fácil ver que:

$$\varphi + \varphi' : (M_1 \oplus M'_1, b_1 \perp b'_1) \rightarrow (M_2 \oplus M'_2, b_2 \perp b'_2),$$

definida por $\varphi + \varphi'(x_1 \oplus x'_1) = \varphi(x_1) + \varphi'(x'_1)$ é uma isometria. Assim como

$$\varphi \otimes \varphi' : (M_1 \otimes M'_1, b_1 \otimes b'_1) \rightarrow (M_2 \otimes M'_2, b_2 \otimes b'_2),$$

definida por $\varphi \otimes \varphi'(x_1 \otimes x'_1) = \varphi(x_1) \otimes \varphi'(x'_1)$ é uma isometria.

Observação 1.17 Convencionamos como sendo o elemento neutro da soma ortogonal o espaço $(\emptyset, 0)$ que assumimos não singular. O elemento neutro do produto tensorial é o espaço unidimensional (Ae, b) , com $b(e, e) = 1$, que denotamos por $\langle 1 \rangle$.

1.3 Subespaços

Nesta seção voltamos a considerar os módulos bilineares, sem exigirmos que sejam não singulares.

Seja (M, b) um módulo bilinear. Para todo subconjunto $U \subseteq M$ consideremos o conjunto:

$$U^\perp = \{x \in M : b(x, y) = 0, \forall y \in U\},$$

que é um submódulo de M .

Lema 1.18 (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 $\square$

Definição 1.19 Um submódulo $U \subseteq M$ é chamado um *subespaço* de (M, b) , se U é somando direto de M , ou seja, se existe $V \subseteq M$, tal que $M = U \oplus V$.

Se $M = U \oplus V$ e $U \subseteq V^\perp$, dizemos que M é a *soma ortogonal* de U e V e denotamos por $M = U \perp V$. A restrição da forma bilinear b ao submódulo $U \subseteq M$ denotaremos por $(U, b|_U)$. 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 *totalmente isotrópico* se $U \subseteq U^\perp$, ou seja, se $b(x, y) = 0$, para todo $x, y \in U$. Dizemos que um elemento $x \in M$ é *isotrópico* se $Ax \subseteq M$ é um subespaço totalmente isotrópico, ou seja, se $b(x, x) = 0$. Se $b(x, x) \in A^*$ dizemos que x é *anisotrópico*.

Proposição 1.20 *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 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.: (i) Por hipótese temos que existe $V \subseteq M$ tal que $M = U \oplus V$. Logo, a seqüência $M^* \rightarrow U^* \rightarrow 0$ é exata. Como M é não singular, temos que $d : M \rightarrow M^*$ é um isomorfismo. Através de composições obtemos a seguinte seqüência exata $M \rightarrow U^* \rightarrow 0$. Note que $d : M \rightarrow U^*$ leva $x \in M$ em $d(x) \in U^*$, onde $d(x)(y) = b(x, y)$ para todo $y \in U$, logo seu núcleo é $U^\perp$. Obtemos assim a seqüência exata curta:

$$0 \rightarrow U^\perp \rightarrow M \rightarrow U^* \rightarrow 0.$$

Como U é projetivo temos que esta seqüência exata cinde, ou seja, $M \cong U^\perp \oplus U^*$. O que mostra que $U^\perp$ é um subespaço de M .

Resta mostrarmos que $U = U^{\perp\perp}$. Para tanto consideremos o isomorfismo $d : M/U^\perp \rightarrow U^*$. Continuamos denotando por d as aplicações que são definidas a partir da forma bilinear b . Este isomorfismo induz uma função bilinear não singular $b : U \times M/U^\perp \rightarrow A$; denotamos também por b as restrições da forma bilinear b a subespaços de M . Esta função bilinear aplicada a $U^\perp$ nos fornece

$b : U^\perp \times M/U^{\perp\perp} \rightarrow A$. Por outro lado, temos o isomorfismo $M \cong (U^\perp)^* \oplus U$ que decorre dos isomorfismos :

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

Assim, o isomorfismo $d : M/U \rightarrow (U^\perp)^*$ induz a função bilinear não singular $b : U^\perp \times M/U \rightarrow A$. Por (1.18) temos que $U \subseteq U^{\perp\perp}$. Suponhamos que $U \neq U^{\perp\perp}$; logo, existe $y \in U^{\perp\perp} - U$. Da primeira função bilinear obtida segue que $b(x, y) = 0$ para todo $x \in U^\perp$, pois $y = 0$ em $M/U^{\perp\perp}$. Da segunda função bilinear segue que existe $x \in U^\perp$ tal que $b(x, y) \neq 0$, pois $y \neq 0$ em M/U e b é não singular. Chegamos assim a uma contradição. Portanto $U = U^{\perp\perp}$.

(ii) Como $(U, b|_U)$ é não singular temos que $d : U \rightarrow U^*$ é um isomorfismo. Todo elemento $x \in M$ define um elemento em U^* por $b(x, y)$ para todo $y \in U$. Como $d : U \rightarrow U^*$ é sobrejetora, existe $z \in U$ tal que $b(z, y) = b(x, y)$ para todo $y \in U$. Assim $x - z \in U^\perp$ e como $x = z + (x - z)$ segue que $M = U + U^\perp$. Pelo fato de $d : U \rightarrow U^*$ ser injetora segue que $U \cap U^\perp = \{0\}$. Assim $M = U \oplus U^\perp$, o que mostra que U é um subespaço de M . Pelo Lema (1.18), $U \subseteq U^{\perp\perp}$; portanto, $M = U \perp U^\perp$. $\square$

Proposição 1.21 *Sejam M um espaço bilinear sobre A e $U \subseteq M$ um subespaço totalmente isotrópico maximal, isto é, $U = U^\perp$. Então existe um subespaço $V \subseteq M$ tal que $U \cong V^*$ e $M = U \oplus V$.*

Dem.: Pela demonstração do item (i) da proposição (1.20) temos que $M \cong U^\perp \oplus U^*$. Basta tomarmos $V = U^*$ e temos que $V^* = U^{**} \cong U$. Como $U = U^\perp$ temos que $M \cong U \oplus V$. $\square$

1.4 Espaços Metabólicos

Nesta seção estudamos uma classe especial de espaços bilineares, a qual é ferramenta básica para desenvolvermos a teoria do próximo capítulo.

Definição 1.22 Seja (U, b) um módulo bilinear sobre A . Definimos em $U \oplus U^*$ uma forma bilinear simétrica dada por:

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

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

Proposição 1.23 Para todo módulo bilinear (U, b) sobre A , $M(U)$ é um espaço bilinear.

Dem.: Desde que $M(U) = U \oplus U^*$, segue que $M(U)^* = U^* \oplus U^{**}$. Seja $j_U : U \rightarrow U^{**}$ o isomorfismo canônico. A matriz da aplicação $d_U : M(U) \rightarrow M(U)^*$ é:

$$d_U = \begin{pmatrix} d & j_U \\ id_U & 0 \end{pmatrix}$$

onde $d : U \rightarrow U^*$ pode não ser um isomorfismo. Assim, $\det(d_U) = \det(j_U)\det(id_U)$. Logo, $\det(d_U) \in A^*$, pois $\det(j_U), \det(id_U) \in A^*$. Portanto, $M(U)$ é não singular. $\square$

Observação 1.24 Em $M(U)$, U^* é sempre um subespaço totalmente isotrópico, o mesmo pode não ocorrer com U . Se $b = 0$, então U também é um subespaço totalmente isotrópico de $M(U, 0)$. Neste caso, dizemos que $M(U, 0)$ é um *espaço bilinear hiperbólico* que denotamos também por $H(U)$.

Tomemos (U, b) tal que $U = Ae$ e $b(e, e) = 0$. Uma base para $U \oplus U^*$ é $\{e, e^*\}$ e assim, $b_U(e, e) = 0$, $b_U(e, e^*) = e^*(e) = 1$ e $b_U(e^*, e^*) = 0$. Logo,

$$H(U) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

A este espaço bilinear hiperbólico damos o nome de *plano hiperbólico* e denotamos simplesmente por $\mathbf{H}$.

Todo espaço bilinear hiperbólico é uma soma ortogonal de planos hiperbólicos. De fato, consideremos $(U, 0)$ tal que $\dim U = n$. Sejam $\{e_1, \dots, e_n\}$ e $\{e_1^*, \dots, e_n^*\}$ bases de U e U^* respectivamente. Podemos considerar $\{e_1, e_1^*, e_2, e_2^*, \dots, e_n, e_n^*\}$ como base de $U \oplus U^*$. Nesta base

$$\mathbf{H}(U) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \dots \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

com n parcelas. Portanto, $\mathbf{H}(U) = n\mathbf{H}$, onde $n = \dim U$.

Exemplo 1.25 Consideremos (Ae, b) tal que $b(e, e) = \alpha$. Denotamos este módulo simplesmente por $\langle \alpha \rangle$. Como é fácil verificar, $\langle \alpha \rangle$ representa um espaço bilinear se, e somente se, $\alpha \in A^*$. Neste caso,

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

Consideremos agora a seguinte soma ortogonal $\langle \alpha_1 \rangle \perp \langle \alpha_2 \rangle \perp \dots \perp \langle \alpha_n \rangle$, a qual também denotamos por $\langle \alpha_1, \dots, \alpha_n \rangle$. Para $\langle \alpha_1, \dots, \alpha_n \rangle$ ser um espaço bilinear é necessário que $\alpha_i \in A^*$ ($i = 1, \dots, n$), e

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

Esta decomposição fica mais clara com a seguinte proposição:

Proposição 1.26 Se (U, b) admite uma decomposição $U = U_1 \perp U_2$, então $\mathbf{M}(U) \simeq \mathbf{M}(U_1) \perp \mathbf{M}(U_2)$.

Dem.: Imediata. $\square$

O seguinte resultado caracteriza os espaços metabólicos.

Teorema 1.27 *Seja (M, b) um espaço bilinear sobre A . M 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 . De (1.24) segue que V^* é um subespaço totalmente isotrópico e conseqüentemente $V^* \subseteq V^{\perp}$. Mostremos que V^* é maximal. Para tanto, resta mostrarmos que $V^{\perp} \subseteq V^*$. Consideremos $\{e_1, \dots, e_n\}$ e $\{e_1^*, \dots, e_n^*\}$ bases de V e V^* . Seja $u + u^* \in V^{\perp}$. Então $b_V(u + u^*, v^*) = 0$ para todo $v^* \in V^*$, em particular $b_V(u + u^*, e_i^*) = 0$ para $i = 1, \dots, n$. Assim $u_i = e_i^*(u) = 0$ ($i = 1, \dots, n$), onde u_i é a i -ésima coordenada de u na base $\{e_1, \dots, e_n\}$. Logo, $u = 0$, ou seja, $u + u^* \in V^*$. Portanto, $V^{\perp} \subseteq V^*$.

