Ideais Primários em Anéis de Witt

Daniela Cristina Rebolho

Orientadora: *Profa. Dra. Ires Dias*

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Área: Matemática.

USP – São Carlos
Março de 2000

"À minha família."

Inicialmente agradeço À DEUS, pelo dom da vida e por ter me dado forças suficientes a fim de superar os obstáculos e conquistar meu objetivo. Agradeço a Profª. Drª. Ires Dias, pela sua dedicada e precisa orientação, e por sua amizade; a FAPESP pelo custeio parcial de meus estudos de Pós-Graduação; aos meus pais Dirceu e Maria, meu irmão Danilo e toda minha família que sempre me apoiaram e incentivaram; aos velhos e novos amigos, pelo apoio e companherismo, em especial as amigas Andréa, Luciene e Silvia e ao amigo Miguel; a todos meus professores da escola, da UNESP e da USP, pelos conhecimentos transmitidos; aos funcionários do ICMC e a todos que direta ou indiretamente contribuíram para o andamento e conclusão deste trabalho.

Resumo

Neste trabalho apresentamos generalizações dos resultados sobre ideais primários em anéis de Witt contidos em [05], para anéis de Witt de anéis semilocais.

Abstract

In this work we generalize the results about primary ideals in Witt rings contained in **[05]**, for Witt rings of semilocal rings.

Índice

Introdução

Desde seu nascimento (provavelmente na Babilonia) até 1936 o estudo de formas quadráticas era feito com formas sobre o corpo dos números reais, o corpo dos números complexos ou o anel dos inteiros. A fundamentação da teoria das formas quadráticas sobre um corpo genérico apareceu em um trabalho de Ernst Witt, em 1937, 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 corpo genérico de característica distinta de 2. Este conjunto, ele repartiu em classes de equivalências e construiu um objeto algébrico - o anel de Witt - que tornou-se o principal objeto de toda a teoria. Mas, demorou 30 anos para que fosse demonstrada a importância das idéias de Witt por Albrecht Pfister com seus teoremas de estruturas, criando assim a teoria "algébrica"das formas quadráticas. A partir daí, todo o estudo de classificação de formas quadráticas se resume ao estudo da estrutura do anel de Witt.

Em [08] e [09], Knebusch, Rosenberg e Ware apresentam resultados sobre a estrutura de anéis de Witt vistos como quocientes de anéis de grupos abelianos. Com tais resultados, obtemos a classificação dos ideais primos do anel de Witt das formas bilineares sobre um anel semilocal.

Em [05] Robert W. Fitzgerald apresenta, um estudo sobre os ideais primários do anel de Witt dos espaços bilineares sobre um corpo de característica distinta de 2. Usando as técnicas utilizadas em [08], [09] e também em [04], neste trabalho apresentamos o desenvolvimento de Fitzgerald para anéis de Witt dos espaços bilineares sobre um anel semilocal sem impormos condições sobre 2 ser ou não inversível em

tais anéis.

Para tanto, nos capítulos I e II, apresentamos alguns resultados de álgebra comutativa e noções básicas sobre espaços bilineares sobre anéis semilocais necessários à compreensão do restante do trabalho.

O capítulo III contém resultados sobre a estrutura do anel de Witt, $\mathcal{W}(A)$, dos espaços bilineares sobre um anel semilocal A. Mais precisamente, apresentamos a caracterização dos geradores de $\mathcal{W}(A)$ e dos ideais primos de $\mathcal{W}(A)$. Alguns resultados sobre assinaturas, os elementos nilpotentes e os elementos de torção de $\mathcal{W}(A)$ são também apresentados neste capítulo.

O capítulo IV, consiste do que nos propomos a desenvolver no projeto, ou seja, as generalizações dos resultados de Fitzgerald para o anel de Witt dos espaços bilineares sobre um anel semilocal A. Na primeira seção, usando a caracterização dos ideais primos de $\mathcal{W}(A)$, apresentamos a caracterização dos ideais $\mathcal{P}$-primários de $\mathcal{W}(A)$, para cada tipo de ideal primo $\mathcal{P}$ de $\mathcal{W}(A)$. A seção 2 contém resultados sobre decomposição primária em $\mathcal{W}(A)$ e, o principal deles, apresenta condições necessárias e suficientes sobre o anel semilocal A para que todo ideal de $\mathcal{W}(A)$ seja decomponível. Finalmente, na última seção apresentamos alguns resultados sobre os ideais de $\mathcal{W}(A)$ que não estão contidos no ideal fundamental $\mathcal{I}(A)$, ou seja, sobre os ideais que contém formas de dimensão ímpar.

Capítulo 1

Preliminares

Neste capítulo apresentaremos alguns fatos básicos de álgebra comutativa, bem como a introdução e algumas propriedades dos ideais primários, necessários para o desenvolvimento deste trabalho. Algumas demonstrações serão omitidas, as quais podem ser encontradas na literatura, como por exemplo em [**01**]. No que segue e nos demais capítulos, A denotará sempre um anel comutativo com elemento identidade 1. Indicaremos por $\mathrm{Spec}(A)$ o conjunto dos ideais primos de A, por $\mathrm{Spm}(A)$ o conjunto dos ideais maximais de A, por $\mathcal{J}(A)$ o radical de Jacobson de A e por A^* o grupo das unidades de A. Assumiremos, também que todo A-módulo será unitário e que todo homomorfismo de aneis leva elemento identidade em elemento identidade.

Os próximos resultados serão usados frequentemente no decorrer deste trabalho. O primeiro deles caracteriza $\mathcal{J}(A)$.

Proposição 1.1 *Um elemento $x \in A$ está em $\mathcal{J}(A)$ se, e somente se $1 - xy \in A^*$, para todo $y \in A$.*

Dem.: Ver **(1.9)** de [**01**]. ∎

Proposição 1.2 *Sejam $\mathfrak{I}$ um ideal de A contido em $\mathcal{J}(A)$ e $a \in A$. Então $\overline{a} = a + \mathfrak{I}$ é uma unidade em $A/\mathfrak{I}$ se, e somente se a é uma unidade em A.*

Dem.: Se a é uma unidade em A, então é imediato que $a+\mathfrak{I}$ é inversível em $A/\mathfrak{I}$. Reciprocamente, se $a+\mathfrak{I} \in (A/\mathfrak{I})^*$, então existe $b \in A$ tal que $(a+\mathfrak{I})(b+\mathfrak{I}) = 1+\mathfrak{I}$, ou seja, $1-ab \in \mathfrak{I} \subseteq \mathfrak{J}(A)$. De **(1.1)** temos $ab \in A^*$ e, consequentemente $a \in A^*$. ■

Para $\mathfrak{M} \in \operatorname{Spm}(A)$, denotaremos por $A_{\mathfrak{M}}$ a localização de A em $\mathfrak{M}$.

Proposição 1.3 *Seja $a \in A$. São equivalentes:*

(i) $a \in A^*$;

(ii) $\frac{a}{1} \in (A_{\mathfrak{M}})^*$, *para todo* $\mathfrak{M} \in \operatorname{Spm}(A)$;

(iii) $\overline{a} \neq \overline{0}$ *em* $(A/\mathfrak{M})^*$, *para todo* $\mathfrak{M} \in \operatorname{Spm}(A)$.

Dem.: Imediata. ■

Definição 1.4 Dizemos que um anel comutativo A, com elemento identidade 1 é um *anel semilocal* se $\operatorname{Spm}(A)$ é finito, ou seja, se A tem somente um número finito de ideais maximais.

Exemplo 1.5 Todo corpo é um anel semilocal, ou mais geralmente, todo produto direto finito de corpos é um anel semilocal. Da correspondência entre os ideais de A e os ideais do anel quociente, temos que toda imagem homomórfica de um anel semilocal é também semilocal. Mais ainda, se A é um anel semilocal, então $A_{\mathcal{P}}$ também o é, para todo $\mathcal{P} \in \operatorname{Spec}(A)$.

Proposição 1.6 *Sejam A um anel semilocal com* $\operatorname{Spm}(A) = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_r\}$. *Então*

$$\frac{A}{\mathfrak{J}(A)} \cong \frac{A}{\mathfrak{M}_1} \times \ldots \times \frac{A}{\mathfrak{M}_r},$$

onde $\cong$ denota isomorfismo de anéis.

Dem.: Segue diretamente de **(1.10)** de **[01]**. ■

Como, neste trabalho, apresentaremos um estudo dos ideais primários do anel de Witt dos espaços bilineares sobre um anel semilocal, achamos conveniente recordar o conceito e alguns resultados básicos sobre ideais primários de um anel comutativo. Tais resultados serão apresentados sem demonstrações as quais podem ser encontradas, por exemplo, em **[01]**.

Definição 1.7 Um ideal $\mathfrak{I}$ do anel A é dito ser um *ideal primário* se $\mathfrak{I} \neq A$ e se $xy \in \mathfrak{I}$, então $x \in \mathfrak{I}$ ou $y^n \in \mathfrak{I}$, para algum $n > 0$. Em outras palavras, $\mathfrak{I}$ é um ideal primário de A se, e somente se $A/\mathfrak{I} \neq 0$ e todo divisor de zero em $A/\mathfrak{I}$ é nilpotente.

Seja $\mathfrak{I}$ um ideal primário de A e $r(\mathfrak{I}) = \{x \in A;\ x^n \in \mathfrak{I}, \text{ para algum } n \geq 1\}$ o *radical* de $\mathfrak{I}$, o qual é um ideal primo. Se $r(\mathfrak{I}) = \mathcal{P} \in \mathrm{Spec}\,(A)$, dizemos que $\mathfrak{I}$ é um ideal $\mathcal{P}$-primário. Recordemos também que dados $\mathfrak{I}$ e $\mathcal{H}$ ideais de A, o ideal *quociente* de $\mathfrak{I}$ por $\mathcal{H}$ é o ideal de A, $(\mathfrak{I} : \mathcal{H}) = \{x \in A;\ x\mathcal{H} \subseteq \mathfrak{I}\}$.

Mais ainda, um ideal $\mathfrak{I}$ do anel A é dito ser *decomponível* se $\mathfrak{I}$ admite uma decomposição como uma intersecção finita de ideais primários. Todo ideal decomponível $\mathfrak{I}$ admite uma *decomposição primária reduzida*, ou seja,

$$\mathfrak{I} = \Omega_1 \cap \Omega_2 \cap \ldots \cap \Omega_n,$$

onde os ideais $\{\Omega_1, \ldots, \Omega_n\}$ satisfazem:

(i) Ω_i é primário, para cada $i = 1, \ldots, n$;

(ii) $r(\Omega_i) \neq r(\Omega_j)$, se $i \neq j$, $1 \leq i, j, \leq n$;

(iii) $\bigcap_{j \neq i} \Omega_j \not\subseteq \Omega_i$, para cada $i = 1, \ldots, n$.

Para cada ideal $\mathfrak{I}$ de A, um ideal primo $\mathcal{P}$ é dito ser um *divisor primo associado* de $\mathfrak{I}$ se $(\mathfrak{I} : Ax)$ é $\mathcal{P}$-primário, para algum $x \in A$. Denotamos por $Assoc\ (\mathfrak{I})$ o conjunto dos divisores primos associados de $\mathfrak{I}$.

Sobre a unicidade de decomposições primárias de ideais temos os seguintes resultados gerais:

Teorema 1.8 *Sejam $\mathfrak{I}$ um ideal decomponível de A e $\bigcap_{i=1}^{n} \Omega_i$ uma decomposição primária reduzida de $\mathfrak{I}$. Se $\mathcal{P}_i = r(\Omega_i)$, $1 \leq i \leq n$, então estes são precisamente os ideais primos que aparecem no conjunto de ideais $\{r(\mathfrak{I} : Ax);\ x \in A\}$ e, portanto, são independentes da particular decomposição de $\mathfrak{I}$.*

Dem.: Ver **(4.5)** de **[01]**. ■

Um conjunto $\sum \subseteq Assoc\ (\mathfrak{I})$ é dito ser um *conjunto isolado*, se $\sum$ satisfaz a seguinte condição: Se $\mathcal{P}$ é um ideal primo associado com $\mathfrak{I}$ e $\mathcal{P}' \subseteq \mathcal{P}$ para algum $\mathcal{P} \in \sum$, então $\mathcal{P}' \in \sum$.

Como um segundo teorema de unicidade de decomposições primárias temos:

Teorema 1.9 *Sejam $\mathfrak{I}$ um ideal decomponível de A, e $\bigcap_{i=1}^{n} \Omega_i$ uma decomposição primária reduzida de $\mathfrak{I}$, e $\{\mathcal{P}_{i_1}, \ldots, \mathcal{P}_{i_m}\} \subseteq Assoc\ (\mathfrak{I})$ um conjunto isolado. Então $\Omega_{i_1} \cap \ldots \cap \Omega_{i_m}$ é independente da decomposição.*

Dem.: Ver **(4.10)** de **[01]**. ■

Sejam A um anel e M um A-módulo. Para um ideal $\mathfrak{I}$ de A, denotamos por $M(\mathfrak{I})$ o $\frac{A}{\mathfrak{I}}$-módulo $M \otimes (\frac{A}{\mathfrak{I}}) \cong \frac{M}{\mathfrak{I}M}$, onde $\otimes$ denotará sempre $\otimes_A$. Para $\mathcal{P} \in \mathrm{Spec}\,(A)$, denotamos por $M_{\mathcal{P}}$ o $A_{\mathcal{P}}$-módulo $M \otimes A_{\mathcal{P}}$. Um A-módulo M é dito ser *livre* se M admite uma base, ou seja se existe um conjunto $\{x_i;\ i \in \Gamma\}$ de elementos de M, tais que $M \cong \bigoplus_{i \in \Gamma} A\,x_i$. Se, além disso, Γ é finito com m elementos, dizemos que M é livre de dimensão m e escrevemos $\dim(M) = m$.

Proposição 1.10 *Seja $A = F_1 \times \ldots \times F_r$ um produto direto finito de corpos. Se M é um A-módulo livre de dimensão m, então $M \cong M_1 \times \ldots \times M_r$ onde cada M_i é um F_i-espaço vetorial de dimensão m, para $i = 1, \ldots, r$.*

Dem.: Segue diretamente do fato que o produto cartesiano comuta com a soma direta. ∎

Proposição 1.11 *Sejam A um anel semilocal, $\mathfrak{I}$ um ideal de A com $\mathfrak{I} \subseteq \mathfrak{J}(A)$ e M um A-módulo. Se $\{x_1, \ldots, x_n\} \subseteq M$ são tais que $\{\overline{x_1}, \ldots, \overline{x_n}\}$ é uma base de $M(\mathfrak{I})$ sobre $A/\mathfrak{I}$, então $\{x_1, \ldots, x_n\}$ é uma base de M sobre A.*

Dem.: Seja $N = A\,x_1 + \ldots + A\,x_n \subseteq M$. Desde que $\{\overline{x_1}, \ldots, \overline{x_n}\}$ é uma base de $M(\mathfrak{I})$ sobre $A/\mathfrak{I}$ e $N(\mathfrak{I}) = (A/\mathfrak{I})\,\overline{x_1} + \ldots + (A/\mathfrak{I})\,\overline{x_n}$, temos que $M(\mathfrak{I}) = N(\mathfrak{I})$, ou seja, $M/\mathfrak{I}M = N/\mathfrak{I}N$. Assim $M = N + \mathfrak{I}M$ e, desde que $\mathfrak{I} \subseteq \mathfrak{J}(A)$, do Lema de Nakayama temos que $M = N$, ou seja $\{x_1, \ldots, x_n\}$ é um conjunto de geradores de M.

Se existe $i = 1, \ldots, n$ tal que $x_i \in A\,x_1 + \ldots + A\,x_{i-1} + A\,x_{i+1} + \ldots + A\,x_n$, então $\overline{x_i} \in (A/\mathfrak{I})\,\overline{x_1} + \ldots + (A/\mathfrak{I})\,\overline{x_{i-1}} + (A/\mathfrak{I})\,\overline{x_{i+1}} + \ldots + (A/\mathfrak{I})\,\overline{x_n}$, o que contradiz o fato de $\{\overline{x_1}, \ldots, \overline{x_n}\}$ ser uma base de $M(\mathfrak{I})$. Consequentemente, $\{x_1, \ldots, x_n\}$ é uma base de M sobre A, como queríamos. ∎

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 dita ser *exata em M_i* se $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. 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

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

cinde em M_i, se o submódulo $X = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$ 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 exata *cinde.*

Proposição 1.12 *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* $X \oplus Z$.

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 $X = \mathrm{Im}(f) = \mathrm{Ker}(g)$. Assim, desde que g é sobrejetor, temos

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

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. ■

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.

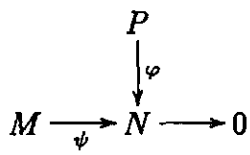
(b) Toda seqüência exata curta de A-módulos $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$, cinde.

(c) Para toda seqüência exata curta de A-módulos $0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$, a seqüência de A-módulos

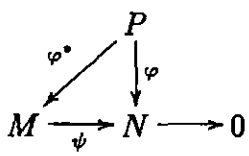
$$0 \longrightarrow \mathrm{Hom}(P, X) \longrightarrow \mathrm{Hom}(P, Y) \longrightarrow \mathrm{Hom}(P, Z) \longrightarrow 0$$

é exata.

(d) Para todo diagrama de A-módulos e A-homomorfismos



existe um levantamento de φ, $\varphi^* : P \longrightarrow M$, tal que o diagrama abaixo é comutativo, isto é, $\psi \circ \varphi^* = \varphi$.



Não apresentaremos aqui a demonstração das equivalências que caracterizam um A-módulo projetivo, pois fojem dos objetivos de nosso trabalho mas, esta caracterização é clássica e pode ser encontrada, por exemplo, em [12].

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

Se M é um A-módulo projetivo finitamente gerado, e $\mathfrak{M} \in \mathrm{Spm}(A)$, definimos o *posto de M módulo $\mathfrak{M}$*, como sendo a dimensão do $(A/\mathfrak{M})$-espaço vetorial $M(\mathfrak{M})$. Dizemos que M é um A-módulo projetivo finitamente gerado de *posto constante* se a aplicação $\rho : \mathrm{Spm}(A) \longrightarrow \mathbb{Z}$, definida por $\rho(\mathfrak{M}) = \dim_{A/\mathfrak{M}} M(\mathfrak{M})$ é constante.

A teoria algébrica das formas bilineares sobre anéis é desenvolvida na categoria dos módulos projetivos finitamente gerados e de posto constante. Finalizaremos este capítulo mostrando que, sobre anéis semilocais, esta categoria coincide com a categoria dos módulos livres de dimensão finita. Para tanto, usaremos o seguinte resultado auxiliar.

Lema 1.13 *Sejam P um A-módulo projetivo finitamente gerado e $\mathfrak{I} \subseteq \mathfrak{J}(A)$ um ideal de A. Se $P(\mathfrak{I})$ é um $(A/\mathfrak{I})$-módulo livre, então P é um A-módulo livre.*

Dem.: Desde que $P(\mathfrak{I})$ é um $(A/\mathfrak{I})$-módulo livre e P é finitamente gerado, então existe $m \in \mathbb{N}$ tal que $P(\mathfrak{I}) \cong (A/\mathfrak{I})^m$. Considerando as sobrejeções naturais de P em $P(\mathfrak{I})$ e de A^m em $(A/\mathfrak{I})^m$, temos o seguinte diagrama de A-módulos.

$$\begin{array}{ccc} P & & A^m \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ P(\mathfrak{I}) & \xrightarrow{\overline{\varphi}} & \left(\dfrac{A}{\mathfrak{I}}\right)^m \end{array}$$

onde π denota as sobrejeções naturais e $\overline{\varphi}$ é um isomorfismo de $(A/\mathfrak{I})$-módulos e, portanto, de A-módulos. Temos então o diagrama

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \overline{\varphi}\circ\pi} & & \\ A^m & \xrightarrow{\pi} & \left(\dfrac{A}{\mathfrak{I}}\right)^m & \longrightarrow & 0 \end{array}$$

e, desde que P é projetivo, temos que existe $\varphi : P \longrightarrow A^m$ tal que o diagrama abaixo é comutativo

$$\begin{array}{ccc} P & \xrightarrow{\varphi} & A^m \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ P(\mathfrak{I}) & \xrightarrow{\overline{\varphi}} & \left(\dfrac{A}{\mathfrak{I}}\right)^m \end{array}$$

Agora, é suficiente mostrarmos que φ é um isomorfismo. Desde que $\pi \circ \varphi = \overline{\varphi} \circ \pi$ é sobrejetor, temos que $\pi(\mathrm{Im}\,(\varphi)) = (A/\mathfrak{I})^m$, ou seja, $\mathrm{Im}\,(\varphi) + \mathfrak{I}A^m = A^m$. Como $\mathfrak{I} \subseteq \mathfrak{J}(A)$, do Lema de Nakayama temos que $\mathrm{Im}\,(\varphi) = A^m$, isto é, φ é sobrejetor. Logo temos a seqüência exata $0 \longrightarrow \mathrm{Ker}\,(\varphi) \longrightarrow P \longrightarrow A^m \longrightarrow 0$. Mas, A^m é um A-módulo livre e, portanto projetivo, o que implica que $P \cong \mathrm{Ker}\,(\varphi) \oplus A^m$. Assim $\mathrm{Ker}\,(\varphi)$ é um A-módulo finitamente gerado tal que $\dfrac{\mathrm{Ker}\,(\varphi)}{\mathfrak{I}\,\mathrm{Ker}\,(\varphi)} = \mathrm{Ker}\,(\overline{\varphi}) = \{0\}$, pois $\overline{\varphi}$ é injetor.

Portanto $\mathrm{Ker}\,(\varphi) \cong \mathfrak{I}\,\mathrm{Ker}\,(\varphi)$ e, novamente pelo Lema de Nakayama, temos que $\mathrm{Ker}\,(\varphi) = \{0\}$, o que completa a demonstração. ■

No que segue, exceto menção em contrário, A denotará um anel semilocal, $\mathrm{Spm}(A) = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_r\}$ o conjunto do todos os ideais maximais de A, e todos os módulos considerados serão A-módulos.

Teorema 1.14 *Todo módulo projetivo finitamente gerado e de posto constante sobre um anel semilocal é livre.*

Dem.: Seja P um módulo projetivo finitamente gerado e de posto constante sobre A, com $n = \rho(P)$, ou seja, $n = \dim_{A/\mathfrak{M}_i}(P(\mathfrak{M}_i))$, para qualquer $\mathfrak{M}_i \in \mathrm{Spm}(A)$. Para $\overline{P} = \dfrac{P}{\mathcal{J}(A)\,P}$, temos

$$\overline{P} \cong \frac{P}{\mathfrak{M}_1\,P} \oplus \ldots \oplus \frac{P}{\mathfrak{M}_r\,P} \cong \left(\frac{A}{\mathfrak{M}_1}\right)^n \oplus \ldots \oplus \left(\frac{A}{\mathfrak{M}_r}\right)^n \cong \left(\frac{A}{\mathfrak{M}_1} \times \ldots \times \frac{A}{\mathfrak{M}_r}\right)^n.$$

Logo $\overline{P}$ é um $\overline{A} = (A/\mathcal{J}(A))$-módulo livre de dimensão n e, do lema anterior, segue que P é um A-módulo livre. ■

Capítulo 2

Espaços Bilineares

Neste capítulo apresentaremos a noção e alguns resultados básicos da teoria das formas bilineares sobre um anel semilocal A. Alguns destes resultados valem mais geral para um anel comutativo com elemento identidade.

Em geral, a teoria das formas bilineares sobre um anel A, é feita na categoria dos A-módulos projetivos finitamente gerados e de posto constante. Como os principais resultados apresentados neste trabalho são sobre espaços bilineares sobre aneis semilocais e, de **(1.14)** temos que, neste caso, todo módulo projetivo finitamente gerado e de posto constante é livre, por conveniência de redação, trabalharemos desde o início com a categoria dos A-módulos livres de dimensão finita. Denotaremos tal categoria por $\mathcal{L}(A)$. Exceto quando mencionado o contrário, $\otimes$ significará sempre $\otimes_A$. Para cada $M \in \mathcal{L}(A)$, denotaremos por M^* o A-módulo dual $\mathrm{Hom}_A(M, A) \in \mathcal{L}(A)$.