Reciprocamente, se $U \subseteq M$ é um subespaço totalmente isotrópico com $U = U^{\perp}$, então por (1.21) temos que existe $V \subseteq M$ tal que $U \cong V^*$ e $M \cong V \oplus U$. Consideremos a aplicação $d : U \rightarrow V^*$, onde $d(u)(v) = b(u, v)$ para todo $u \in U$ e $v \in V$. Como $b : U \times V \rightarrow A$ é não singular, segue que d é um isomorfismo. Seja $f : M \rightarrow M(V) = V \oplus V^*$ o isomorfismo definido por $f(v + u) = v + d(u)$. Mostremos que f é uma isometria. De fato, $b_V(f(v + u), f(v' + u')) = b_V(v + d(u), v' + d(u')) = b(v, v') + d(u)(v') + d(u')(v) = b(v, v') + b(u, v') + b(u', v) = b(v + u, v' + u')$ sendo que a última igualdade decorre de $b(u, u') = 0$. Portanto, $M \cong M(V)$ é metabólico. $\square$

Corolário 1.28 (i) *Para $(V, b) \in \text{Bil}(A)$ e (U, b') um módulo bilinear temos que $M(U) \otimes (V, b) \simeq M(U \otimes V)$.*

(ii) *Seja $(U, b) \in \text{Bil}(A)$. Então $(U, b) \perp (U, -b) \simeq M(U)$, onde $-b(x, y) = (-1)b(x, y)$ para todo $x, y \in U$.*

Dem.:(i) Desde que

$$M(U) \otimes V = (U \oplus U^*) \otimes V = (U \otimes V) \oplus (U^* \otimes V)$$

e U^* é um subespaço totalmente isotrópico de $M(U)$ temos que $U^* \otimes V$ é um subespaço totalmente isotrópico de $M(U) \otimes V$ e, conseqüentemente, $U^* \otimes V \subseteq (U^* \otimes V)^{\perp}$. Pelo teorema resta mostrarmos que $(U^* \otimes V)^{\perp} \subseteq U^* \otimes V$, ou seja,

que $U^* \otimes V$ é um subespaço totalmente isotrópico maximal de $M(U) \otimes V$. Para tanto, consideremos $(u_1 + u_1^*) \otimes v_1$ um elemento genérico de $(U^* \otimes V)^\perp$. 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 b é não singular segue que existem $v_1, v \in V$ tais que $b(v_1, v) \in A^*$. Logo,

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

para todo $u^* \in U^*$. Consequentemente, $u^*(u_1) = 0$ para todo $u^* \in U^*$, ou seja, $u_1 = 0$, o que mostra que $(U^* \otimes V)^\perp \subseteq U^* \otimes V$ como queríamos.

(ii) O resultado segue do fato de que $(U, b) \perp (U, -b)$ contém o subespaço totalmente isotrópico maximal $V = \{(x, x) : x \in U\}$ que é naturalmente isomorfo a U . $\square$

1.5 Decomposição de Espaços Bilineares

Um resultado básico da teoria de formas quadráticas sobre corpos é que todo espaço quadrático sobre um corpo de característica distinta de 2 admite uma base ortogonal. No caso em que o corpo tem característica 2, todo espaço quadrático é uma soma ortogonal de subespaços bidimensionais. Para o caso de um anel local mostramos um resultado análogo que depende da próxima definição.

Definição 1.29 Sejam $(M, b) \in \text{Bil}(A)$ e $\{b(x, x) : x \in M\}$ um subconjunto de A . Se o ideal gerado por este subconjunto é todo o anel A , diremos que o espaço (M, b) é *próprio*. Caso contrário, dizemos que (M, b) é *impróprio*.

Teorema 1.30 Seja $(M, b) \in \text{Bil}(A)$.

- (i) Se (M, b) é próprio, então (M, b) admite uma base ortogonal.
- (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 $\alpha, \beta \in M$.

Dem.: Se $\dim M = 1$ nada há a demonstrar. Podemos então supor $\dim M = n \geq 2$. Seja $\{e_1, \dots, e_n\}$ uma base de M . Mostremos, primeiramente,

que existem $w_1, w_2 \in M$ tais que $\det(b(w_i, w_j)) \in A^*$ para $1 \leq i, j \leq 2$. No caso em que (M, b) é próprio, também é possível escolher w_1 tal que $b(w_1, w_1) \in A^*$. Consideremos, separadamente, os casos próprio e impróprio.

(M, b) é próprio. Então existe $x \in M$ tal que $b(x, x) \in A^*$, pois A é um anel local. Assim (Ax, b) é um subespaço não singular de (M, b) e de (1.20) segue que $(M, b) \simeq (Ax, b) \perp (V_1, b)$ onde $V_1 = (Ax)^\perp$. Denotamos simplesmente por b as restrições de b a subespaços de M . Agora, se V_1 também é próprio, então existe $y \in V_1$ tal que $b(y, y) \in A^*$. Neste caso $w_1 = x$ e $w_2 = y$ satisfazem o requerido. Porém, se V_1 é impróprio existem $y, z \in V_1$ tais que $b(y, z) \in A^*$, pois (V_1, b) é não singular. Tomando $w_1 = x + y$ e $w_2 = x + \lambda z$ onde $\lambda = -b(x, x)/b(y, z)$, temos que $\det(b(w_i, w_j)) \in A^*$ e $b(w_1, w_1) \in A^*$.

(M, b) é impróprio. Como (M, b) é não singular a matriz (b_{ij}) que determina b é inversível, ou seja, cada linha ou coluna gera o anel A e, como A é local, isto só ocorre se algum elemento da linha (ou coluna) for unidade. Temos então em cada linha (ou coluna) um elemento $b(e_i, e_j) \in A^*$ com $i \neq j$, pois $b(e_i, e_i) \notin A^*$ para $i = 1, \dots, n$. Assim, $b_{1j} \in A^*$ para algum $j \neq 1$ e $b_{i1} \in A^*$ para algum $i \neq 1$. Se trocarmos a segunda coluna pela j -ésima coluna e a segunda linha pela i -ésima linha, obtemos uma nova matriz (b'_{ij}) . A submatriz

$$\begin{pmatrix} b'_{11} & b'_{12} \\ b'_{21} & b'_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{1j} \\ b_{i1} & b_{ij} \end{pmatrix}$$

é inversível. Isto mostra que existe uma matriz mudança de base T (que reorganiza as linhas e colunas de (b_{ij})) tal que para $w_1 = T[e_1]$ e $w_2 = T[e_2]$ temos $\det(b(w_i, w_j)) \in A^*$, $1 \leq i, j \leq 2$, como queríamos.

Agora, se (M, b) é próprio então existem $w_1, w_2 \in M$ tais que $\det(b(w_i, w_j))b(w_1, w_1) \in A^*$ para $1 \leq i, j \leq 2$. Logo, $(Aw_1 + Aw_2, b)$ é um subespaço não singular de M , o que implica que $(M, b) \simeq (Aw_1 + Aw_2, b) \perp (M_1, b)$ onde $M_1 = (Aw_1 + Aw_2)^\perp$ (cf.1.20). Sendo $(Aw_1 + Aw_2, b)$ não singular e $b(w_1, w_1) \in A^*$ temos que $(Aw_1 + Aw_2, b) \simeq (Aw_1, b) \perp (M_2, b)$ onde $M_2 = (Aw_1)^\perp$. Assim, existe $u_2 \in M$ tal que $(M_2, b) \simeq (Au_2, b)$ onde $b(u_2, u_2) \in A^*$. Logo, $(M, b) \simeq Aw_1 \perp M_3$ com (M_3, b) próprio, e o item (i) segue por indução sobre $\dim_A M$.

Se (M, b) é impróprio provamos que existem $w_1, w_2 \in M$ tais que $(Aw_1 + Aw_2, b)$ é um subespaço não singular de M . Assim, $(M, b) \simeq (Aw_1 + Aw_2, b) \perp (M_1, b)$. Considerando que se (M, b) é impróprio então todos os seus subespaços também o são, temos que (M_1, b) é impróprio. Por indução sobre $\dim_A M$ obtemos que $(M, b) \simeq (M_1, b) \perp \cdots \perp (M_r, b)$ com $\dim M_i = 2$ ($i = 1, \dots, r$). Desta decomposição segue, em particular, que $\dim_A M$ é par.

Para provarmos completamente (ii), resta mostrarmos que cada subespaço (M_i, b) pode ser escrito na forma

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

com $\alpha, \beta \in \mathcal{M}$. Para tanto, seja $\{w_1, w_2\}$ uma base de M_i . Se $c_{ij} = b(w_i, w_j)$ para $1 \leq i, j \leq 2$, então $\det(c_{ij}) \in A^*$. Desde que (c_{ij}) é inversível, temos que cada linha ou coluna de (c_{ij}) gera A . Em particular, os elementos c_{11} e c_{12} geram A . Como $c_{11} \notin A^*$ e A é um anel local temos que $c_{12} \in A^*$. Logo, tomando $w'_1 = c_{12}^{-1}w_1$ e $w'_2 = w_2$ temos

$$(M_i, b) \simeq \begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$$

com $\alpha = c_{12}^{-2}c_{11} \in \mathcal{M}$ e $\beta = c_{22} \in \mathcal{M}$, como queríamos. $\square$

Corolário 1.31 *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. $\square$

Capítulo 2

O Anel de Witt

Neste capítulo construímos o Anel de Witt dos espaços bilineares sobre um anel local e apresentamos uma caracterização de seus geradores.

2.1 $\widehat{W}(A)$ e $W(A)$

Consideremos o conjunto $Bil(A)$ com suas operações $\perp$ e $\otimes$. Denotamos por B o conjunto das classes de isometria de espaços bilineares sobre A . Cada elemento de B é representado simplesmente por b . As operações induzidas em B por $\perp$ e $\otimes$ são também denotadas por $\perp$ e $\otimes$.

No conjunto $B \times B$ definamos a seguinte relação de equivalência:

$$(b_1, b_2) \sim (b'_1, b'_2) \iff \exists b_3 \in Bil(A) ; b_1 \perp b'_2 \perp b_3 \simeq b'_1 \perp b_2 \perp b_3.$$

É fácil verificar que $B \times B / \sim$, com as operações $+$, $\cdot$ induzidas de $B \times B$, é um anel comutativo com elemento identidade. Este anel é denominado o *Anel de Witt-Groethendieck dos espaços bilineares sobre A* e denotado por $\widehat{W}(A)$.

Os elementos de $\widehat{W}(A)$ são denotados por $[(b_1, b_2)]$. O elemento neutro da soma é $[(0, 0)]$, onde 0 é o espaço bilinear $(\emptyset, 0)$, o elemento identidade é $[(1, 0)]$, onde $1 = \langle 1 \rangle$, e o oposto de $[(b_1, b_2)]$ é $[(b_2, b_1)]$.

Considerando o homomorfismo $f : B \rightarrow \widehat{W}(A)$ dado por $f(b) = [(b, 0)]$, que denotamos simplesmente por $[b]$, com esta notação, temos que todo elemento $[(b_1, b_2)]$ de $\widehat{W}(A)$ pode ser escrito na forma $[b_1] - [b_2]$. Neste contexto, $[b_1] - [b_2] = [b'_1] - [b'_2]$ em $\widehat{W}(A)$ se, e somente se, existe $b \in \text{Bil}(A)$ tal que $b_1 \perp b'_2 \perp b \simeq b_2 \perp b'_1 \perp b$.

Observação 2.1 O Anel $\widehat{W}(A)$ satisfaz a propriedade universal, ou seja, qualquer homomorfismo de grupos $f : B \rightarrow G$, com G um grupo abeliano, se estende a um único homomorfismo de grupos $g : \widehat{W}(A) \rightarrow G$ definido por $g([b_1] - [b_2]) = f(b_1) - f(b_2)$. Devido a esta propriedade, $\widehat{W}(A)$ é também chamado o grupo universal de B .

Consideremos agora o seguinte subconjunto de $\widehat{W}(A)$:

$$\widehat{M}(A) = \{ [M(U)] - [M(V)] : U, V \text{ são módulos bilineares} \}.$$

Decorre facilmente do fato de que a soma de dois espaços metabólicos é também metabólico e de (1.28-i), que $\widehat{M}(A)$ é um ideal de $\widehat{W}(A)$.

Definição 2.2 O anel quociente $\widehat{W}(A)/\widehat{M}(A)$ é chamado o *Anel de Witt dos espaços bilineares sobre A* e denotado por $W(A)$. Usamos a mesma notação de $\widehat{W}(A)$ para denotarmos os elementos de $W(A)$.

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 (1.28-ii) 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 $b \in \text{Bil}(A)$.

Proposição 2.3 Em $W(A)$, $[b_1] = [b_2]$ se, e somente se, existem U, V módulos bilineares tais que $b_1 \perp M(U) \simeq b_2 \perp M(V)$.

Dem.: Se $[b_1] = [b_2]$ em $W(A)$, então $[b_1] - [b_2] = [0]$, ou seja, $[b_1] - [b_2] \in \widehat{M}(A)$. Logo, $[b_1] - [b_2] = [M(U_1)] - [M(U_2)]$ em $\widehat{W}(A)$, com U_1, U_2 módulos bilineares. Isto implica que existe $b \in Bil(A)$, tal que $b_1 \perp M(U_2) \perp b \simeq b_2 \perp M(U_1) \perp b$. Logo,

$$b_1 \perp M(U_2) \perp b \perp -b \simeq b_2 \perp M(U_1) \perp b \perp -b.$$

Portanto, de (1.28-ii), temos que $b_1 \perp M(U) \simeq b_2 \perp M(V)$, com U, V módulos bilineares.

Reciprocamente, se $b_1 \perp M(U) \simeq b_2 \perp M(V)$, então $[b_1 \perp M(U)] = [b_2 \perp M(V)]$ em $W(A)$. É fácil ver que $[b \perp M(W)] = [b]$ em $W(A)$ para todo $b \in Bil(A)$ e $M(W)$ um espaço metabólico qualquer. Portanto $[b_1] = [b_2]$ em $W(A)$. $\square$

O próximo resultado estabelece uma relação estrita entre os espaços metabólicos e os espaços bilineares hiperbólicos. Estes últimos, por serem somas ortogonais de planos hiperbólicos, são, muitas vezes, mais convenientes de se trabalhar.

Proposição 2.4 *Seja (U, b) um módulo bilinear. Então*

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

Dem.: Recordemos que $M(U, b) = (U \oplus U^*, b_U)$ onde

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

Sejam $\{e_1, \dots, e_n\}$ e $\{e_1^*, \dots, e_n^*\}$ bases de U e U^* respectivamente. Na base $\{e_1^*, \dots, e_n^*, e_1, \dots, e_n\}$ de $U \oplus U^*$ temos que

$$M(U, b) = \begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix},$$

onde b representa a matriz do módulo bilinear b relativa a base $\{e_1, \dots, e_n\}$ e, $1, 0$ representam a matriz identidade e a matriz nula $n \times n$ respectivamente. Note

que nesta base temos ainda que:

$$\mathbf{M}(U, -b) = \begin{pmatrix} 0 & -1 \\ -1 & -b \end{pmatrix},$$

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

Considerando a matriz inversível $C = \begin{pmatrix} 1 & 0 & 1 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, obtemos

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

Desta igualdade de matrizes e de (1.14) segue que

$$\mathbf{M}(U, b) \perp \mathbf{M}(U, -b) \simeq \mathbf{H}(U) \perp \mathbf{M}(U, -b). \quad \square$$

Corolário 2.5 *Para todo módulo bilinear (U, b) sobre A , $\mathbf{M}(U) = \mathbf{H}(U)$ em $\widehat{W}(A)$.*

Dem.: Imediata. $\square$

Consideremos o subconjunto de $\widehat{W}(A)$:

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

Pelo resultado acima temos que $\widehat{\mathbf{H}}(A) = \widehat{\mathbf{M}}(A)$. Agora, de (1.24), se $\dim U = m$ e $\dim V = n$ temos que $\mathbf{H}(U) \simeq m\mathbf{H}$ e $\mathbf{H}(V) \simeq n\mathbf{H}$. Assim,

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

com $m - n \in \mathbf{Z}$. Portanto, podemos identificar $\widehat{\mathbf{H}}(A)$ com $\mathbf{ZH}$.

Das observações acima e da definição de $W(A)$ segue que

$$W(A) = \widehat{W}(A)/ZH.$$

Obviamente, $[b_1] = [b_2]$ em $W(A)$ se, e somente se, existem $m, n \in \mathbb{Z}$ tais que $b_1 \perp mH \simeq b_2 \perp nH$.

Proposição 2.6 *Dois espaços bilineares são iguais em $\widehat{W}(A)$ se, e somente se, são iguais em $W(A)$ e tem a mesma dimensão.*

Dem.: 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 $b_1 \perp mH \simeq b_2 \perp nH$. Como $\dim b_1 = \dim b_2$, igualando as dimensões temos que $m = n$. Portanto, $[b_1] = [b_2]$ em $\widehat{W}(A)$. A recíproca é imediata. $\square$

2.2 Geradores de $W(A)$

Nesta seção caracterizamos os geradores do anel $W(A)$, o que facilita o desenvolvimento dos próximos capítulos.

Consideremos o grupo das classes quadradas $G = A^*/(A^*)^2$ e o homomorfismo de grupos $f : G \rightarrow W(A)$ que leva cada classe $(a) \in G$ em $[< a >] \in W(A)$.

Proposição 2.7 *O anel $W(A)$ é aditivamente gerado por $f(G)$.*

Dem.: Seja b um espaço bilinear sobre A . O espaço $b \perp < 1 >$ é próprio e portanto tem uma base ortogonal, ou seja, existem $\beta_1, \dots, \beta_n \in A^*$ tais que $b \perp < 1 > \simeq < \beta_1 > \perp \dots \perp < \beta_n >$. Assim,

$$b \perp < 1 > \perp < -1 > \simeq < \beta_1 > \perp \dots \perp < \beta_n > \perp < -1 > .$$

Logo, em $W(A)$ temos que

$$[b] = [< \beta_1, \dots, \beta_n, -1 >] = [< \beta_1 >] + \dots + [< \beta_n >] + [< -1 >].$$

Portanto, todo elemento de $W(A)$ se escreve como uma soma de elementos de $f(G)$. $\square$

Baseados neste resultado podemos afirmar que existe um homomorfismo de anéis sobrejetor $\varphi : \mathbf{Z}[G] \rightarrow W(A)$, que é a extensão de f . O próximo resultado caracteriza o núcleo $\mathcal{K}$ deste homomorfismo.

Proposição 2.8 *O ideal $\mathcal{K}$ é aditivamente gerado por $(1) + (-1)$ e por todos os elementos da forma $\sum_{i=1}^n (\alpha_i) - \sum_{i=1}^n (\beta_i)$, para algum $n \in \mathbf{N}$, tais que*

$$< \alpha_1, \dots, \alpha_n > \simeq < \beta_1, \dots, \beta_n > .$$

Dem.: Claramente os elementos deste tipo estão em $\mathcal{K}$. Por outro lado, seja $z = (\alpha_1) + \dots + (\alpha_r) - (\beta_1) - \dots - (\beta_s) \in \mathcal{K}$. Trocando z por $-z$ se necessário, podemos assumir $r \geq s$.

Assim, $0 = \varphi(z) = [< \alpha_1, \dots, \alpha_r >] - [< \beta_1, \dots, \beta_s >]$ em $W(A)$. Logo, $b_1 = < \alpha_1, \dots, \alpha_r >$ e $b_2 = < \beta_1, \dots, \beta_s >$ são tais que $[b_1] = [b_2]$ em $W(A)$, ou seja, existem $m, n \in \mathbf{Z}$ tais que $b_1 \perp m\mathbf{H} \simeq b_2 \perp n\mathbf{H}$.

Calculando as dimensões temos que $r + 2m = s + 2n$, ou seja, $r - s = 2t$ para algum $t \in \mathbf{N}$. Obviamente $[b_1] = [b_2 \perp t < 1, -1 >]$ em $W(A)$ e os espaços b_1 e $b_2 \perp t < 1, -1 >$ tem a mesma dimensão. Logo, de (2.6) segue que eles representam o mesmo elemento em $\widehat{W}(A)$. Assim, existe $b_3 \in \text{Bil}(A)$ tal que

$$b_1 \perp b_3 \simeq b_2 \perp t < 1, -1 > \perp b_3.$$

Adicionando $< 1 >$ em ambos os lados, se necessário, podemos assumir que b_3 é próprio, ou seja, existem $\alpha_{r+1}, \dots, \alpha_n \in A^*$ tais que $b_3 \simeq < \alpha_{r+1}, \dots, \alpha_n >$. Logo, $b_1 \perp b_3 \simeq < \alpha_1, \dots, \alpha_n >$. Conseqüentemente, tomando $\beta_i = \pm 1$ para $s < i \leq r$ e $\beta_i = \alpha_i$ para $r < i \leq n$, obtemos

$$b_2 \perp t < 1, -1 > \perp b_3 \simeq < \beta_1, \dots, \beta_n > .$$

Assim,

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

$$\text{pois } \sum_{i=r+1}^n (\alpha_i) = b_3 = \sum_{i=r+1}^n (\beta_i).$$

Portanto,

$$z = t((1) + (-1)) + \sum_{i=1}^n (\alpha_i) - \sum_{i=1}^n (\beta_i) \quad \text{para algum } t \in \mathbb{N} \text{ e algum } n \in \mathbb{N},$$

com $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$, como queríamos. $\square$

Quando não houver perigo de confusão denotamos os elementos $[b]$ de $W(A)$ simplesmente por b . Dentro do contexto se torna claro quando consideramos b como um elemento de $W(A)$ ou um elemento de $Bil(A)$.