2.1 Definições

Definição 2.1 O par (M, b) consistindo de um módulo $M \in \mathcal{L}(A)$ e de uma forma bilinear simétrica $b : M \times M \to A$ é dito ser um *módulo bilinear* sobre A. O módulo bilinear (M, b) é *não singular*, ou simplesmente e um *espaço bilinear*, se a função A-linear $d_b : M \to M^*$, definida por $d_b(x) = b(x, \quad)$, para todo $x \in M$, é um isomor-

fismo de A-módulos. A função d_b é chamada *a adjunta da forma bilinear* b. Se o A-módulo M tem dimensão n, dizemos que o espaço bilinear (M, b) tem dimensão n e indicamos por $\dim(M, b) = n$, ou simplesmente por $\dim(M) = n$, ou ainda $\dim(b) = n$. Uma *isometria* entre dois módulos bilineares (M_1, b_1) e (M_2, b_2) é um isomorfismo de A-módulos $\varphi : M_1 \to M_2$, 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 $\{x_1, \cdots, x_n\}$ é uma base de M, então a forma bilinear b é determinada pela matriz quadrada $(b_{ij}) = (b(x_i, x_j))$, $1 \leq i, j \leq n$, pois para $x = \sum_{i=1}^{n} \alpha_i x_i$ e $y = \sum_{j=1}^{n} \beta_j x_j$ em M, temos $b(x, y) = \sum_{i,j=1}^{n} b_{ij} \alpha_i \beta_j$. Reciprocamente, para cada matriz simétrica $n \times n$, (b_{ij}) sobre A 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.

Chamaremos de determinante do espaço bilinear b e denotaremos por $\det(b)$ o determinante da matriz (b_{ij}). 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.

Denotamos a categoria dos espaços bilineares sobre A por $\mathcal{B}il(A)$, onde os morfismos desta categoria são as isometrias. Em $\mathcal{B}il(A)$ definimos duas operações, uma soma e um produto.

Definição 2.2 Definimos a *soma ortogonal* dos espaços $(M_i, b_i) \in \mathcal{B}il(A)$, 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 $(b_1 \perp b_2)(x_1 + x_2, y_1 + y_2) = b_1(x_1, y_1) + b_2(x_2, y_2)$, 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 $b_1 \perp b_2$, ou ainda $M_1 \perp M_2$.

Definição 2.3 Definimos o *produto tensorial* dos espaços $(M_i, b_i) \in \mathcal{B}il(A)$, $i = 1, 2$, 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, $y_i \in M_i$. 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 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 2.4 Sejam $M = Ax$ e $\alpha \in A$. A forma bilinear $b : M \times M \to A$ definida por $b(\gamma x, \beta x) = \gamma \beta\, b(x, x) = \gamma \beta\, \alpha$, para todo γ, $\beta \in A$, é não singular se, e somente se $\alpha \in A^*$. Denotaremos esta forma bilinear, simplesmente por $\langle \alpha \rangle$. Mais geralmente, a forma bilinear $b = \langle \alpha_1 \rangle \perp \ldots \perp \langle \alpha_n \rangle$ será denotada por $b = \langle \alpha_1, \ldots, \alpha_n \rangle$ e, neste caso, b é não singular se, e somente se $\alpha_1\, \alpha_2 \ldots \alpha_n \in A^*$.

Sejam $M = Ax \oplus Ay$ e α, $\beta \in A$. Definimos uma forma A-bilinear $b : M \times M \to A$ por $b(x, x) = \alpha$, $b(y, y) = \beta$ e $b(x, y) = 1$. Esta forma bilinear é denotada por $b = \begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$ e, b é não singular se, e somente se $1 - \alpha\beta \in A^*$.

2.2 Extensão de escalares

Sejam $\varphi : A \longrightarrow A'$ um homomorfismo de anéis e $(M, b) \in \mathcal{B}il(A)$. É facil ver que se $\{x_1, x_2, \ldots, x_n\}$ é uma base de M sobre A, então $\{x_1 \otimes 1, x_2 \otimes 1, \ldots, x_n \otimes 1\}$ é

uma base de $M \otimes A'$ sobre A', ou seja, $M \otimes A' \in \mathcal{L}(A')$. Sobre tal A'-módulo difinimos uma forma bilinear simétrica $b' = b \otimes A'$ por $b'(x \otimes \alpha, y \otimes \beta) = \varphi(b(x,y))\,\alpha\,\beta$ para todo $x,\ y \in M$ e $\alpha,\ \beta \in A$. Agora, se $(b_{ij}) = (b(x_i, x_j))$ é a matriz associada ao espaço bilinear (M,b), então, em relação à base $\{x_1 \otimes 1, \ldots, x_n \otimes 1\}$ de $M \otimes A'$, o módulo bilinear $(M \otimes A', b')$ tem a matriz associada $(b'_{ij}) = (b'(x_i \otimes 1, x_j \otimes 1)) = (b(x_i, x_j)) = (b_{ij})$, o que mostra que b' é também não singular. O espaço bilinear $(M \otimes A', b \otimes A')$ de $\mathcal{B}il(A')$ é dito ser o espaço obtido de (M,b) por *estensão de escalares.*

Em particular, para $\mathfrak{M}$ um ideal maximal de A, seja $\varphi : A \longrightarrow A_{\mathfrak{M}}$ o homomorfismo canônico $\varphi(\alpha) = \dfrac{\alpha}{1}$, para todo $\alpha \in A$. Dado $(M,b) \in \mathcal{B}il(A)$, temos que $M \otimes A_{\mathfrak{M}} \cong M_{\mathfrak{M}}$ e, $b_{\mathfrak{M}} = b \otimes A_{\mathfrak{M}}$ é dada por $b_{\mathfrak{M}}\left(\dfrac{x}{\alpha}, \dfrac{y}{\beta}\right) = \dfrac{b(x,y)}{\alpha\,\beta}$, para todo $x,\ y \in M$ e $\alpha,\ \beta \in A - \mathfrak{M}$. O espaço bilinear $(M_{\mathfrak{M}}, b_{\mathfrak{M}})$ é chamado a *localização de* (M,b) *em* $\mathfrak{M}$.

Para um ideal $\mathfrak{I}$ qualquer de A, considerando a projeção canônica $\varphi : A \longrightarrow A/\mathfrak{I}$, temos que para todo espaço bilinear $(M,b) \in \mathcal{B}il(A)$ $\varphi^*(M,b) = (M(\mathfrak{I}), b(\mathfrak{I}))$ é um elemento de $\mathcal{B}il(A/\mathfrak{I})$, onde $M(\mathfrak{I}) = M \otimes (A/\mathfrak{I}) \cong M/\mathfrak{I}M$ e $b(\mathfrak{I})(\overline{x}, \overline{y}) = \varphi(b(x,y)) = \overline{b(x,y)}$, para todo $\overline{x},\ \overline{y} \in M/\mathfrak{I}M$. O espaço $(M(\mathfrak{I}), b(\mathfrak{I}))$ é chamado a *redução módulo* $\mathfrak{I}$ *de* (M,b).

Com esta noção de redução e localização para módulos bilineares temos

Proposição 2.5 *Seja* (M,b) *um módulo bilinear sobre* A. *São equivalentes:*

(i) (M,b) *é não singular;*

(ii) $(M_{\mathfrak{M}}, b_{\mathfrak{M}})$ *é não singular, para todo* $\mathfrak{M} \in \mathrm{Spm}(A)$;

(iii) $(M(\mathfrak{M}), b(\mathfrak{M}))$ *é não singular, para todo* $\mathfrak{M} \in \mathrm{Spm}(A)$.

Dem.: Basta observarmos que dada uma base $\{x_1, \ldots, x_n\}$ de M, temos que $\left\{\dfrac{x_1}{1}, \ldots, \dfrac{x_n}{1}\right\}$ é uma base de $M_{\mathfrak{M}}$ sobre $A_{\mathfrak{M}}$ e que $\{x_1 + M(\mathfrak{M}), \ldots, x_n + M(\mathfrak{M})\}$ é uma base de $M(\mathfrak{M})$ sobre $A/\mathfrak{M}$. Agora, a demostração da proposição segue de **(1.3)** e da definição de não singularidade. ■

Outra forma de redução que usaremos no decorrer do trabalho é quando $A = F_1 \times \ldots \times F_r$ é um produto finito de corpos e, (M, b) um módulo bilinear sobre A. Neste caso, para cada $i = 1, \ldots, r$ a i-ésima projeção canônica $\pi_i : A \longrightarrow F_i$ induz uma redução $\pi_i^*(M, b) = (M_i, b_i)$, onde $b_i = \pi_i \circ b$. De **(1.10)** temos que $M \cong M_1 \times \ldots \times M_r$ e, $\pi = (\pi_1, \ldots, \pi_r)$ induz a redução

$$\pi^*(M, b) = (M_1, b_1) \times \ldots \times (M_r, b_r),$$

onde $b = \pi^*(b) = (\pi_1 \circ b, \ldots, \pi_r \circ b) = (b_1, \ldots, b_r)$. Com estas notações temos:

Proposição 2.6 *Se $A = F_1 \times \ldots \times F_r$ e (M, b) é um módulo bilinear sobre A com $M = M_1 \times \ldots \times M_r$, então $b = (b_1, \ldots, b_r)$ e (M, b) é não singular se, e somente se (M_i, b_i) é não singular, para cada $i = 1, \ldots, n$.*

Dem.: Basta observar que a adjunta de b, $d_b = (d_{b_1}, \ldots, d_{b_r})$ e, consequentemente, d_b é um isomorfismo se, e somente se cada d_{b_i} o é, para $i = 1, \ldots, r$. ■

2.3 Subespaços

Seja (M, b) um módulo bilinear sobre um anel A. Para cada subconjunto U de M, o conjunto

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

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 2.7 *Sejam (M, b) um módulo bilinear sobre A e U, V subconjuntos de M.*

(i) *Se $V \subseteq U$, então $U^{\perp} \subseteq V^{\perp}$;*

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

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

Dem.: Imediata. ∎

Um submódulo U de M é dito ser um *subespaço* de (M, b) se U é um somando direto de M. Dizemos que x é um *elemento primitivo* de M se Ax é um subespaço de M.

Se U e V são submódulos de M tais que $M = U \oplus V$ 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 subespaço U de 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 é um subespaço totalmente isotrópico de M, ou seja, x é um elemento primitivo de M tal que $b(x, x) = 0$. Um elemento $y \in M$ é dito ser *anisotrópico* se Ay é um subespaço de M com $b(y, y) \in A^*$. 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.*

Proposição 2.8 *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.: Se (M, b) é não singular e U é um subespaço de M, então existe um submódulo V de M tal que $M = U \oplus V$. Assim, $M^* = (U \oplus V)^* \cong U^* \oplus V^*$ e, temos a seqüência

exata $M^* \longrightarrow U^* \longrightarrow 0$. Como (M, b) é um espaço bilinear não singular, temos que a adjunta de b, $d : M \to M^*$ é um isomorfismo. Compondo este isomorfismo com a seqüência acima, obtemos a seqüência exata $M \longrightarrow U^* \longrightarrow 0$, onde o núcleo da composta $d : M \to U^*$ 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 da forma bilinear b a subespaços de M. O isomorfismo $d : \frac{M}{U^\perp} \to U^*$ induz uma forma bilinear não singular $b : U \times \frac{M}{U^\perp} \longrightarrow A$, para todo subespaço U de M, onde $b(x, \overline{y}) = d(\overline{y})(x)$ para todo $x \in U$ e $\overline{y} \in (M/U^\perp)$. Em particular, para o subespaço $U^\perp$ temos uma forma bilinear não singular $b : U^\perp \times \frac{M}{U^{\perp\perp}} \longrightarrow A$. Por outro lado, temos o isomorfismo $M \cong (U^\perp)^* \oplus U$ que decorre dos isomorfismos

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

Assim obtemos o isomorfismo $d : \frac{M}{U} \longrightarrow (U^\perp)^*$ que induz uma forma bilinear não singular $b : U^\perp \times \frac{M}{U} \longrightarrow A$. Destas duas bilineares e do fato que $U \subseteq U^{\perp\perp}$, segue que $U = U^{\perp\perp}$. Pois se $U \subsetneq U^{\perp\perp}$, então existe $y \in U^{\perp\perp} - U$ e, das duas formas bilineares obtidas, temos $\frac{M}{U} \simeq (U^\perp)^* \simeq \frac{M}{U^{\perp\perp}}$. Como $y \in U^{\perp\perp}$, então para todo $x \in U^\perp$, $d(y)(x) = b(x, y) = 0$. Por outro lado, como $y \notin U$, temos que $d(y) \neq 0$. Assim existe $z \in U^\perp$ tal que $d(y)(z) \neq 0$, ou seja, $b(z, y) \neq 0$, o que é uma contradição. Portanto $U = U^{\perp\perp}$, o que mostra (i).