Teorema 2.9 *O anel $W(A)$ é aditivamente gerado por $\{\langle \alpha \rangle; \alpha \in A^*\}$ com as seguintes relações:*

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

Dem.: Os itens (i),(ii),(iii) e (v) seguem facilmente do fato de que dois espaços bilineares isométricos são iguais em $W(A)$. Provemos (iv) com mais detalhes. Consideremos $(M, b) = \langle \alpha \rangle + \langle \beta \rangle$. Então existe uma base $\{e_1, e_2\}$ de M tal que $b(e_1, e_1) = \alpha$, $b(e_2, e_2) = \beta$ e $b(e_1, e_2) = 0$. Assim, $b(e_1 + e_2, e_1 + e_2) = \alpha + \beta$. Se $\alpha + \beta \in A^*$, então $A(e_1 + e_2)$ é um subespaço não singular de M e, mais ainda, $M = A(e_1 + e_2) \perp (A(e_1 + e_2))^\perp$. Como $(A(e_1 + e_2))^\perp$ é um subespaço não singular de M unidimensional, existe $e_3 \in V$ tal que $b(e_3, e_3) = \gamma \in A^*$ e $b(e_1 + e_2, e_3) = 0$. Assim,

$$\langle \alpha \rangle \perp \langle \beta \rangle \simeq \langle \alpha + \beta \rangle \perp \langle \gamma \rangle.$$

De (1.15) segue que $\alpha\beta \equiv \alpha\beta(\alpha+\beta)\gamma \bmod (A^*)^2$. Isto implica que $\alpha\beta(\alpha+\beta)^{-1} \equiv \gamma \bmod (A^*)^2$, ou seja, $\gamma \equiv \alpha\beta(\alpha+\beta) \bmod (A^*)^2$. Logo, $\langle \gamma \rangle = \langle \alpha\beta(\alpha+\beta) \rangle$ por (i). Consequentemente,

$$\langle \alpha \rangle \perp \langle \beta \rangle \simeq \langle \alpha + \beta \rangle \perp \langle \alpha\beta(\alpha + \beta) \rangle .$$

Portanto, $\langle \alpha \rangle + \langle \beta \rangle = \langle \alpha + \beta \rangle + \langle \alpha\beta(\alpha + \beta) \rangle$, por (ii). $\square$

Capítulo 3

Ideais de $W(A)$

3.1 Os Ideais Primos de $W(A)$

Nesta seção caracterizamos os ideais primos de $W(A)$ usando o fato de que $W(A) \cong \mathbf{Z}[G]/\mathcal{K}$, onde $G = A^*/(A^*)^2$ e $\mathcal{K}$ é bem determinado em (2.8), ou seja, usamos o fato de que os ideais primos de $W(A)$ estão em correspondência biunívoca com os ideais primos de $\mathbf{Z}[G]$ que contém $\mathcal{K}$.

Para tanto, comecemos por determinar todos os ideais primos de $\mathbf{Z}[G]$. Os resultados que seguem valem para qualquer grupo G de expoente 2, em particular para $A^*/(A^*)^2$.

Lema 3.1 (i) *Para cada ideal primo $\mathcal{P}$ de $\mathbf{Z}[G]$, com $\mathbf{Z} \cap \mathcal{P} = \{0\}$, existe um único homomorfismo de anéis ϕ de $\mathbf{Z}[G]$ em $\mathbf{Z}$ com núcleo $\mathcal{P}$.*

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

Dem.: Seja $\mathcal{P}$ um ideal primo de $\mathbf{Z}[G]$. Como $g^2 = 1$ para todo $g \in G$, temos que $g^2 - 1 = 0 \in \mathcal{P}$. Assim $(g - 1)(g + 1) \in \mathcal{P}$. O que implica que $g - 1 \in \mathcal{P}$

ou $g + 1 \in \mathcal{P}$, pois $\mathcal{P}$ é primo. Logo, $g \equiv \pm 1 \pmod{\mathcal{P}}$ para todo $g \in G$. Assim, obtemos que

$$\frac{\mathbb{Z}[G]}{\mathcal{P}} \cong_{\bar{\phi}} \mathbb{Z} \quad \text{ou} \quad \frac{\mathbb{Z}[G]}{\mathcal{P}} \cong_{\bar{\psi}} \mathbb{F}_p.$$

No primeiro caso, $\mathbb{Z} \cap \mathcal{P} = \{0\}$ e, no segundo, $\mathbb{Z} \cap \mathcal{P} = p\mathbb{Z}$. Assim, estes isomorfismos induzem os homomorfismos ϕ e ψ requeridos. A unicidade de ϕ e ψ decorre do fato de que $\mathbb{Z}$ e $\mathbb{F}_p$ admitem somente a identidade como automorfismo. $\square$

Como para todo ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, $\mathcal{P} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$, o Lema (3.1) considera todos os ideais primos de $\mathbb{Z}[G]$.

Para melhor caracterizarmos os ideais primos de $\mathbb{Z}[G]$ precisamos descrever, com mais detalhes, os homomorfismos ϕ e ψ .

Como $g^2 = 1$ para todo $g \in G$ 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 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 à 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:

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

onde π é o homomorfismo canônico de $\mathbb{Z}$ em $\mathbb{F}_p$.

Finalmente, 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 $\psi_0 : \mathbb{Z}[G] \rightarrow \mathbb{F}_2$, que é obtido da composição de $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$ com a projeção

canônica sobre $\mathbf{F}_2$, onde ϕ_χ é a extensão de qualquer caracter $\chi : G \rightarrow \{\pm 1\}$.

Destas observações e do Lema (3.1) temos:

Proposição 3.2 (i) Para cada ideal primo $\mathcal{P}$ de $\mathbf{Z}[G]$, com $\mathbf{Z} \cap \mathcal{P} = \{0\}$, existe um único caracter χ de G , tal que $\mathcal{P} = \mathcal{P}_\chi$ é o núcleo do homomorfismo ϕ_χ de $\mathbf{Z}[G]$ em $\mathbf{Z}$.

(ii) Para cada ideal primo $\mathcal{P}$ de $\mathbf{Z}[G]$, com $\mathcal{P} \cap \mathbf{Z} = p\mathbf{Z}$ (p um número primo ímpar), existe um único caracter χ de G , tal que $\mathcal{P}$ coincide com o conjunto

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

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

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

para cada caracter χ de G .

Observação 3.3 Os ideais $\mathcal{P}_\chi$ são todos os ideais primos minimais de $\mathbf{Z}[G]$ e os ideais $\mathcal{P}_{\chi,p}$ e $\mathcal{P}_0$ são todos os maximais.

Conhecidos os ideais primos de $\mathbf{Z}[G]$ vamos caracterizar os ideais primos de $W(A)$. Consideremos o seguinte homomorfismo de anéis $d_o : W(A) \rightarrow \mathbf{F}_2$, definido por $d_o([b]) = (\dim b) \pmod{2}$. Denotamos por $I(A)$ o seu núcleo. Desde que $W(A)/I(A) \cong \mathbf{F}_2$, temos que $I(A)$ é um ideal primo de $W(A)$.

Proposição 3.4 $I(A)$ é o único ideal primo de $W(A)$ que contém $2 < 1 > = 2 \cdot 1_{W(A)}$.

Dem.: Resta mostrarmos apenas a unicidade. O item (iii) da proposição anterior garante que $\mathcal{P}_0$ é o único ideal primo de $\mathbf{Z}[G]$ que contém 2. Como $\varphi(2) = 2 < 1 >$ temos que $\mathcal{P}_0$ está em correspondência com $I(A)$. Portanto, a unicidade de $I(A)$ decorre da unicidade de $\mathcal{P}_0$. $\square$

Definição 3.5 Uma *assinatura* σ 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 tem pelo menos uma assinatura, ou seja, se $Ass(A) \neq \emptyset$. Caso contrário, A é *não formalmente real*.

Pelo Teorema do Isomorfismo para anéis, é imediato que $W(A)/\mathcal{P}_\sigma \cong \mathbb{Z}$ para toda $\sigma \in Ass(A)$.

Proposição 3.6 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 $W(A) \cong \mathbb{Z}[G]/\mathcal{K}$, 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 $\mathcal{P}' \cap \mathbb{Z} = \{0\}$. Pelo item (i) da Prop.(3.2) existe um único homomorfismo de anéis $\phi_\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$, tal que $Ker \phi_\chi = \mathcal{P}'$. Mas $\mathcal{K} \subseteq Ker \phi_\chi$. Logo, existe uma única $\sigma \in Ass(A)$ que faz o diagrama abaixo comutar:

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

Resta mostrarmos que $\mathcal{P} = \mathcal{P}_\sigma$.

Desde que $0 = \phi_\chi(\mathcal{P}') = \sigma \circ \varphi(\mathcal{P}') = \sigma(\mathcal{P})$, temos que $\mathcal{P} \subseteq \mathcal{P}_\sigma$. Por outro lado, tomemos $b \in \mathcal{P}_\sigma$. 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, $x \in Ker \phi_\chi = \mathcal{P}'$. Logo, $\varphi(x) = b \in \mathcal{P}$. Portanto, $\mathcal{P}_\sigma \subseteq \mathcal{P}$, como queríamos. $\square$

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 lema que segue.

Lema 3.7 Para cada caracter χ de G , temos que $\phi_\chi(\mathcal{K}) = 0$ ou $\phi_\chi(\mathcal{K}) = 2^n \mathbb{Z}$, 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.

$$\text{Seja } z = \sum_{i=1}^n (\alpha_i) - \sum_{i=1}^n (\beta_i) \in \mathbb{Z}[G],$$

tal que $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$. Sejam s o número de elementos (α_i) , $1 \leq i \leq n$, com $\phi_\chi((\alpha_i)) = -1$ e t o número de elementos (β_i) , $1 \leq i \leq n$, 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,

$$\prod_{i=1}^n \alpha_i \equiv \prod_{i=1}^n \beta_i \pmod{(A^*)^2}.$$

Aplicando ϕ_χ nesta igualdade e usando que $\phi_\chi((\alpha^2))$, para todo $\alpha \in A^*$, obtemos $(-1)^s = (-1)^t$, isto é, $t-s$ é um número par. Conseqüentemente, $\phi_\chi(z) \equiv 0 \pmod{4}$.

Portanto, $\phi_\chi(\mathcal{K}) = 0$ ou $\phi_\chi(\mathcal{K}) = 2^n \mathbb{Z}$ para algum $n \geq 1$. $\square$

Como consequência imediata deste lema temos:

Corolário 3.8 Se $\phi_\chi(\mathcal{K}) \subseteq p\mathbb{Z}$, para algum primo ímpar p , então $\phi_\chi(\mathcal{K}) = 0$.

Dem.: Imediata $\square$

Proposição 3.9 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 $W(A) \cong \mathbb{Z}[G]/\mathcal{K}$, temos que existe $\mathcal{P}' \subseteq \mathbb{Z}[G]$, tal que $\mathcal{K} \subseteq \mathcal{P}'$ e $\varphi(\mathcal{P}') = \mathcal{P}$. Como $p < 1 \in \mathcal{P}$, segue que $\mathcal{P}' \cap \mathbb{Z} = p\mathbb{Z}$. Por (3.2-ii), temos que existe um único caracter χ de G , tal que $\mathcal{P}' = \mathcal{P}_{\chi,p} = \{z \in \mathbb{Z}[G] : \phi_\chi(z) \equiv 0 \pmod{p}\}$. De $\mathcal{K} \subseteq \mathcal{P}'$, segue que $\phi_\chi(\mathcal{K}) \subseteq p\mathbb{Z}$, ou seja, $\phi_\chi(\mathcal{K}) = 0$ (cf. : 3.7). Assim $\mathcal{K} \subseteq \text{Ker } \phi_\chi$ e, segue deste fato que existe uma única $\sigma \in \text{Ass}(A)$ que faz o diagrama abaixo comutar:

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

Mostremos que $\mathcal{P} = \mathcal{P}_{\sigma,p}$. Seja $b \in \mathcal{P}$. Então existe $x \in \mathcal{P}'$ tal que $\varphi(x) = b$. Pela definição de $\mathcal{P}'$, $\phi_\chi(x) \equiv 0 \pmod{p}$. Assim, $\sigma(b) = \sigma \circ \varphi(x) = \phi_\chi(x) \equiv 0 \pmod{p}$, ou seja, $b \in \mathcal{P}_{\sigma,p}$. Logo, $\mathcal{P} \subseteq \mathcal{P}_{\sigma,p}$. Tomemos agora $b \in \mathcal{P}_{\sigma,p}$. Segue da sobrejetividade da φ que existe $x \in \mathbb{Z}[G]$ tal que $\varphi(x) = b$. Assim, $\phi_\chi(x) = \sigma \circ \varphi(x) = \sigma(b) \equiv 0 \pmod{p}$, ou seja, $x \in \mathcal{P}'$. Logo, $b = \varphi(x) \in \mathcal{P}$. Portanto, $\mathcal{P}_{\sigma,p} \subseteq \mathcal{P}$, como queríamos. $\square$

Concluimos então que $\mathcal{P}_\sigma$, $\mathcal{P}_{\sigma,p}$ (para $\sigma \in \text{Ass}(A)$ e p um primo ímpar) e $I(A)$ são todos os ideais primos de $W(A)$. O conjunto de todos os ideais primos do anel $W(A)$ é chamado *espectro de $W(A)$* e denotado por $\text{Spec } W(A)$. Os próximos resultados caracterizam melhor os elementos do $\text{Spec } W(A)$.

Teorema 3.10 *Se $\text{Ass}(A) \neq \emptyset$, 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 mostrar (iii) e (iv).

(iii) 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

$p < 1 > \in \mathcal{P}_\sigma$, que é $\mathcal{P}_{\sigma,p}$.

Suponhamos que exista um ideal primo minimal $\mathcal{P}_\psi$, tal que $\mathcal{P}_\psi \subseteq \mathcal{P}_{\sigma,p}$. Como $\mathcal{P}_{\sigma,p}$ contém $\mathcal{P}_\psi$ e $p < 1 > \in \mathcal{P}_{\sigma,p}$ temos que $\mathcal{P}_{\sigma,p} = \mathcal{P}_{\psi,p}$. Segue de (3.9) que $\sigma = \psi$.

Portanto $\mathcal{P}_\sigma = \mathcal{P}_\psi$.

(iv) Dado $\sigma \in \text{Ass}(A)$, queremos mostrar que $\mathcal{P}_\sigma \subseteq I(A)$. Para tanto, seja $b = \langle \alpha_1, \dots, \alpha_n \rangle \in \mathcal{P}_\sigma$. Como $\sigma(\langle 1 \rangle) = 1$, temos que $\sigma(\langle \alpha_i \rangle) = \pm 1$ para $1 \leq i \leq n$. Assim, $\sigma(b) = 0$ implica que para metade dos elementos $\langle \alpha_i \rangle$ temos $\sigma(\langle \alpha_i \rangle) = 1$ e para a outra metade, $\sigma(\langle \alpha_i \rangle) = -1$. Logo, $n = 2m$, ou seja, $b \in I(A)$. Portanto, $\mathcal{P}_\sigma \subseteq I(A)$, como queríamos. $\square$

No caso em que A é não formalmente real, temos:

Proposição 3.11 *As seguintes afirmações são equivalentes:*

- (i) $\text{Ass}(A) = \emptyset$
- (ii) $I(A)$ é o único ideal primo de $W(A)$.
- (iii) $2^n W(A) = 0$, para algum $n \geq 1$.

Dem.: (i) $\Rightarrow$ (ii). Segue trivialmente da descrição dos ideais primos de $W(A)$.

(ii) $\Rightarrow$ (iii). Como $I(A)$ é o único ideal primo de $W(A)$ ele é o nilradical de $W(A)$, ou seja, todos os seus elementos são nilpotentes. Em particular, $2 \langle 1 \rangle \in I(A)$ é nilpotente. Assim, existe $n \geq 1$, tal que $2^n \langle 1 \rangle = [2 \langle 1 \rangle]^n = 0$. Portanto, $2^n W(A) = 0$ para algum $n \geq 1$.

(iii) $\Rightarrow$ (i). Por (iii), temos que todo elemento de $W(A)$ é de torção, ou seja, para todo $b \in W(A)$ existe $n \geq 1$ tal que $nb = 0$. Como $\mathbf{Z}$ é livre de torção, não pode existir homomorfismo de anéis de $W(A)$ em $\mathbf{Z}$. Portanto, $\text{Ass}(A) = \emptyset$. $\square$

O próximo resultado é de fundamental importância no decorrer do nosso trabalho.

Corolário 3.12 *Seja A um anel local. Existe uma correspondência biunívoca en-*

tre o conjunto dos ideais primos minimais de $W(A)$ e o conjunto das assinaturas de A .

Dem.: Segue trivialmente de (3.10) e (3.11). $\square$

3.2 Os Ideais Primários de $W(A)$

Esta seção contém uma caracterização dos ideais primários de $W(A)$, onde A é um anel local. Esta caracterização é baseada no que Fitzgerald fez em [5] para corpos de característica distinta de 2. Vale observar que o que é feito aqui, apesar de generalizar o resultado de Fitzgerald, não é relevante para o restante do trabalho.

Estes primeiros resultados sobre ideais primários se encontram demonstrados em [1].

Definição 3.13 Um ideal $Q \subseteq A$, $Q \neq A$ é *primário* se $xy \in Q$ implica em $x \in Q$ ou $y^n \in Q$ para algum $n > 0$. Em outras palavras, Q é primário se, e somente se, $A/Q \neq \{0\}$ e todo divisor de zero em A/Q é nilpotente.

Definição 3.14 Seja $E \subseteq A$ um subconjunto qualquer de A . Definimos como sendo o *radical de E* , que denotamos por $r(E)$, o conjunto:

$$r(E) = \{x \in A : x^n \in E, \text{ para algum } n > 0\}$$

Lema 3.15 Se $\mathcal{A} \subseteq A$, então $r(\mathcal{A})$ é também um ideal de A . Mais ainda, $r(\mathcal{A})$ é a intersecção de todos os ideais primos de A que contém $\mathcal{A}$.

Proposição 3.16 Seja Q um ideal primário de A . Então, $r(Q)$ é o menor ideal primo contendo Q .

Se $\mathcal{P} = r(Q)$ dizemos que Q é $\mathcal{P}$ -*primário*. Em geral, se $r(\mathcal{A})$ é um ideal primo, não podemos afirmar que $\mathcal{A}$ é primário. Vale, porém, o seguinte resultado:

Proposição 3.17 Se $r(\mathcal{A})$ é maximal, então $\mathcal{A}$ é primário. Em particular, as potências de um ideal maximal $\mathcal{M}$ são $\mathcal{M}$ -*primárias*.

Podemos, agora, analisar os ideais primários de $W(A)$.

Lema 3.18 *Cada ideal primo $\mathcal{P}_\sigma$ de (3.10) é gerado pelas formas bilineares $\langle 1, -\alpha \rangle$, onde $\alpha \in A^*$ e $\sigma(\langle \alpha \rangle) = 1$.*

Dem.: Obviamente as formas do tipo $\langle 1, -\alpha \rangle$ pertencem a $\mathcal{P}_\sigma$. Seja $b = \langle \alpha_1, \dots, \alpha_n \rangle \in \mathcal{P}_\sigma$. Então $n = 2m$ para algum m , pois $\mathcal{P}_\sigma \subseteq I(A)$. Como $\sigma(b) = 0$, temos que $\sigma(\langle \alpha_i \rangle) = 1$ para metade dos α_i e $\sigma(\langle \alpha_i \rangle) = -1$, para a outra metade. Consideremos $\alpha_i = \beta_i$, se $\sigma(\langle \alpha_i \rangle) = 1$, e $\alpha_i = -\gamma_i$, se $\sigma(\langle \alpha_i \rangle) = -1$. Assim,

$$\langle \alpha_1, \dots, \alpha_n \rangle = \sum_{i=1}^m \langle 1, -\gamma_i \rangle - \sum_{i=1}^m \langle 1, -\beta_i \rangle$$

em $W(A)$, com $\sigma(\langle \beta_i \rangle) = \sigma(\langle \gamma_i \rangle) = 1$, como queríamos. $\square$

A próxima proposição caracteriza os ideais de $W(A)$ que são $\mathcal{P}_\sigma$ -primário, para $\sigma \in \text{Ass}(A)$.

Proposição 3.19 *Sejam $\mathcal{J} \subseteq W(A)$ um ideal e $\sigma \in \text{Ass}(A)$. Então $\mathcal{J}$ é $\mathcal{P}_\sigma$ -primário se, e somente se, $\mathcal{J} = \mathcal{P}_\sigma$.*

Dem. : Como todo ideal primo é primário e $r(\mathcal{P}_\sigma) = \mathcal{P}_\sigma$, temos que $\mathcal{P}_\sigma$ é $\mathcal{P}_\sigma$ -primário.

Reciprocamente, se $\mathcal{J}$ é $\mathcal{P}_\sigma$ -primário, então $\mathcal{J} \subseteq r(\mathcal{J}) = \mathcal{P}_\sigma$. Suponhamos que $\mathcal{J} \neq \mathcal{P}_\sigma$. Então existe $\alpha \in A^*$ com $\sigma(\langle \alpha \rangle) = 1$, tal que $\langle 1, -\alpha \rangle \notin \mathcal{J}$. Desde que $\langle 1, -\alpha \rangle \in \mathcal{P}_\sigma$ e $\mathcal{J}$ é $\mathcal{P}_\sigma$ -primário, temos que $\langle 1, -\alpha \rangle^m \in \mathcal{J}$, para algum $m > 0$. Mas $\langle 1, -\alpha \rangle^m = 2^{m-1} \langle 1, -\alpha \rangle \in \mathcal{J}$ e $\langle 1, -\alpha \rangle \notin \mathcal{J}$; então, da definição de ideal primário, temos que $2^k \langle 1 \rangle \in \mathcal{J} \subseteq \mathcal{P}_\sigma$ para algum $k > 0$. Isto é uma contradição, pois $I(A)$ é o único ideal primo de $W(A)$ que contém $2^k \langle 1 \rangle$. Portanto, $\mathcal{J} = \mathcal{P}_\sigma$. $\square$

Para $n \in \mathbb{Z}$, $n > 0$ e $\sigma \in \text{Ass}(A)$, consideremos o ideal $\mathcal{P}_{\sigma,n}$ de $W(A)$ definido por:

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

Lema 3.20 *Seja $\sigma \in \text{Ass}(A)$ e $n \in \mathbb{Z}$, $n > 0$. Para todo $i > 0$ temos que $\mathcal{P}_{\sigma,n^i} = (\mathcal{P}_{\sigma,n})^i$.*

Dem.: Mostremos inicialmente que $\mathcal{P}_{\sigma,n} = (n < 1 >) + \mathcal{P}_\sigma$, onde $(n < 1 >)$ é o conjunto dos espaços bilineares aditivamente gerados por $n < 1 >$. Obviamente $(n < 1 >) + \mathcal{P}_\sigma \subseteq \mathcal{P}_{\sigma,n}$.