Seja agora, $(U, b|_U)$ um subespaço não singular de (M, b). Então $d : U \to U^*$ é um isomorfismo. Mas, cada elemento $x \in M$ define um elemento x^* em U^* por $x^*(y) = b(x, y) = d(x)(y)$, para todo $y \in U$. Como $d : U \to U^*$ é sobrejetora, temos que existe $z \in U$ tal que $d(z) = d(x)$, ou seja, $b(z, y) = b(x, y)$, para todo $y \in U$. Logo $b(x, y) - b(z, y) = 0$, o que implica que $b(x - z, y) = 0$, para todo $u \in U$. Assim

$x - z \in U^{\perp}$ e, como $x = z + (x - z)$, temos que $M = U + U^{\perp}$. Do fato de $d : U \to U^*$ ser injetora segue que $\{0\} = \mathrm{Ker}\,(d|_U) = \mathrm{Ker}\,(d) \cap U = U^{\perp} \cap U$, o que mostra que $M = U \oplus U^{\perp}$ e, juntamente com o fato que $U \subseteq U^{\perp\perp}$ temos o item (ii). ■

Corolário 2.9 *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.: Da 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. ■

Corolário 2.10 *Sejam (M, b) um módulo bilinear sobre A e $\mathfrak{I}$ um ideal contido no radical de Jacobson $\mathfrak{J}(A)$ de A. Se $(M(\mathfrak{I}), b(\mathfrak{I}))$ admite uma decomposição ortogonal $M(\mathfrak{I}) = N(\mathfrak{I}) \perp W(\mathfrak{I})$, com $N(\mathfrak{I})$ livre sobre $A/\mathfrak{I}$ tal que $(N(\mathfrak{I}), b(\mathfrak{I}))$ é não singular, então existe uma decomposição ortogonal $M = N \perp W$ de (M, b) com N livre sobre A e (N, b) não singular tal que $N(\mathfrak{I}) = \dfrac{N}{\mathfrak{I}N}$ e $W(\mathfrak{I}) = \dfrac{W}{\mathfrak{I}W}$.*

Dem.: Desde que $(N(\mathfrak{I}), b(\mathfrak{I}))$ é um subespaço não singular de $(M(\mathfrak{I}), b(\mathfrak{I}))$ com $N(\mathfrak{I})$ livre sobre $A/\mathfrak{I}$, temos que existe uma base $\{\overline{x_1}, \ldots, \overline{x_n}\}$ de $N(\mathfrak{I})$ sobre $A/\mathfrak{I}$ tal que $\det(b(\mathfrak{I})(\overline{x_i}, \overline{x_j})) \in (A/\mathfrak{I})^*$. Da proposição **(1.11)** temos que $N = Ax_1 + \ldots + Ax_n$ é um A-módulo livre com base $\{x_i, \ldots, x_n\}$ e $N(\mathfrak{I}) = \dfrac{N}{\mathfrak{I}N}$. A matriz da forma bilinear $b\,|_N$, $(b(x_i, x_j))$, é tal que $\overline{\det(b(x_i, x_j))} = \det(\overline{b(x_i, x_j)}) = \det(b(\mathfrak{I})(\overline{x_i}, \overline{x_j})) \in (A/\mathfrak{I})^*$. Agora segue de **(1.2)** e da definição **(2.1)** que (N, b) é um subespaço não singular de M, e o resultado segue de **(2.8)**. ■

Finalizaremos esta seção mostrando que todo espaço bilinear sobre um anel semilocal admite uma decomposição como soma ortogonal de subespaços de dimensão ≤ 2.

Para tanto, iniciaremos com algumas definições e resultados auxiliares.

No que segue, usaremos as notações $\overline{A}$ para indicarmos o anel $A/\mathcal{J}(A)$ e $(\overline{M},\overline{b})$ para indicarmos a redução módulo $\mathcal{J}(A)$ do espaço bilinear $(M,b) \in \mathcal{B}il(A)$.

Dado $(M,b) \in \mathcal{B}il(A)$, 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*.

Segue imediatamente desta definição e de **(1.2)** que

Lema 2.11 *Sejam A um anel semilocal e $(M,b) \in \mathcal{B}il(A)$. Então (M,b) é um espaço bilinear próprio se, e somente se $(\overline{M},\overline{b})$ é um espaço bilinear próprio sobre $\overline{A}$.*

Dem.: Imediata. ■

Agora, se $A = F_1 \times \ldots \times F_r$ é um produto finito de corpos e $(M,b) \in \mathcal{B}il(A)$, da proposição **(2.6)**, temos que $(M,b) = (M_1,b_1) \times \ldots \times (M_r,b_r)$, com $(M_i,b_i) \in \mathcal{B}il(F_i)$ e $b_i = \pi_i \circ b$, para cada $i = 1, \ldots, r$. Neste caso temos

Lema 2.12 *O espaço bilinear (M,b) é próprio se, e somente se (M_i,b_i) é próprio, para cada $i = 1, \ldots, r$.*

Dem.: Basta observar que se $\mathfrak{I}$ é o ideal de A gerado por $\{b(x,x);\ x \in M\}$ e, para cada $j = 1, \ldots, r$, $\mathfrak{I}_j$ é o ideal de F_j, gerado por $\{b_j(x_j,x_j);\ x_j \in M_j\}$, então $\mathfrak{I} = \mathfrak{I}_1 \times \ldots \times \mathfrak{I}_r$. Assim, $\mathfrak{I} = A$ se, e somente se $\mathfrak{I}_j = F_j$, para cada $j = 1, \ldots, r$. ■

No caso em que A é um anel semilocal, temos o seguinte teorema de decomposição para espaços bilineares

Teorema 2.13 *Seja (M,b) um espaço bilinear sobre um anel semilocal A.*

(i) *Se (M,b) é próprio, então (M,b) é uma soma ortogonal de subespaços de dimensão 1, isto é, M admite uma base ortogonal em relação à forma bilinear b.*

(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* $\alpha,\ \beta \in A$ *tais que* $1-\alpha\beta \in A^*$.

Dem.: Dos lemas **(2.11)** e **(2.12)**, é suficiente mostrarmos o teorema para $(\overline{M},\overline{b})$ sobre $\overline{A} = A/\mathcal{J}(A)$. Podemos então assumir que $\mathcal{J}(A) = \{0\}$, ou seja, que $A = F_1 \times \ldots \times F_r$ é um produto finito de corpos e, consequentemente $M = M_1 \times \ldots \times M_r$ com $b = (b_1, \ldots, b_r)$. Também, usando indução sobre r, é suficiente mostrarmos o caso em que $r = 2$.

Seja $(M,b) = (M_1,b_1) \times (M_2,b_2) \in \mathcal{B}il(A)$, onde $A = F_1 \times F_2$, com $F_1,\ F_2$ corpos. Faremos agora a demonstração por indução sobre $\dim(M)$. Se $\dim(M) = 1$, nada há a demonstrar. Se $\dim(M) > 1$ e (M,b) é próprio então de **(2.12)** temos que (M_i,b_i) é um espaço bilinear próprio sobre o corpo F_i, para cada $i = 1,\ 2$. Como o ideal gerado por $\{b_i(x_i,x_i);\ x_i \in M_i\}$ é F_i, para cada $i = 1,\ 2$, temos que existem $x_1 \in M_1,\ x_2 \in M_2$ tais que $b_1(x_1,x_1) \neq 0$ e $b_2(x_2,x_2) \neq 0$. Assim, $x = (x_1,x_2) \in M$ é tal que $b(x,x) = (b_1(x_1,x_1), b_2(x_2,x_2)) \in A^* = F_1^* \times F_2^*$ e, consequentemente, (Ax,b) é um subespaço não singular de dimensão 1 de (M,b). De **(2.8)** temos que $(M,b) = (Ax,b) \perp (W,b)$, com $W = (Ax)^{\perp}$. Se (W,b) é próprio, então por hipótese de indução (W,b) é uma soma ortogonal de subespaços de dimensão 1 e, portanto, (M,b) também o é.

Se (W,b) é impróprio, desde que $(W,b) = (W_1,b_1) \times (W_2,b_2)$, temos de **(2.12)** que (W_1,b_1) é impróprio ou (W_2,b_2) é impróprio. Temos dois casos a considerar:

Caso 1 - Se (W_i,b_i) é impróprio para $i = 1,\ 2$. Neste caso, desde que (W,b) é não singular, existem $y = (y_1,y_2),\ \ z = (z_1,z_2) \in W$ tais que $b_i(y_i,z_i) \neq 0$ em F_i, $i = 1,\ 2$. Consequentemente, $b(y,z) \in A^*$. Tomando $w_1 = x + y$ e $w_2 = x + \lambda z$, com $\lambda = -\dfrac{b(x,x)}{b(y,z)} \in A$, temos que $(Aw_1 + Aw_2, b)$ é um subespaço não singular de (M,b), pois $(b(w_i,w_j)) = \begin{pmatrix} b(w_1,w_1) & b(w_1,w_2) \\ b(w_2,w_1) & b(w_2,w_2) \end{pmatrix} = \begin{pmatrix} b(x,x) & 0 \\ 0 & b(x,x) \end{pmatrix}$. Mais

ainda, $\{w_1, w_2\}$ é uma base ortogonal deste subespaço. Assim, de **(2.8)**

$$(M, b) = (A\,w_1, b) \perp (A\,w_2, b) \perp (N, b)$$

com $(A\,w_2, b) \perp (N, b)$ próprio que, por hipótese de indução, admite uma base ortogonal. Juntando esta base com w_1, formamos uma base ortogonal de (M, b).

Caso 2 - Se um dos espaços (W_i, b_i) é próprio, renomeando se necessário, podemos assumir que (W_1, b_1) é impróprio e (W_2, b_2) é próprio. Então, neste caso, existem y_1, $z_1 \in W_1$, $y_1 \neq z_1$, e $y_2 \in W_2$ tais que $b_1(y_1, z_1) \neq 0$ em F_1 e $b_2(y_2, y_2) \neq 0$ em F_2. Agora, os elementos $w_1 = (x_1 + y_1,\, x_2)$ e $w_2 = (x_1 + \lambda\, z_1,\, y_2)$ de M com $\lambda = -\dfrac{b(x_1, x_1)}{b(y_1, z_1)} \in F_1^*$, são tais que

$$(b(w_i, w_j)) = \begin{pmatrix} (b_1(x_1, x_1), b_2(x_2, x_2)) & (0,0) \\ (0,0) & (b_1(x_1, x_1), b_2(y_2, y_2)) \end{pmatrix},$$

ou seja $\{w_1, w_2\}$ é uma base ortogonal de um subespaço não singular de (M, b) e, como no **Caso 1**, temos que (M, b) admite uma base ortogonal. Com isso, completamos a demostração do item **(i)** do teorema.