Tomemos $b = < \alpha_1, \dots, \alpha_r > \in \mathcal{P}_{\sigma,n}$. Logo, $\sigma(< \alpha_1, \dots, \alpha_r >) = nz$ para algum $z \in \mathbb{Z}$. Assim, $b = < \alpha_1, \dots, \alpha_s > + < \alpha_{s+1}, \dots, \alpha_r >$, com $\sigma(< \alpha_{s+1}, \dots, \alpha_r >) = 0$ e $\sigma(< \alpha_1, \dots, \alpha_s >) = nz$. Se $z = 0$, então $b \in \mathcal{P}_\sigma$. Podemos supor $z > 0$, trocando α_i por $-\alpha_i$ se necessário. Logo, $\sigma(< \alpha_i >) = 1$ para $1 \leq i \leq s$ e $s = nz$. Em $W(A)$, temos que $< \alpha_1, \dots, \alpha_s > = < \alpha_1, \dots, \alpha_s > + s < 1, -1 >$. Logo,

$$< \alpha_1, \dots, \alpha_s > = s < 1 > - \sum_{i=1}^s < 1, -\alpha_i > \text{ em } W(A),$$

com $\sigma(< \alpha_i >) = 1$ para $1 \leq i \leq s$. De (3.18) segue que $\sum_{i=1}^s < 1, -\alpha_i > \in \mathcal{P}_\sigma$. Obtemos que:

$$< \alpha_1, \dots, \alpha_s > \in (n < 1 >) + \mathcal{P}_\sigma \text{ e } < \alpha_{s+1}, \dots, \alpha_r > \in \mathcal{P}_\sigma.$$

Portanto $b = < \alpha_1, \dots, \alpha_r > \in (n < 1 >) + \mathcal{P}_\sigma$, o que mostra a igualdade desejada.

Mostremos, agora, que $\mathcal{P}_{\sigma,n^i} = (\mathcal{P}_{\sigma,n})^i$. Claramente $(\mathcal{P}_{\sigma,n})^i \subseteq \mathcal{P}_{\sigma,n^i}$. Para mostrarmos que $\mathcal{P}_{\sigma,n^i} = (n^i < 1 >) + \mathcal{P}_\sigma \subseteq (\mathcal{P}_{\sigma,n})^i$ basta mostrarmos que $\mathcal{P}_\sigma \subseteq (\mathcal{P}_{\sigma,n})^i$, pois obviamente $n^i < 1 > \in (\mathcal{P}_{\sigma,n})^i$. Para tanto, tomemos $\alpha \in A^*$ tal que $\sigma(< \alpha >) = 1$. Então para $k = (n-1)/2$, temos que $k < 1, \alpha > \perp < 1 > \in \mathcal{P}_{\sigma,n}$. Em $W(A)$, $< 1, -\alpha > = < 1, -\alpha > \otimes (k < 1, \alpha > \perp < 1 >)^i \in (\mathcal{P}_{\sigma,n})^i$ para todo $\alpha \in A^*$ tal que $\sigma(< \alpha >) = 1$. Logo, de (3.18) segue que $\mathcal{P}_\sigma \subseteq (\mathcal{P}_{\sigma,n})^i$. Portanto, $\mathcal{P}_{\sigma,n^i} = (\mathcal{P}_{\sigma,n})^i$. $\square$

Vamos, agora, caracterizar os ideais de $W(A)$ que são $\mathcal{P}_{\sigma,p}$ -primários, para $\sigma \in \text{Ass}(A)$ e p um número primo ímpar.

Proposição 3.21 *Seja $\mathcal{J} \subseteq W(A)$ um ideal, p um número primo ímpar e $\sigma \in \text{Ass}(A)$. Então $\mathcal{J}$ é $\mathcal{P}_{\sigma,p}$ -primário se, e somente se, $\mathcal{J} = (\mathcal{P}_{\sigma,p})^i$ para algum $i \geq 1$.*

Dem.: De (3.17) é imediato que $(\mathcal{P}_{\sigma,p})^i$ é $\mathcal{P}_{\sigma,p}$ -primário, para $i \geq 1$.

Para provarmos a recíproca, consideremos $\mathcal{J}$ um ideal $\mathcal{P}_{\sigma,p}$ -primário de $W(A)$. Inicialmente, mostremos que $\mathcal{P}_{\sigma} \subseteq \mathcal{J}$. Por (3.18), basta mostrar que $\langle 1, -\alpha \rangle \in \mathcal{J}$ para $\alpha \in A^*$ com $\sigma(\langle \alpha \rangle) = 1$. Consideremos a forma $k \langle 1, \alpha \rangle \perp \langle 1 \rangle$, com $k = (p-1)/2$. Então, $k \langle 1, \alpha \rangle \perp \langle 1 \rangle \in \mathcal{P}_{\sigma,p}$. Assim $(k \langle 1, \alpha \rangle \perp \langle 1 \rangle)^m \in \mathcal{J}$ para algum $m > 0$. Desde que $\langle 1, -\alpha \rangle \otimes (k \langle 1, \alpha \rangle \perp \langle 1 \rangle) = \langle 1, -\alpha \rangle$ em $W(A)$, temos que $\langle 1, -\alpha \rangle = \langle 1, -\alpha \rangle \otimes (k \langle 1, \alpha \rangle \perp \langle 1 \rangle)^m \in \mathcal{J}$.

Consideremos, agora, a sequência de homomorfismos:

$$\mathbf{Z} \xrightarrow{t} \frac{W(A)}{\mathcal{P}_{\sigma}} \xrightarrow{\pi} \frac{W(A)}{\mathcal{J}},$$

onde $t(z) = z \langle 1 \rangle + \mathcal{P}_{\sigma}$ e π é a projeção. Na verdade, t é o isomorfismo inverso do isomorfismo induzido pela assinatura σ . Logo, a composição $\pi \circ t$ é sobrejetora. Assim, $W(A)/\mathcal{J} \cong \mathbf{Z}/m\mathbf{Z}$, para algum $m \geq 0$. Como $p \langle 1 \rangle \in \mathcal{P}_{\sigma,p}$ e $r(\mathcal{J}) = \mathcal{P}_{\sigma,p}$, segue que $p^k \langle 1 \rangle \in \mathcal{J}$, para algum $k \geq 0$. Então, $\pi \circ t(p^k) = 0$ e, conseqüentemente, $p^k \in m\mathbf{Z}$. Logo, $m = p^i$ para algum $i > 0$. Como $\pi \circ t(m) = 0$ em $W(A)/\mathcal{J}$, temos que $m \langle 1 \rangle = p^i \langle 1 \rangle \in \mathcal{J}$. Assim,

$$\frac{W(A)}{\mathcal{J}} \cong \frac{\mathbf{Z}}{p^i \mathbf{Z}} \cong \frac{W(A)}{\mathcal{P}_{\sigma,p^i}}.$$

O segundo isomorfismo segue do homomorfismo $s : W(A) \rightarrow \mathbf{Z}/p^i \mathbf{Z}$ dado por $s(b) = \pi \circ \sigma(b)$, onde π é a projeção canônica. Concluindo, $\mathcal{P}_{\sigma,p^i} = (p^i \langle 1 \rangle) + \mathcal{P}_{\sigma} \subseteq \mathcal{J}$ e, portanto, $\mathcal{J} = \mathcal{P}_{\sigma,p^i} = (\mathcal{P}_{\sigma,p})^i$. $\square$

Finalmente, para caracterizarmos os ideais $I(A)$ -primários de $W(A)$, consideremos o seguinte lema.

Lema 3.22 *O ideal $I(A)$ 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 $W(A)$, como queríamos. $\square$

Proposição 3.23 *Seja $\mathcal{J} \subseteq W(A)$ um ideal. Então $\mathcal{J}$ é $I(A)$ -primário se, e somente se, $2^k \langle 1 \rangle \in \mathcal{J}$ para algum $k > 0$.*

Dem.: Se $\mathcal{J}$ é $I(A)$ -primário, então $r(\mathcal{J}) = I(A)$. Como $2 \langle 1 \rangle \in I(A)$, existe $k > 0$ tal que $2^k \langle 1 \rangle \in \mathcal{J}$. Reciprocamente, suponhamos que $2^k \langle 1 \rangle \in \mathcal{J}$ para algum $k > 0$. Então $\mathcal{J} \subseteq I(A)$, pois $I(A)$ é o único ideal maximal de $W(A)$ que contém $2^k \langle 1 \rangle$. Assim, $r(\mathcal{J}) \subseteq I(A)$, pois $I(A)$ é primo. Resta mostrarmos que $I(A) \subseteq r(\mathcal{J})$. Por (3.22) basta mostrarmos que $\langle 1, \alpha \rangle \in r(\mathcal{J})$ para todo $\alpha \in A^*$. Mas $\langle 1, \alpha \rangle^{k+1} = 2^k \langle 1, \alpha \rangle \in \mathcal{J}$, ou seja, $\langle 1, \alpha \rangle \in r(\mathcal{J})$. Portanto, $\mathcal{J}$ é $I(A)$ -primário. $\square$

Resumindo, temos:

Teorema 3.24 *Se $\text{Ass}(A) \neq \emptyset$, então os ideais primários de $W(A)$ são:*

- (1) $\mathcal{P}_\sigma$, para toda $\sigma \in \text{Ass}(A)$.
- (2) $(\mathcal{P}_{\sigma,p})^i$, para toda $\sigma \in \text{Ass}(A)$, p um número primo ímpar e $i \geq 1$.
- (3) Todo ideal $\mathcal{J}$ contendo $2^k \langle 1 \rangle$, para algum $k > 0$.

Os ideais do tipo (1) são os $\mathcal{P}_\sigma$ -primários, do tipo (2) são os $\mathcal{P}_{\sigma,p}$ -primários e do tipo (3) são os $I(A)$ -primários.