Consideremos agora que $\dim(M) > 1$ e que $(M, b) = (M_1, b_1) \times (M_2, b_2)$ é um espaço bilinear impróprio sobre $A = F_1 \times F_2$. De **(2.12)** temos que (M_1, b_1) é impróprio ou (M_2, b_2) é impróprio. Novamente temos dois casos a considerar:

Caso 1 - Se (M_i, b_i) é impróprio para $i = 1, 2$. Neste caso, como no **Caso 1** acima, existem y, $z \in M$, $y \neq z$, tais que $b(y, z) \in A^*$. O conjunto $\{y, z\}$ forma uma base de um subespaço não singular de (M, b), pois a matriz da forma bilinear b em relação à estes elementos é

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

que tem determinante inversível em A. Logo, mostramos que (M, b) admite um subespaço não singular de dimensão 2. Trocando z por $\lambda\, z$, com $\lambda = \dfrac{1}{b(y, z)}$, temos que

(M,b) admite um subespaço não singular da forma $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$, com $1-\alpha\beta = 1 \in A^*$.

Caso 2 - Se um dos espaços (M_i, b_i) é próprio. Sem perda de generalidade, podemos supor que (M_1, b_1) é impróprio e (M_2, b_2) é próprio. Como no **Caso 2** anterior, podemos obter $\{y_1, z_1\} \subseteq W_1$, $\{y_2, z_2\} \subseteq W_2$ tais que $b_1(y_1, z_1) \neq 0$, $b_1(y_1, y_1) = b_1(z_1, z_1) = 0$, $b_2(y_2, z_2) = 0$, $b_2(y_2, y_2) \neq 0$ e $b_2(z_2, z_2) \neq 0$. Tomando $w_1 = (y_1, y_2 + z_2)$ e $w_2 = (\lambda_1 z_1, \lambda_2 z_2)$ em M, onde $\lambda_1 = \dfrac{1}{b_1(y_1, z_1)} \in F_1^*$ e $\lambda_2 = \dfrac{1}{b_2(z_2, z_2)} \in F_2^*$, temos que $\{w_1, w_2\}$ é uma base de um subespaço de dimensão 2 de (M,b) e, a matriz da forma bilinear restrita à este subespaço é $(b(w_i, w_j)) = \begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$ onde $\alpha = b(w_1, w_1) = (0, b_2(y_2, y_2) + b_2(z_2, z_2)) \in A$ e $\beta = b(w_2, w_2) = (0, \lambda_2^2 b_2(z_2, z_2)) \in A$ são tais que $1 - \alpha\beta = (1,1) - \left(0, \dfrac{b_2(y_2, y_2)}{b_2(z_2, z_2)} + 1\right) = \left(1, -\dfrac{b_2(y_2, y_2)}{b_2(z_2, z_2)}\right) \in A^*$. Agora, o item **(ii)** do teorema segue de **(2.8)** e da hipótese de indução, pois todo subespaço não singular de um espaço bilinear impróprio é também impróprio. ■

Corolário 2.14 *Todo espaço bilinear próprio sobre um anel semilocal A é da forma $\langle \alpha_1, \ldots, \alpha_n \rangle$, com $\alpha_i \in A^*$, $1 \leq i \leq n$.*

Dem.: Imediata. ■

2.4 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:

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

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 $\mathbb{M}(U, b)$, ou simplesmente por $\mathbb{M}(U)$, ou ainda $\mathbb{M}(b)$. Provamos a seguir que este módulo é de fato não singular.

Proposição 2.15 *Para todo módulo bilinear (U, b) sobre A, $\mathbb{M}(U)$ é um espaço bilinear.*

Dem.: Consideremos $\{e_1, \ldots, e_n, e_1^*, \ldots, e_n^*\}$ uma base de $\mathbb{M}(U) = U \oplus U^*$, onde $\{e_1, \ldots, e_n\}$ é uma base de U e $\{e_1^*, \ldots, e_n^*\}$ é a base dual de U^*. A matriz de b_U com relação a esta base é a matriz em blocos

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

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 $-\det(I)\det(I)$, 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 $\{e_1, \cdots, e_n\}$ e $\{e_1^*, \cdots, e_n^*\}$ bases de U e U^*, respectivamente. Podemos considerar $\{e_1, e_1^*, e_2, e_2^*, \cdots, e_n, e_n^*\}$ como base de $U \oplus U^*$ e em relação a esta base

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

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

Consideremos agora, $(U,b) = (A\,x, \langle\alpha\rangle)$, então

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

Mais geralmente,

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

Proposição 2.16 *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 vemos que é suficiente mostrarmos que, para todo $\alpha \in A$, temos

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

Seja $(A\,x \oplus A\,y, b) = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$, ou seja, $b(x,x) = \alpha\,, b(x,y) = 1$ e $b(y,y) = 0$. Os elementos $x' = x - \dfrac{\alpha}{2}y$ e $y' = y \in A\,x \oplus A\,y$ são tais que $b(x',x') = 0 = b(y',y')$ e $b(x',y') = 1$. Assim $(A\,x' \oplus A\,y', b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ é um subespaço não singular de

$\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$. Agora,de **(2.8)** 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 $x'' = \dfrac{x'+y'}{2}$ e $y'' = \dfrac{x'-y'}{2}$, é um subespaço não singular de $\mathbb{H}$ da forma $\langle 1, -1\rangle$ e, como acima, obtemos que $\mathbb{H} \simeq \langle 1, -1\rangle$. ■

Teorema 2.17 *Seja (M, b) um espaço bilinear sobre A. Se $U \subseteq M$ é um subespaço totalmente isotrópico de M, então existe um subespaço $V \subseteq M$ tal que $M = U^{\perp} \oplus V$ e $(U \oplus V, b)$ é metabólico.*

Dem.: De **(2.8)** temos que $U^{\perp}$ é subespaço de M e então existe $V \subseteq M$ tal que $M = U^{\perp} \oplus V$. Mais ainda, da demonstração de **(2.8)**, temos que $b : U \times M/U^{\perp} \longrightarrow A$ é não singular, isto é, $b : U \times V \longrightarrow A$ é não singular. Obtemos assim o isomorfismo $d : U \longrightarrow V^*$. Temos que $U \cap V = \{0\}$, pois $U \subseteq U^{\perp}$ e $U^{\perp} \cap V = \{0\}$. Assim $U \oplus V$ é um subespaço de M. Mostremos que $b : (U \oplus V) \times (U \oplus V) \longrightarrow A$ é não singular. Como $U \subseteq U^{\perp}$, a matriz de b em relação a decomposição $(U \oplus V) \times (U \oplus V) = (U \times U) \oplus (U \times V) \oplus (V \times U) \oplus (V \times V)$, é a matriz em blocos

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

onde B_{12} é a matriz de $b\,|_{U \times V}$ e B_{22} é a matriz de $b\,|_{V \times V}$. Como $b : U \times V \longrightarrow A$ é não singular então B_{12} é inversível. Assim

$$B^{-1} = \begin{pmatrix} -B_{12}^{-1} B_{22} B_{12}^{-1} & B_{12}^{-1} \\ B_{12}^{-1} & 0 \end{pmatrix}$$

é a inversa de B, donde concluimos que B é inversível, ou seja, $(U \oplus V, b)$ é não singular e de **(2.8)** temos que $M = (U \oplus V) \perp (U \oplus V)^{\perp}$.

Seja $f : U \oplus V \longrightarrow \mathbb{M}(V) = V \oplus V^*$ definida por $f(u+v) = v + d(u)$, para todo $u \in U$ e $v \in V$. 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 $u+v$, $u'+v'$ em $U \oplus V$, temos

$$b_V(f(u+v), f(u'+v')) = b_V(v + d(u), v' + d(u')) = b(v,v') + d(u)(v') + d(u')(v) =$$

$$= b(v,v') + b(u,v') + b(u',v) = b(u+v,v') + b(u',v+u) = b(u+v,u'+v').$$ Assim, $U \oplus V \simeq \mathbb{M}(V)$, donde concluimos que $(U \oplus V, b)$ é metabólico. ■

Corolário 2.18 *Se $x \in (M,b)$ é um elemento primitivo e isotrópico, então existe $y \in M$ tal que $(Ax \oplus Ay, b) = \begin{pmatrix} 0 & 1 \\ 1 & b(y,y) \end{pmatrix}$ é um subespaço metabólico não singular de (M,b).*

Dem.: No teorema anterior, consideremos $U = Ax$, temos que existe $V = Ay'$ tal que $(Ax \oplus Ay', b)$ é não singular e metabólico. A matriz de b com relação a base $\{x, y'\}$ é dada por $\begin{pmatrix} 0 & b(x,y') \\ b(x,y') & b(y',y') \end{pmatrix}$. Como b é não singular, temos que $b(x,y')$ é uma unidade. Tomando $y = \dfrac{1}{b(x,y')} y'$, temos que a matriz de b com relação a base $\{x, y\}$ é $\begin{pmatrix} 0 & 1 \\ 1 & b(y,y) \end{pmatrix}$, como queríamos. ■

O próximo teorema caracteriza os espaços metabólicos.

Teorema 2.19 *Seja (M,b) um espaço bilinear sobre A. Então (M,b) é um espaço metabólico se, e somente se M contém um subespaço U totalmente isotrópico maximal, isto é, $U = U^{\perp}$.*

Dem.: Seja (M,b) um espaço metabólico. Então $M = V \oplus V^*$ para algum módulo bilinear (V,b'). Como $U = V^*$ é um subespaço totalmente isotrópico, temos que $V^* \subseteq (V^*)^\perp$. Vamos mostrar que $(V^*)^\perp \subseteq V^*$, ou seja, que V^* é um subespaço totalmente isotrópico maximal de M. Consideremos $\{x_1, \ldots, x_n\}$ uma base de V e $\{x_1^*, \ldots, x_n^*\}$ a base dual de V^*. Para $v + v^* \in (V^*)^\perp$, temos $b_V(v + v^*, v_1^*) = 0$, para todo $v_1^* \in V^*$, em particular, $b_V(v + v^*, x_i^*) = 0$, para todo $i = 1, \ldots, n$. Mas $b_V(v+v^*, x_i^*) = b(v,0)+v^*(0)+x_i^*(v) = 0$, ou seja, $x_i^*(v) = 0$, para todo $i = 1, \ldots, n$. Escrevendo $v = u_1\, x_1 + \ldots + u_n\, x_n$, temos $0 = x_i^*(v) = x_i^*(u_1\, x_1 + \ldots + u_n\, x_n) = u_i$, para todo $i = 1, \ldots, n$. Logo $v = 0$ e, assim $v + v^* = v^* \in V^*$, ou seja, $(V^*)^\perp \subseteq V^*$. Portanto $V^* = (V^*)^\perp$. A recíproca segue imediatamente do teorema **(2.17)**. ■

Corolário 2.20 *Seja* $(V,b) \in \mathcal{B}il\,(A)$.

(i) *Se* (U,b') *é um módulo bilinear sobre* A, *então* $\mathbb{M}\,(U) \otimes (V,b) \simeq \mathbb{M}\,(U \otimes V)$.

(ii) $(V,b) \perp (V,-b) \simeq \mathbb{M}\,(V)$, *onde* $-b(x,y) = (-1)\,b(x,y)$, *para todo* $x,\ y \in V$.

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)**, usando o 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 $(u_i \oplus u_i^*) \otimes v_i$, com $u_i \in U$ e v_i em alguma base de V. Para tais elementos temos

$$(b_U \otimes b)((u_i + u_i^*) \otimes v_i, u^* \otimes v) = 0,$$

para todo $u^* \in U^*$ e $v \in V$. Como v_i pertence a alguma base de V e (V,b) é não singular, temos que existe $v \in V$ tal que $b(v_i, v) \in A^*$. Assim $0 = b_U(u_i + u_i^*, u^*)$ ·

$b(v_i, v)$, para todo $u^* \in U^*$, o que implica que $0 = b_U(u_i + u_i^*, u^*) = b(u_i, 0) + u_i^*(0) + u^*(u_i)$, 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 $U = \{(x, x);\ x \in V\}$ é um subespaço totalmente isotrópico maximal de $(V, b) \perp (V, -b)$. ■

Proposição 2.21 *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 $\{x_1, \ldots, x_n, x_1^*, \ldots, x_n^*\}$ uma base de $U \oplus U^*$, onde $\{x_1, \ldots, x_n\}$ é uma base de U e $\{x_1^*, \ldots, x_n^*\}$ 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 dada. 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. ■

Capítulo 3

O Anel de Witt

Neste capítulo apresentaremos um estudo da estrutura do anel $\mathcal{W}(A)$, o anel de Witt dos espaços bilineares sobre um anel semilocal A. Mais especificamente, daremos uma descrição dos ideais primos e dos geradores de $\mathcal{W}(A)$. Apresentaremos também um estudo dos elementos de torção, dos elementos nilpotentes e dos divisores de zero de $\mathcal{W}(A)$.