Para o caso em que A é não formalmente real, vale o seguinte resultado:

Proposição 3.25 *Se $\text{Ass}(A) = \emptyset$, então todo ideal de $W(A)$ é $I(A)$ -primário.*

Dem.: Por (3.11), se $\text{Ass}(A) = \emptyset$, então $2^n < 1 > = 0$ em $W(A)$ para algum $n > 0$. Logo, $2^n < 1 >$ pertence a todo ideal de $W(A)$. De (3.23) segue que todo ideal de $W(A)$ é $I(A)$ -primário. $\square$

Capítulo 4

Correspondências entre Ordens, Assinaturas e Ideais Primos

Neste capítulo introduzimos o conceito de ordem de um anel local A , bem como estabelecemos correspondências entre o conjunto das assinaturas de A e um subconjunto específico de ordens de A . No final, são feitas correspondências importantes entre ordens, assinaturas e ideais primos.

Definição 4.1 Um subconjunto $P \subseteq A$ é uma ordem de A se:

- (a) $P + P \subseteq P$
- (b) $P \cdot P \subseteq P$
- (c) $P \cup (-P) = A$
- (d) $P \cap (-P) = \mathcal{P}$, com $\mathcal{P} \in \text{Spec}A$.

O ideal primo $\mathcal{P}$ é chamado *suporte* da ordem P . Dizemos que P é uma *ordem maximal* de A se, para toda ordem P' de A , com $P \subseteq P'$, temos que $P = P'$, ou seja, P é maximal com relação à inclusão. Denotamos por $\mathcal{O}(A)$ o conjunto de todas as ordens de A e por $\mathcal{O}_m(A)$ o conjunto das ordens maximais de A .

Primeiramente, nosso objetivo é construir uma ordem de A a partir de uma assinatura de A . O próximo resultado básico sobre assinaturas nos é útil nesta construção.

Lema 4.2 Se $\sigma \in \text{Ass}(A)$, então:

(i) $\sigma(< -1 >) = -1$

(ii) Se $\alpha_1, \dots, \alpha_n$ são unidades de A com $\sigma(< \alpha_1 >) = \dots = \sigma(< \alpha_n >) = 1$ e $\gamma_1, \dots, \gamma_n$ elementos de A tais que $\beta = \gamma_1^2 \alpha_1 + \dots + \gamma_n^2 \alpha_n$ é uma unidade de A , então $\sigma(< \beta >) = 1$.

Dem.: (i) Como $< 1 > + < -1 > = 0$ em $W(A)$ temos que $\sigma(< 1 >) + \sigma(< -1 >) = 0$. Mas $\sigma(< 1 >) = 1$; logo, $\sigma(< -1 >) = -1$.

(ii) Consideremos $\alpha_1, \dots, \alpha_n \in A^*$ e $\gamma_1, \dots, \gamma_n \in A$ tais que $\beta = \gamma_1^2 \alpha_1 + \dots + \gamma_n^2 \alpha_n \in A^*$. Então $< \beta >$ é um subespaço não-singular de $< \alpha_1, \dots, \alpha_n >$. Logo, de (1.20), $< \alpha_1, \dots, \alpha_n > \simeq < \beta > \perp b'$, para algum $b' \in \text{Bil}(A)$, com $\dim b' = n - 1$. Como $b' \perp < 1 >$ é próprio, segue de (1.31) que existem $\beta_1, \dots, \beta_n \in A^*$, tais que $b' \perp < 1 > \simeq < \beta_1, \dots, \beta_n >$. Assim, $< 1, \alpha_1, \dots, \alpha_n > \simeq < \beta, \beta_1, \dots, \beta_n >$, o que implica que

$$n + 1 = \sigma(< 1, \alpha_1, \dots, \alpha_n >) = \sigma(< \beta, \beta_1, \dots, \beta_n >),$$

pois $\sigma(< \alpha_1 >) = \dots = \sigma(< \alpha_n >) = 1$. Portanto, $\sigma(< \beta_1 >) = \dots = \sigma(< \beta_n >) = \sigma(< \beta >) = 1$. $\square$

Para $\sigma \in \text{Ass}(A)$, consideremos os seguintes subconjuntos de A :

$$\Gamma(\sigma) = \{\alpha \in A^* : \sigma(\alpha) = 1\}$$

$$Q(\sigma) = \{\alpha_1 + \dots + \alpha_r : \alpha_i \in \Gamma(\sigma)\}.$$

Lema 4.3 Seja $\sigma \in \text{Ass}(A)$. Então $Q(\sigma) \cap A^* = \Gamma(\sigma)$. Mais ainda, todo elemento de $Q(\sigma)$ é um elemento de $\Gamma(\sigma)$ ou soma de dois elementos de $\Gamma(\sigma)$.

Dem.: A igualdade $Q(\sigma) \cap A^* = \Gamma(\sigma)$ segue diretamente de (4.2). Agora, usando o fato que A é um anel local, para todo $x \in Q(\sigma)$ obtemos que $x \in Q(\sigma) \cap A^*$ ou $x \in Q(\sigma) \cap \mathcal{M}$, onde $\mathcal{M}$ é o ideal maximal de A . Se $x \in Q(\sigma) \cap A^*$, então $x \in \Gamma(\sigma)$. Caso contrário, $x = \alpha_1 + \dots + \alpha_r \in \mathcal{M}$, com $r > 1$, $\alpha_i \in A^*$ e

$\sigma(\langle \alpha_i \rangle) = 1$, para $1 \leq i \leq r$. Tomando $\alpha = \alpha_1 + \dots + \alpha_{r-1}$, $\beta = \alpha_r$, temos que $\alpha, \beta \in A^*$, pois $\alpha = x - \alpha_r$ e A é um anel local. Como $\sigma(\langle \alpha_1 \rangle) = \dots = \sigma(\langle \alpha_{r-1} \rangle) = 1$ segue de (4.2) que $\sigma(\langle \alpha \rangle) = 1$. Portanto, $x = \alpha \in \Gamma(\sigma)$ ou $x = \alpha + \beta$ com $\alpha, \beta \in \Gamma(\sigma)$. $\square$

Observação 4.4 Usando o fato de que σ é um homomorfismo de anéis, temos que para todo $x \in \Gamma(\sigma)$ o seu inverso $x^{-1} \in \Gamma(\sigma)$. Também é imediato que:

$$Q(\sigma) \cdot Q(\sigma) \subseteq Q(\sigma)$$

$$Q(\sigma) \cdot -Q(\sigma) \subseteq -Q(\sigma).$$

Proposição 4.5 *Seja $\sigma \in \text{Ass}(A)$. Então:*

(i) $Q(\sigma) \cap -Q(\sigma) = \emptyset$

(ii) *Se $x, y \in A$ e $x + y \in Q(\sigma)$, então $x \in Q(\sigma)$ ou $y \in Q(\sigma)$.*

(iii) $\mathcal{P} = A - (Q(\sigma) \cup -Q(\sigma))$ é um ideal primo de A .

Dem.: (i) Suponhamos que $Q(\sigma) \cap -Q(\sigma) \neq \emptyset$. Então existem $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s \in \Gamma(\sigma)$ tais que:

$$\alpha_1 + \dots + \alpha_r = -\beta_1 - \dots - \beta_s.$$

Se $\alpha_1 + \dots + \alpha_r \in A^*$, então $\sigma(\langle \alpha_1 + \dots + \alpha_r \rangle) = 1$ e $\beta_1 + \dots + \beta_s \in A^*$; logo, $\sigma(\langle \beta_1 + \dots + \beta_s \rangle) = 1$, por (4.1). Mas de (4.1) segue também que

$$1 = \sigma(\langle \alpha_1 + \dots + \alpha_r \rangle) = \sigma(\langle -(\beta_1 + \dots + \beta_s) \rangle) = -1,$$

pois $\sigma(\langle -1 \rangle) = -1$. Isto é uma contradição, pois $1 \neq -1$ em $\mathbb{Z}$.

Se $\alpha_1 + \dots + \alpha_r \in \mathcal{M}$, então $\alpha_1 + \dots + \alpha_{r-1} \in A^*$. Assim, $\alpha_1 + \dots + \alpha_{r-1} = -\alpha_r - \beta_1 - \dots - \beta_s$ com $\alpha_1 + \dots + \alpha_{r-1} \in A^*$, o que recai no caso acima. Portanto, $Q(\sigma) \cap -Q(\sigma) = \emptyset$.

(ii) Consideremos $x, y \in A$ com $x + y \in Q(\sigma)$. Então $x + y = \alpha_1 + \dots + \alpha_r$, com $\alpha_i \in \Gamma(\sigma)$, $1 \leq i \leq r$. Temos dois casos a analisar: se x ou y é uma unidade e se x e y são não-unidades.

Para analisarmos o primeiro caso, basta considerarmos $x \in A^*$, pois o caso $y \in A^*$ é análogo. Se $x \in A^*$, então $x \in \Gamma(\sigma)$ ou $-x \in \Gamma(\sigma)$. Se $x \in \Gamma(\sigma)$ é imediato que

$x \in Q(\sigma)$. Caso contrário, $y = -x + \alpha_1 + \cdots + \alpha_r \in Q(\sigma)$. Portanto, $x \in Q(\sigma)$ ou $y \in Q(\sigma)$.

Suponhamos, agora, que $x, y \in \mathcal{M}$, ou seja, x e y são não-unidades. Como $\alpha_1, \dots, \alpha_r \in A^*$ certamente $r \geq 2$. Assim, $x + (y - \alpha_1) = \alpha_2 + \cdots + \alpha_r$ e $y - \alpha_1 \in A^*$, pelo caso anterior temos que $x \in Q(\sigma)$ ou $y - \alpha_1 \in Q(\sigma)$. Como $\alpha_1 \in Q(\sigma)$, se $y - \alpha_1 \in Q(\sigma)$ então $y \in Q(\sigma)$. Portanto, em ambos os casos $x \in Q(\sigma)$ ou $y \in Q(\sigma)$.

(iii) Mostremos agora que $\mathcal{P} = A - (Q(\sigma) \cup -Q(\sigma))$ é um ideal primo de A . Pelo item (ii) se $x \notin Q(\sigma)$ e $y \notin Q(\sigma)$, então $x + y \notin Q(\sigma)$, analogamente para $-Q(\sigma)$. Logo, se $x, y \in \mathcal{P}$ então $x + y \in \mathcal{P}$. Da definição de $\mathcal{P}$ segue que $\mathcal{P} = -\mathcal{P}$. Portanto $\mathcal{P}$ é um subgrupo aditivo de A .

Consideremos $x \in A$ e $y \in \mathcal{P}$. Vamos mostrar que $xy \in \mathcal{P}$. Mas $A = Q(\sigma) \cup -Q(\sigma) \cup \mathcal{P}$; logo, $x \in Q(\sigma)$ ou $x \in -Q(\sigma)$ ou $x \in \mathcal{P}$.