3.1 Geradores de $\mathcal{W}(A)$

À categoria $\mathcal{B}il(A)$ associamos seu correspondente *Anel de Grothendieck*, o qual é chamado, *Anel de Witt-Grothendieck* dos espaços bilineares sobre A. Tal anel será denotado por $\widehat{\mathcal{W}}(A)$. Se $[b]$ denota a classe de isometrias do espaço bilinear b, então os elementos de $\widehat{\mathcal{W}}(A)$ 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 $b \in \mathcal{B}il(A)$ 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 $\widehat{\mathcal{W}}(A)$ são as operações induzidas pelas operações soma ortogonal e produto tensorial de $\mathcal{B}il(A)$.

Seja $\widehat{\mathbb{M}}(A) = \{[b]-[b'] \in \widehat{\mathcal{W}}(A);\ b \text{ e } b' \text{ são metábolicos}\}$. De **(2.20)**, decorre que $\widehat{\mathbb{M}}(A)$ é um ideal de $\widehat{\mathcal{W}}(A)$. Assim definimos o *anel de Witt dos espaços bilineares*

sobre A como sendo o anel quociente $\mathcal{W}(A) = \dfrac{\widehat{\mathcal{W}}(A)}{\widehat{\mathbb{M}}(A)}$.

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

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

De **(2.20)** temos que $b_2 \perp (-b_2)$ é metabólico; logo $[b_2 \perp (-b_2)] = [0]$ em $\mathcal{W}(A)$. Assim, $[b_1] - [b_2] = [b_1 \perp (-b_2)]$, ou seja, todo elemento de $\mathcal{W}(A)$ pode ser escrito na da forma $[b]$, com b em $\mathcal{B}il\,(A)$.

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

Vemos facilmente que $\mathcal{W}(A)$, com as operações induzidas por $\perp$ e $\otimes$, é de fato um anel comutativo com elemento identidade, onde $-[b] = [(-b)]$ e $1_{\mathcal{W}(A)} = [\langle 1 \rangle]$. Quando não houver perigo de confusão denotaremos simplesmente por b o elemento $[b]$ de $\mathcal{W}(A)$, dentro do contexto se tornará claro quando consideramos b como um elemento de $\mathcal{W}(A)$ ou como um elemento de $\mathcal{B}il\,(A)$.

Decorre de **(2.21)** que, para todo módulo bilinear (U, b), $\mathbb{M}(U) = \mathbb{H}(U)$ em $\mathcal{W}(A)$. Desta forma se considerarmos o subconjunto de $\widehat{\mathcal{W}}(A)$

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

temos que $\widehat{\mathbb{H}}(A) = \widehat{\mathbb{M}}(A)$ em $\widehat{\mathcal{W}}(A)$. 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 $\mathcal{W}(A)$ 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 $\mathcal{W}(A) = \dfrac{\widehat{\mathcal{W}}(A)}{\mathbb{Z}\,\mathbb{H}}$.

Proposição 3.1 *Dois espaços bilineares são iguais em* $\widehat{\mathcal{W}}(A)$ *se, e somente se são iguais em* $\mathcal{W}(A)$ *e tem a mesma dimensão.*

Dem.: Se $[b_1] = [b_2]$ em $\widehat{\mathcal{W}}(A)$, então existe $(V,b) \in \mathcal{B}il(A)$ 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 **(2.20)**, que $b_1 \perp \mathbb{M}(V) \simeq b_2 \perp \mathbb{M}(V)$, ou seja, $[b_1] = [b_2]$ em $\mathcal{W}(A)$. Reciprocamente, sejam $b_1, b_2 \in \mathcal{B}il(A)$ espaços de mesma dimensão tais que $[b_1] = [b_2]$ em $\mathcal{W}(A)$. 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 $\widehat{\mathcal{W}}(A)$. ■

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

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

Teorema 3.2 *O anel $\mathcal{W}(A)$ é aditivamente gerado por $f(G)$, a imagem de f.*

Dem.: Seja $b \in \mathcal{B}il(A)$. O espaço bilinear $b \perp \langle 1\rangle$ é próprio e, de **(2.13)**, $b \perp \langle 1\rangle$ admite uma base ortogonal, ou seja, existem $\beta_1, \ldots, \beta_n \in A^\star$ tais que:

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

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

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

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

Observação 3.3 O resultado acima mostra, em particular, que todo elemento de $\mathcal{W}(A)$ 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 do teorema anterior, podemos afirmar que existe um homomorfismo de anéis sobrejetor $\varphi : \mathbb{Z}[G] \to \mathcal{W}(A)$, que é a extensão por linearidade de f. O próximo resultado caracteriza o núcleo $\mathcal{K}$ deste homomorfismo.

Proposição 3.4 *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*

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

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 $\langle \alpha_1, \ldots, \alpha_r \rangle = \langle \beta_1, \ldots, \beta_s \rangle$ em $\mathcal{W}(A)$, ou seja, existem U_1, $U_2 \in \mathcal{B}il(A)$, tais que

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

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 $b_1 = \langle \alpha_1, \ldots, \alpha_r \rangle$ e $b_2 = \langle \beta_1, \ldots, \beta_s \rangle \perp t\langle 1, -1 \rangle$. Desde que $b_1 = b_2$ em $\mathcal{W}(A)$ e $\dim(b_1) = \dim(b_2)$, temos por **(3.1)** que eles representam o mesmo elemento em $\widehat{\mathcal{W}}(A)$. Assim, existe $b_3 \in \mathcal{B}il(A)$ tal que

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

Somando $\langle 1 \rangle$ em ambos os lados, se necessário, podemos assumir que b_3 é próprio, ou seja $b_3 \simeq \langle \alpha_{r+1}, \ldots, \alpha_n \rangle$. Tomando $\beta_i = \pm 1$ para $s < i \leq r$ e $\beta_i = \alpha_i$ para $r < i \leq n$, obtemos $\langle \alpha_1, \ldots, \alpha_n \rangle \simeq \langle \beta_1, \ldots, \beta_n \rangle$ e $z = t((1) + (-1)) + \sum_{i=1}^{n}(\alpha_i) - \sum_{i=1}^{n}(\beta_i)$, como queríamos. ∎

Teorema 3.5 *O anel $\mathcal{W}(A)$ 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) $\langle \alpha_1 \rangle + \cdots + \langle \alpha_n \rangle = \langle \beta_1 \rangle + \cdots + \langle \beta_n \rangle \iff \langle \alpha, \ldots, \alpha_n \rangle \simeq \langle \beta_1, \ldots, \beta_n \rangle$.

(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.: Para mostrarmos que **(i)**, **(ii)** ,**(iii)** e **(v)** valem para $\mathcal{W}(A)$, basta observarmos que $\mathcal{W}(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$ e usarmos a proposição anterior.

Mostremos então o item **(iv)**. Consideremos o espaço bilinear (M, b) com uma base $\{x, y\}$ tal que, $b(x, y) = 0$, $b(x, x) = \alpha$ e $b(y, y) = \beta$, ou seja $b = \langle \alpha, \beta \rangle$. Então, $b(x + y, x + y) = \alpha + \beta \in A^*$. Como $\alpha + \beta \in A^*$ temos que $(A(x + y), b)$ é um subespaço não singular de (M, b) e de **(2.8)**, $M = A(x + y) \perp (A(x + y))^{\perp}$. Como $(A(x + y))^{\perp}$ é um subespaço não singular de (M, b) 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,

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

Comparando os determinantes, temos $\alpha \beta \equiv (\alpha + \beta)\gamma \bmod (A^*)^2$. 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, de **(i)** $\langle \gamma \rangle = \langle \alpha \beta (\alpha + \beta) \rangle$. Consequentemente,

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

Portanto, $\langle \alpha \rangle + \langle \beta \rangle = \langle \alpha + \beta \rangle + \langle \alpha \beta (\alpha + \beta) \rangle$ em $\mathcal{W}(A)$, por **(ii)**. ■

3.2 Os ideais primos de $\mathcal{W}(A)$

Nesta seção caracterizaremos os ideais primos de $\mathcal{W}(A)$ usando o isomorfismo de anéis $\mathcal{W}(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$, onde $G = A^*/A^{*2}$ e $\mathcal{K}$ é bem determinado em **(3.4)**, ou seja,

usaremos o fato que os ideais primos de $\mathcal{W}(A)$ 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 3.6 *Para cada ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, temos*

(i) *Se $\mathcal{P} \cap \mathbb{Z} = \{0\}$, então existe um único homomorfismo de anéis ϕ de $\mathbb{Z}[G]$ em $\mathbb{Z}$ com núcleo $\mathcal{P}$.*

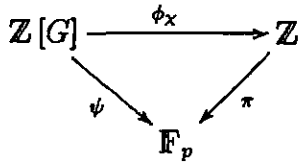
(ii) *Se $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, onde p é um número inteiro primo, então existe um único homomorfismo de anéis ψ de $\mathbb{Z}[G]$ em $\mathbb{F}_p$, com núcleo $\mathcal{P}$, onde $\mathbb{F}_p$ denota o corpo finito com p elementos.*

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

Se $\mathcal{P} \cap \mathbb{Z} = \{0\}$, então $\mathbb{Z} \cong \frac{\mathbb{Z}[G]}{\mathcal{P}}$ e se $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, 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 $\phi : \mathbb{Z}[G] \to \mathbb{Z}$, $\phi(g)^2 = \phi(g^2) = \phi(1) = 1$. Como $\phi(g) \in \mathbb{Z}$, temos que $\phi(g) = \pm 1$. Logo, todo homomorfismo de aneis 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 $\chi : G \to \{\pm 1\}$, ele se estende, de maneira única, a um homomorfismo de aneis $\phi_\chi : \mathbb{Z}[G] \to \mathbb{Z}$, 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 aneis $\psi : \mathbb{Z}[G] \to \mathbb{F}_p$ ao grupo G, é também um caracter $\chi : G \to \{\pm 1\}$. Assim, existe uma única extensão $\phi_\chi : \mathbb{Z}[G] \to \mathbb{Z}$ que faz o diagrama abaixo comutar



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 aneis $\psi_o : \mathbb{Z}[G] \to \mathbb{F}_2$, que é obtido da composição de $\phi_\chi : \mathbb{Z}[G] \to \mathbb{Z}$ com a projeção canônica sobre $\mathbb{F}_2$, onde ϕ_χ é a extensão de qualquer caracter $\chi : G \to \{\pm 1\}$.

Destas observações e do lema **(3.6)**, temos

Proposição 3.7 *Para cada ideal primo $\mathcal{P}$ de $\mathbb{Z}[G]$, temos*

(i) *Se $\mathcal{P} \cap \mathbb{Z} = \{0\}$, então existe um único caracter χ de G, tal que $\mathcal{P} = \mathcal{P}_\chi$ é o núcleo do homomorfismo $\phi_\chi : \mathbb{Z}[G] \to \mathbb{Z}$.*

(ii) *Se $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, p um número primo ímpar, então existe um único caracter χ de G, tal que $\mathcal{P}$ coincide com o conjunto*

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

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

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

para cada caracter χ de G.

Observação 3.8 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 $\mathcal{W}(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$. Denotemos por $\mathcal{I}(A)$ o núcleo do homomorfismo de anéis $d_0 : \mathcal{W}(A) \to \mathbf{F}_2$, definido por

$$d_0([b]) = (\dim(b)) \bmod 2.$$

Desde que $\frac{\mathcal{W}(A)}{\mathcal{I}(A)} \cong \mathbf{F}_2$ é corpo, temos que $\mathcal{I}(A)$ é um ideal maximal de $\mathcal{W}(A)$, chamado o *o ideal fundamental* de $\mathcal{W}(A)$.