Se $x \in Q(\sigma)$, segue de (4.3) que $x = \alpha \in \Gamma(\sigma)$ ou $x = \alpha + \beta$, com $\alpha, \beta \in \Gamma(\sigma)$. Suponhamos que $x \in \Gamma(\sigma)$, então $x^{-1} \in \Gamma(\sigma) \subseteq Q(\sigma)$. Assim $xy \in \mathcal{P}$, pois, caso contrário, $xy \in Q(\sigma) \cup -Q(\sigma)$ o que implica em $y \in Q(\sigma) \cup -Q(\sigma)$, que é uma contradição. Agora, se $x = \alpha + \beta$ com $\alpha, \beta \in \Gamma(\sigma)$, então $xy = \alpha y + \beta y$. Se $xy \in Q(\sigma)$, por (ii) temos que $\alpha y \in Q(\sigma)$ ou $\beta y \in Q(\sigma)$, ou seja, em ambos os casos $y \in Q(\sigma)$. Isto é uma contradição. De maneira análoga chegamos a uma contradição supondo $xy \in -Q(\sigma)$. Logo $xy \notin Q(\sigma) \cup -Q(\sigma)$, ou seja, $xy \in \mathcal{P}$.

Se $x \in -Q(\sigma)$, com técnicas análogas às usadas acima conclui-se que $xy \in \mathcal{P}$.

Se $x \in \mathcal{P}$, então $1 + x \in Q(\sigma)$, pois $\mathcal{P}$ é fechado para a adição e $1 + x \in -Q(\sigma)$, implica $x \in -Q(\sigma)$. Logo, $(1 + x)y \in \mathcal{P}$, conseqüentemente $xy = (1 + x)y - y \in \mathcal{P}$.

Assim, se $x \in A$ e $y \in \mathcal{P}$, então $xy \in \mathcal{P}$, o que nos permite concluir que $\mathcal{P}$ é um ideal de A . E mais, desde que $Q(\sigma) \cup -Q(\sigma)$ é fechado para a multiplicação, temos que se $x \notin \mathcal{P}$ e $y \notin \mathcal{P}$, então $xy \notin \mathcal{P}$. Portanto $\mathcal{P}$ é um ideal primo de A . $\square$

Corolário 4.6 *O conjunto $P(\sigma) = Q(\sigma) \cup \mathcal{P}$ é uma ordem de A com suporte $\mathcal{P}$.*

Dem.: As condições (ii),(iii),(iv) da definição (4.1) decorrem facilmente da Proposição (4.5). Para a condição (i) é suficiente provarmos que se $x \in \mathcal{P}$ e $y \in Q(\sigma)$ então $x + y \in Q(\sigma)$. Certamente $x + y \notin \mathcal{P}$, pois $\mathcal{P}$ é um ideal de A . Supondo $x + y \in -Q(\sigma)$, temos $x = (x + y) - y \in -Q(\sigma)$, o que é uma contradição. Portanto $x + y \in Q(\sigma)$. $\square$

Veremos a seguir que, na verdade, $P(\sigma)$ é uma ordem maximal de A .

Proposição 4.7 *Seja $\sigma \in \text{Ass}(A)$. Então $P(\sigma) = Q(\sigma) \cup \mathcal{P}$ é uma ordem maximal de A , ou seja, $P(\sigma) \in \mathcal{O}_m(A)$.*

Dem.: Suponhamos que exista $P \in \mathcal{O}(A)$, tal que $P(\sigma) \subseteq P$ e $P(\sigma) \neq P$. Logo, existe $x \in P - P(\sigma)$. Como $P(\sigma) = Q(\sigma) \cup \mathcal{P}$, temos que $x \in -Q(\sigma)$. De (4.3) segue que $x = -\alpha$ ou $x = -\alpha - \beta$, com $\alpha, \beta \in \Gamma(\sigma)$. Se $x = -\alpha \in -Q(\sigma) \subseteq -P(\sigma)$, então $x \in -P$, pois $-P(\sigma) \subseteq -P$. Logo, $x \in P \cap -P$, o que é uma contradição, pois $x \in A^*$. Se $x = -\alpha - \beta$, então $x + \alpha = -\beta \in -P(\sigma) \subseteq -P$. Por outro lado, $\alpha \in P(\sigma) \subseteq P$ e $x \in P$. Logo, $-\beta = x + \alpha \in P$, pois $P + P \subseteq P$. Assim, $-\beta \in P \cap -P$, o que é uma contradição, pois $-\beta \in A^*$. Portanto, $P(\sigma) = P$, ou seja, $P(\sigma) \in \mathcal{O}_m(A)$. $\square$

Construimos para cada assinatura σ de A , uma ordem maximal $P(\sigma)$ de A . Na verdade existe uma relação mais estrita entre os conjuntos $\text{Ass}(A)$ e $\mathcal{O}_m(A)$, conforme o teorema que segue.

Teorema 4.8 *Existe uma correspondência biunívoca entre o conjunto das assinaturas de A e o conjunto das ordens maximais de A .*

Dem.: Dada uma assinatura σ de A , de (4.7) temos que $P(\sigma) = Q(\sigma) \cup \mathcal{P}$ é uma ordem maximal de A . Reciprocamente, dada uma ordem maximal P de

A definimos uma assinatura σ_P de A , tal que para todo $\alpha \in A^*$:

$$\sigma_P(< \alpha >) = \begin{cases} 1 & \text{se } \alpha \in P \\ -1 & \text{se } \alpha \in -P \end{cases}$$

Assim estabelecemos uma correspondência entre $\text{Ass}(A)$ e $\mathcal{O}_m(A)$. Resta mostrarmos que esta correspondência é biunívoca, ou seja, que $\sigma_{P(\sigma)} = \sigma$ e $P(\sigma_P) = P$. Por definição, para todo $\alpha \in A^*$:

$$\sigma_{P(\sigma)}(< \alpha >) = \begin{cases} 1 & \text{se } \alpha \in P(\sigma) \\ -1 & \text{se } \alpha \in -P(\sigma) \end{cases}$$

Usando o fato de que α é uma unidade e $P(\sigma) \cap A^* = \Gamma(\sigma)$ verifica-se facilmente que $\sigma_{P(\sigma)}(< \alpha >) = \sigma(< \alpha >)$ para todo $\alpha \in A^*$. Portanto, $\sigma_{P(\sigma)} = \sigma$.

Seja $P \in \mathcal{O}_m(A)$. Queremos mostrar que $P(\sigma_P) = P$. Para tanto, basta mostrarmos que $P \subseteq P(\sigma_P)$. Tomemos $x \in P$. Se $x = \alpha \in A^*$, então $\sigma_P(< \alpha >) = 1$, ou seja, $x \in Q(\sigma_P) \subseteq P(\sigma_P)$. Se $x \notin A^*$, suponhamos, por absurdo, que $x \in -Q(\sigma_P)$. Então $x = -\alpha - \beta$, com $\alpha, \beta \in A^*$ e $\sigma_P(< \alpha >) = \sigma_P(< \beta >) = 1$. Logo, $x + \alpha = -\beta \in -Q(\sigma_P)$ e mais, $\sigma_P(< x + \alpha >) = \sigma_P(< -\beta >) = -1$. Assim $x + \alpha \in -P$. Conseqüentemente, $\alpha = (x + \alpha) - x \in -P$, ou seja, $\sigma_P(< \alpha >) = -1$, o que é uma contradição. Logo, $x \notin -Q(\sigma_P)$, o que implica que $x \in P(\sigma_P)$. Portanto, $P(\sigma_P) = P$. $\square$

Em (3.12) estabelecemos uma correspondência biunívoca entre o conjunto das assinaturas de um anel local A e o conjunto dos ideais primos minimais de $W(A)$. Deste fato e do teorema anterior decorre o resultado central desta dissertação.

Teorema 4.9 *Seja A um anel local. Existe uma correspondência biunívoca entre o conjunto dos ideais primos minimais de $W(A)$ e o conjunto das ordens maximais de A .*

Veremos agora que este resultado generaliza o teorema (3.1) de [8] provado por Teruo Kanzaki e Kazuo Kitamura. Segundo este teorema existe uma correspondência biunívoca entre o conjunto dos ideais primos minimais de

$W(A)$ é o conjunto das ordens das unidades de A (cf.4.10), onde A é um anel local com 2 inversível em A .

Definição 4.10 Um subconjunto $P \subseteq A^*$ é uma *ordem das unidades* se:

- (a) $P \cup -P = A^*$
- (b) $P \cap -P = \emptyset$
- (c) $P \cdot P \subseteq P$
- (d) $(P + P) \cap A^* \subseteq P$.

Na verdade, o conjunto das ordens das unidades está em correspondência biunívoca com o conjunto das ordens maximais de A . Isto decorre do próximo resultado.

Proposição 4.11 *Seja A um anel local. Então existe uma correspondência biunívoca entre o conjunto das ordens das unidades de A e o conjunto das assinaturas de A .*

Dem.: Dada P uma ordem das unidades de A , podemos definir uma assinatura σ_P , por:

$$\sigma_P(< \alpha >) = \begin{cases} 1 & \text{se } \alpha \in P \\ -1 & \text{se } \alpha \in -P \end{cases}$$

para todo $\alpha \in A^*$.

Por outro lado, dada $\sigma \in \text{Ass}(A)$, podemos definir a seguinte ordem das unidades:

$$P(\sigma) = \{\alpha \in A^* : \sigma(< \alpha >) = 1\}.$$

O conjunto $P(\sigma)$ satisfaz as quatro condições de (4.10). A quarta condição decorre de (4.3) e as demais são triviais. É fácil ver que $\sigma_{P(\sigma)} = \sigma$ e $P(\sigma_P) = P$. $\square$

Bibliografia

- [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, 1978.
- [3] CAVICHIA, M.C. , *Estudos de Relações entre um Corpo Formalmente Real e seu Anel de Witt* , Dissertação de Mestrado , IMECC-UNICAMP, 1989.
- [4] DIAS, I. , *Formas Quadráticas sobre LG-Anéis* , Tese de Doutorado , IMECC-UNICAMP , 1988.
- [5] FITZGERALD, R.W. , *Primary Ideals in Witt Rings* , Journal of Algebra 96, 368-385, 1985.
- [6] FITZGERALD, R.W. , *Ideal Class Groups of Witt Rings* , Journal of Algebra 124, 506-520, 1989.
- [7] HU, SZE-TSEN , *Introduction to Homological Algebra* , University of California , Los Angeles, 1968.
- [8] KANZAKI, T. e KITAMURA, K. , *On Prime Ideals of a Witt Ring over a Local Ring* , Osaka Journal Mathematics 9, 225-229, 1972
- [9] KNEBUSCH, M. e ROSENBERG, A. , *An Invitation to Real Spectra* , Lecture at Conference on Quadratic Forms , Hamilton, 1983.
- [10] KNEBUSCH, M. e ROSENBERG, A. , *Real Closures of Commutative Rings* , Journal für Mathematik, 1973.

- [11] KNEBUSCH, M. , *Symmetric Bilinear Forms over Algebraic Varieties* , Lecture at the Quadratic Forms Conference Queen's University, Kingston/Ontario, 107-179, 1976.
- [12] LAM, T.Y. , *The Algebraic Theory of Quadratic Forms* , University of California, 1973.