Proposição 3.9 *O ideal fundamental $\mathcal{I}(A)$ é o único ideal primo de $\mathcal{W}(A)$ que contém $2\langle 1\rangle = 2.1_{\mathcal{W}(A)}$.*

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 $(2) \in G$. Como $\varphi\langle 2\rangle = 2\langle 1\rangle$, temos que $\mathcal{I}(A)$ corresponde ao ideal $\mathcal{P}_0$ de $\mathbb{Z}[G]$, na correspondência entre os ideais de $\mathcal{W}(A)$ e os ideais de $\mathbb{Z}[G]$ que contém $\mathcal{K}$. Portanto, a unicidade de $\mathcal{I}(A)$ decorre da unicidade de $\mathcal{P}_0$. ∎

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

Definição 3.10 Uma *assinatura de A* é um homomorfismo de anéis de $\mathcal{W}(A)$ 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.*

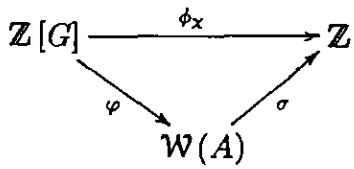
Assumimos primeiro, que A é um anel formalmente real, ou seja, $Ass(A) \neq \emptyset$.

Do teorema do isomorfismo para anéis, segue imediatamente que $\frac{\mathcal{W}(A)}{\mathcal{P}_\sigma} \cong \mathbb{Z}$, para toda $\sigma \in Ass(A)$.

Proposição 3.11 *Para cada ideal primo $\mathcal{P}$ de $\mathcal{W}(A)$ que não contém $p\langle 1\rangle$, 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 $\mathcal{W}(A)$ que não contém $p\langle 1\rangle$, para todo número primo p. Desde que $\mathcal{W}(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$, temos que existe $\mathcal{P}' = \varphi^{-1}(\mathcal{P})$, ideal primo de $\mathbb{Z}[G]$ tal que $\mathcal{K} \subseteq \mathcal{P}'$. Como $p\langle 1\rangle \notin \mathcal{P}$ para todo número primo p, o ideal $\mathcal{P}'$ é tal que $\mathcal{P}' \cap \mathbb{Z} = \{0\}$.

Pelo item **(i)** da proposição **(3.7)** existe um único homomorfismo de anéis $\phi_\chi : \mathbb{Z}[G] \to \mathbb{Z}$, tal que $Ker(\phi_\chi) = \mathcal{P}'$. Mas $\mathcal{K} \subseteq Ker(\phi_\chi) = \mathcal{P}'$. Logo, existe uma única $\sigma \in Ass(A)$ que faz o seguinte diagrama comutar



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 $x \in Ker(\phi_\chi) = \mathcal{P}$. Logo, $\varphi(x) = b \in \mathcal{P}$. Portanto $\mathcal{P}_\sigma \subseteq \mathcal{P}$, como queríamos. ■

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

Lema 3.12 *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 analizarmos 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 $(\alpha_1, \ldots, \alpha_n) \simeq (\beta_1, \ldots, \beta_n)$. 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,

$$\phi_\chi(z) = \phi_\chi\left(\sum_{i=1}^{n} (\alpha_i)\right) - \phi_\chi\left(\sum_{i=1}^{n} (\beta_i)\right) = -s + (n-s) + t - (n-t) = 2(t-s).$$

Mas $(\alpha_1, \ldots, \alpha_n) \simeq (\beta_1, \ldots, \beta_n)$, o que implica que seus determinantes diferem por quadrados, ou seja,

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

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, $\phi_\chi(z) \equiv 0 \bmod 4$. Portanto, $\phi_\chi(\mathcal{K}) = 0$ ou $\phi_\chi(\mathcal{K}) \subseteq 2^n\mathbb{Z}$, para algum $n \geq 1$. ∎

Corolário 3.13 *Se $\phi_\chi(\mathcal{K}) \subseteq p\mathbb{Z}$, para algum primo ímpar p, então $\phi_\chi(\mathcal{K}) = 0$.*

Dem.: Imediata. ∎

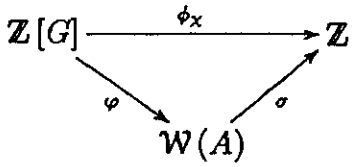
Proposição 3.14 *Seja p um número primo ímpar. Para cada ideal primo $\mathcal{P}$ de $\mathcal{W}(A)$ com $p\langle 1\rangle \in \mathcal{P}$, existe uma única assinatura σ de A tal que $\mathcal{P}$ coincide com o conjunto*

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

Dem.: Seja $\mathcal{P}$ um ideal primo de $\mathcal{W}(A)$ com $p\langle 1\rangle \in \mathcal{P}$. Novamente pelo isomorfismo $\mathcal{W}(A) \cong \frac{\mathbb{Z}[G]}{\mathcal{K}}$ temos que existe $\mathcal{P}' \subseteq \mathbb{Z}[G]$ tal que $\mathcal{K} \subseteq \mathcal{P}'$ e $\varphi(\mathcal{P}') = \mathcal{P}$. Como

$p\langle 1\rangle \in \mathcal{P}$, temos que $\mathcal{P}' \cap \mathbb{Z} = p\mathbb{Z}$. Por **(3.7)**, temos que existe um único caracter χ de G, tal que $\mathcal{P}' = \mathcal{P}_{\chi,p} = \{z \in \mathbb{Z}[G];\ \phi_\chi(z) \equiv 0 \bmod p\}$.

Do fato que $\mathcal{K} \subseteq \mathcal{P}' = \mathcal{P}_{\chi,p}$, segue que $\phi_\chi(\mathcal{K}) = p\mathbb{Z}$. Assim de **(3.13)** temos que $\phi_\chi(\mathcal{K}) = 0$. Logo $\mathcal{K} \subseteq Ker(\phi_\chi)$ e, consequentemente, existe uma única $\sigma \in Ass(A)$ que faz o diagrama abaixo comutar



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 $\phi_\chi(x) \equiv 0 \bmod p$. Assim, $\sigma(b) = \sigma \circ \varphi(x) = \phi_\chi(x) \equiv 0 \bmod p$, 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, $\phi_\chi(x) = \sigma \circ \varphi(x) = \sigma(b) \equiv 0 \bmod p$, ou seja, $x \in \mathcal{P}'$. Logo, $b = \varphi(x) \in \mathcal{P}$. Portanto, $\mathcal{P}_{\sigma,p} = \mathcal{P}$, como queríamos. ∎

De **(3.7)** e da correspondência entre os ideais de $\mathcal{W}(A)$ com os ideais de $\mathbb{Z}[G]$, que contém $\mathcal{K}$, concluimos que se $Ass(A) \neq \emptyset$ então $\mathcal{P}_\sigma$, $\mathcal{P}_{\sigma,p}$, para cada $\sigma \in Ass(A)$ e todo número primo ímpar p, e $\mathcal{J}(A)$ são todos os ideais primos de $\mathcal{W}(A)$.

Teorema 3.15 *Se A é um anel semilocal formalmente real, então:*

(i) *Os $\mathcal{P}_\sigma$, com $\sigma \in Ass(A)$, são todos os ideais primos minimais de $\mathcal{W}(A)$.*

(ii) *Os $\mathcal{P}_{\sigma,p}$ com $\sigma \in Ass(A)$ e p um número primo ímpar, e $\mathcal{J}(A)$ são todos os ideais primos maximais de $\mathcal{W}(A)$.*

(iii) *Cada $\mathcal{P}_{\sigma,p}$ contém um único ideal primo minimal, a saber $\mathcal{P}_\sigma$.*

(iv) *$\mathcal{J}(A)$ 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 $\mathcal{W}(A)/\mathcal{P}_\sigma \cong \mathbb{Z}$, existe um único ideal maximal de $\mathcal{W}(A)$ que contém $p\langle 1\rangle$ e $\mathcal{P}_\sigma$, que é claramente $\mathcal{P}_{\sigma,p}$. Suponhamos que exista um ideal primo minimal $\mathcal{P}_\psi$ de $\mathcal{W}(A)$, tal que $\mathcal{P}_\psi$ também esta contido em $\mathcal{P}_{\sigma,p}$. Como $\mathcal{P}_{\sigma,p}$ contém $\mathcal{P}_\psi$ e $p\langle 1\rangle$ temos que $\mathcal{P}_{\sigma,p} = \mathcal{P}_{\psi,p}$. Segue então de **(3.14)** que $\sigma = \psi$. Portanto $\mathcal{P}_\sigma = \mathcal{P}_\psi$, o que mostra **(iii)**.

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

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

Teorema 3.16 *O anel A é não formalmente real se, e somente se $\mathcal{I}(A)$ é o único ideal primo de $\mathcal{W}(A)$.*

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

Como uma consequência imediata deste teorema temos:

Corolário 3.17 *Se A é não formalmente real, então os divisores de zero de $\mathcal{W}(A)$ tem dimensão par, isto é, são representados por um espaço bilinear de dimensão par.*

Dem.: De **(3.16)** temos que $\mathcal{W}(A)$ é um anel local com único ideal maximal $\mathcal{J}(A)$. Logo, os divisores de zero, que não são inversíveis, estão em $\mathcal{J}(A)$. ■

3.3 $\mathcal{N}il(\mathcal{W}(A))$ e $\mathcal{W}_t(A)$

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 $\mathcal{W}(A)$ é um anel comutativo com elemento identidade $\langle 1\rangle$, o conjunto dos elementos nilpotentes de $\mathcal{W}(A)$ formam o nilradical de $\mathcal{W}(A)$, que denotaremos por $\mathcal{N}il(\mathcal{W}(A))$. O ideal dos elementos de torção de $\mathcal{W}(A)$ será denotado por $\mathcal{W}_t(A)$.

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 $\mathcal{W}(A)$ tem somente 2-torção.

Ao contrário da seção anterior, assumiremos primeiramente que A é um anel semilocal não formalmente real. Neste caso, como conseqüência imediata do teorema **(3.16)** e sua demonstração, temos

Teorema 3.18 *Se A é um anel semilocal não formalmente real, então*

(i) $\mathcal{N}il(\mathcal{W}(A)) = \mathcal{J}(A)$.

(ii) $\mathcal{W}_t(A) = \mathcal{W}(A)$.

(iii) $\mathcal{W}(A)$ *tem somente 2-torção.*

Dem.: Imediata. ■

Agora seja A um anel semilocal formalmente real. Desde que os $\mathcal{P}_\sigma$, com σ em $\mathcal{A}ss(A)$, são todos os ideais primos minimais de $\mathcal{W}(A)$, temos

Proposição 3.19 *Um elemento $b \in \mathcal{W}(A)$ é nilpotente se, e somente se $\sigma(b) = 0$ para toda $\sigma \in Ass(A)$, isto é, $\mathcal{N}il(\mathcal{W}(A)) = \bigcap_{\sigma \in Ass(A)} \mathrm{Ker}(\sigma)$.*

Dem.: Imediata. ∎

Para o ideal de torção temos

Proposição 3.20 *Se A é um anel semilocal formalmente real, então*

$$\mathcal{W}_t(A) = \mathcal{N}il(\mathcal{W}(A)).$$

Dem.: Sejam $b \in \mathcal{W}_t(A)$ e $n \in \mathbb{N}$, $n \geq 1$, tal que $nb = 0$. Então, para cada $\sigma \in Ass(A)$, temos $\sigma(nb) = n\sigma(b) = 0$, o que implica que $\sigma(b) = 0$. Assim, b pertence a $\bigcap_{\sigma \in Ass(A)} \mathrm{Ker}(\sigma) = \mathcal{N}il(\mathcal{W}(A))$, o que mostra que $\mathcal{W}_t(A) \subseteq \mathcal{N}il(\mathcal{W}(A))$. Reciprocamente, dado $b = \langle \alpha_1, ..., \alpha_n \rangle \in \mathcal{N}il(\mathcal{W}(A))$; consideremos H o subgrupo de G gerado por $\{(\alpha_1), \ldots, (\alpha_n)\}$. Então, desde que todo elemento de G tem ordem 2, temos que H é um subgrupo finito de G e b está no subanel R de $\mathcal{W}(A)$ isomorfo à $\frac{\mathbb{Z}[H]}{(\mathcal{K} \cap \mathbb{Z}[H])}$. Usando o teorema de Maschke, ver **(3.6)** em **[13]**, temos que o anel de grupo $\mathbb{Q}[H] \cong \mathbb{Q} \otimes \mathbb{Z}[H]$ é semi-simples, ou seja, $\mathcal{N}il(\mathbb{Q}[H]) = \{0\}$.

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 **[13]** que $\mathcal{N}il(\mathbb{Q} \otimes R) = \{0\}$.

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

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

Teorema 3.21 (Princípio Local-Global de Pfister) *Seja A um anel semilocal formalmente real. Então uma forma bilinear b representa um elemento de torção em $\mathcal{W}(A)$ se, e somente se $\sigma(b) = 0$, para toda $\sigma \in Ass(A)$.*

Dem.: Imediata. ∎

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

Teorema 3.22 *Se A é um anel semilocal formalmente real, então $\mathcal{W}(A)$ tem somente 2-torção.*

Dem.: Seja $b = \langle \alpha_1, \ldots, \alpha_n \rangle \in \mathcal{W}_t(A)$. Desde que $\mathcal{W}_t(A) = \mathcal{N}il(\mathcal{W}(A))$, temos que $b \in \mathcal{N}il(\mathcal{W}(A))$ e, como na demonstração da proposição anterior, b está no subanel R de $\mathcal{W}(A)$ isomorfo à $\dfrac{\mathbb{Z}[H]}{(\mathcal{K} \cap \mathbb{Z}[H])}$, onde H é o subgrupo de G gerado por $\{(\alpha_1), \ldots, (\alpha_n)\}$. Agora, para mostrarmos que b é 2-torção em $\mathcal{W}(A)$, 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 $R \cong \dfrac{\mathbb{Z}[H]}{(\mathcal{K} \cap \mathbb{Z}[H])}$, temos que $\dfrac{R}{pR} \cong \dfrac{\mathbb{F}_p[H]}{\mathcal{K}'}$, para algum subgrupo $\mathcal{K}'$ 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, $\mathcal{N}il(R/pR) = \{0\}$.

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

Se $b_0 \in R$ tem p-torção, entao $b_0 \in R_t = pR_t$, ou seja, $b_0 = pb_1$, com b_1 em R_t que também tem p-torção, o que implica que $b_1 = p\ b_2$, para algum $b_2 \in R_t$ e consequentemente, $b_0 = p^2\ b_2$. 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 $\mathcal{W}(A)$ tem dimensão par.

Corolário 3.23 *Os divisores de zero de $\mathcal{W}(A)$ tem dimensão par.*

Dem.: Em [07], página 3, temos que o conjunto dos divisores de zero de $\mathcal{W}(A)$ é uma união de ideais primos. Suponhamos que $p\langle 1\rangle$ é um divisor de zero, para algum número primo ímpar p. Então existe $b \in \mathcal{W}(A)$, $b \neq 0$, tal que $p\langle 1\rangle \otimes b = 0$ em $\mathcal{W}(A)$, o que implica que b tem p-torção em $\mathcal{W}(A)$. Mas, do teorema anterior temos que $\mathcal{W}(A)$ tem somente 2-torção. Assim, $p\langle 1\rangle$ não é divisor de zero para nenhum primo ímpar p. Assim, na união dos ideais primos que compoem os divisores de zero, não aparece ideais primos da forma $\mathcal{P}_{\sigma,p}$, com $\sigma \in \mathcal{A}ss(A)$ e p um número primo ímpar, ou seja, de **(3.15)**, temos que cada ideal primo que aparece na união é minimal ou $\mathcal{J}(A)$. Desde que $\mathcal{P}_\sigma \subseteq \mathcal{J}(A)$, para todo $\sigma \in \mathcal{A}ss(A)$, o resultado segue. ■

Capítulo 4

Ideais Primários no Anel de Witt

Neste capítulo apresentaremos uma caracterização dos ideais primários de $\mathcal{W}(A)$ cujos radicais estão caracterizados em **(3.15)** e **(3.16)**. Apresentaremos também condições necessárias e suficientes para que todo ideal de $\mathcal{W}(A)$ admita uma decomposição primária, bem como alguns resultados sobre ideais decomponíveis contendo uma forma de dimensão ímpar.

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

4.1 Ideais Primários de $\mathcal{W}(A)$

Nesta seção apresentaremos a caracterização dos ideais $\mathcal{P}$-primários para cada tipo de ideal primo caracterizado em **(3.15)** e **(3.16)**, onde A é um anel semilocal. Iniciaremos com a caracterização dos ideais $\mathcal{I}(A)$-primários, onde $\mathcal{I}(A)$ é o ideal fundamental de $\mathcal{W}(A)$, ou seja $\mathcal{I}(A) = \{b \in \mathcal{W}(A);\ \dim(b) \text{ é par}\}$. Para tanto, necessitaremos dos seguintes resultados auxiliares

Lema 4.1 *O ideal fundamental $\mathcal{I}(A)$ é aditivamente gerado pelo conjunto*

$\{\langle 1,\alpha\rangle \in \mathcal{W}(A);\ \alpha \in A^*\}$.

Dem.: Dado $b \in \mathcal{I}(A)$, de **(3.2)**, podemos escrever $b = \langle \alpha_1, \ldots, \alpha_{2n}\rangle$, com $\alpha_i \in A^*$, $i = 1, \ldots, 2n$. Desde que $\langle 1,-1\rangle = 0$ em $\mathcal{W}(A)$, temos que $b = \perp_{i=1}^{n} \langle 1,\alpha_i\rangle - \perp_{i=n+1}^{2n} \langle 1,-\alpha_i\rangle$, o que mostra o lema. ■

Lema 4.2 *Para cada $\alpha \in A^*$, temos que $\langle 1,\alpha\rangle^{k+1} = 2^k\langle 1,\alpha\rangle$ em $\mathcal{W}(A)$, para todo inteiro $k \geq 1$.*

Dem.: A demonstração será feita usando indução sobre k. Se $k = 1$, então $\langle 1,\alpha\rangle^2 = \langle 1,\alpha\rangle \otimes \langle 1,\alpha\rangle = \langle 1,\alpha,\alpha,\alpha^2\rangle = \langle 1,\alpha,1,\alpha\rangle = 2\langle 1,\alpha\rangle$. Suponhamos agora que o resultado vale para $k-1$, ou seja, $\langle 1,\alpha\rangle^k = 2^{k-1}\langle 1,\alpha\rangle$. Assim

$$\langle 1,\alpha\rangle^{k+1} = \langle 1,\alpha\rangle^k.\langle 1,\alpha\rangle = 2^{k-1}\langle 1,\alpha\rangle \cdot \langle 1,\alpha\rangle = 2^k\langle 1,\alpha\rangle,$$

o que conclui a demonstração. ■

Teorema 4.3 *Seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal. Então $\mathcal{J}$ é $\mathcal{I}(A)$-primário se, e somente se $2^k\langle 1\rangle \in \mathcal{J}$, para algum inteiro positivo k.*

Dem.: Se $\mathcal{J}$ é $\mathcal{I}(A)$-primário então $2^k\langle 1\rangle = (2\langle 1\rangle)^k \in \mathcal{J}$, para algum inteiro $k \geq 1$, pois $2\langle 1\rangle = \langle 1,1\rangle \in \mathcal{I}(A) = r(\mathcal{J})$.

Reciprocamente, suponhamos que $2^k\langle 1\rangle \in \mathcal{J}$, para algum inteiro $k \geq 1$. Assim, $2\langle 1\rangle \in r(\mathcal{J})$ e, como de **(3.9)** $\mathcal{I}(A)$ é o único ideal maximal de $\mathcal{W}(A)$ que contém $2\langle 1\rangle$, obtemos que $r(\mathcal{J}) \subseteq \mathcal{I}(A)$. Para provarmos que $\mathcal{I}(A) \subseteq r(\mathcal{J})$, usando o lema **(4.1)** é suficiente mostrarmos que $\langle 1,\alpha\rangle \in r(\mathcal{J})$, para todo $\alpha \in A^*$. Dado $\alpha \in A^*$, desde que $2^k\langle 1\rangle \in \mathcal{J}$ para algum $k \geq 1$ e $2^k\langle 1,\alpha\rangle = 2^k\langle 1\rangle + 2^k\langle 1\rangle \cdot \langle\alpha\rangle$, temos do lema **(4.2)** que $\langle 1,\alpha\rangle^{k+1} \in \mathcal{J}$, ou seja, $\langle 1,\alpha\rangle \in r(\mathcal{J})$. Assim, $r(\mathcal{J}) = \mathcal{I}(A)$ e de **(4.2)** de **[01]**, temos que $\mathcal{J}$ é $\mathcal{I}(A)$-primário. ■

Corolário 4.4 *Se A é não formalmente real então todo ideal de $\mathcal{W}(A)$ é $\mathcal{I}(A)$-primário.*

Dem.: Da demonstração de **(3.16)** temos que $2\langle 1\rangle$ é um elemento nilpotente de $\mathcal{W}(A)$. Assim, existe um inteiro $k \geq 1$ tal que $(2\langle 1\rangle)^k = 2^k\langle 1\rangle = 0$, consequentemente $2^k\langle 1\rangle \in \mathcal{J}$, para cada ideal $\mathcal{J}$ de $\mathcal{W}(A)$. Agora o resultado segue de **(4.3)**. ■

O próximo passo é analizarmos os ideais $\mathcal{P}$-primários correspondentes aos ideais primos $\mathcal{P}$ de $\mathcal{W}(A)$ distintos de $\mathcal{I}(A)$. De **(3.15)** e **(3.16)** temos que tais ideais primos existem se, e somente se $Ass(A) \neq \emptyset$. Portanto, no que segue, assumiremos que A é um anel semilocal formalmente real. Para os ideais primos minimais temos:

Teorema 4.5 *Sejam $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal e $\sigma \in Ass(A)$. Então $\mathcal{J}$ é $\mathcal{P}_\sigma$-primário se, e somente se $\mathcal{J} = \mathcal{P}_\sigma$.*

Dem.: Claramente $\mathcal{P}_\sigma$ é $\mathcal{P}_\sigma$-primário. Reciprocamente, seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal $\mathcal{P}_\sigma$-primário. Suponhamos que $\mathcal{J} \neq \mathcal{P}_\sigma$. Como $\mathcal{J} \subseteq r(\mathcal{J}) = \mathcal{P}_\sigma \subseteq \mathcal{I}(A)$, obtemos de **(4.1)** que existe $\alpha \in A^*$ tal que $\langle 1, -\alpha\rangle \in \mathcal{P}_\sigma - \mathcal{J}$. Como $\langle 1, -\alpha\rangle \in \mathcal{P}_\sigma$ então $\langle 1, -\alpha\rangle^m \in \mathcal{J}$, para algum inteiro $m > 1$. Mas, de **(4.2)**, temos que $\langle 1, -\alpha\rangle^m = 2^{(m-1)}\langle 1, -\alpha\rangle = 2^{m-1}\langle 1\rangle \cdot \langle 1, -\alpha\rangle$. Agora, como $\mathcal{J}$ é um ideal primário de $\mathcal{W}(A)$ e $\langle 1, -\alpha\rangle \notin \mathcal{J}$, temos que existe um inteiro $s \geq 1$ tal que $(2^{m-1}\langle 1\rangle)^s \in \mathcal{J}$, ou seja, $2^k\langle 1\rangle \in \mathcal{J}$ para algum inteiro positivo k. Mas, isto é uma contradição, pois $\mathcal{J} \subseteq \mathcal{P}_\sigma$ e $\sigma(2^k\langle 1\rangle) = 2^k \neq 0$. Logo $\mathcal{J} = \mathcal{P}_\sigma$ como queríamos. ■

Finalmente, caracterizaremos os ideais $\mathcal{P}$-primários onde $\mathcal{P}$ é um ideal primo maximal de $\mathcal{W}(A)$ distinto de $\mathcal{I}(A)$. Mostraremos, neste caso, que os ideais $\mathcal{P}$-primários são exatamente as potências de $\mathcal{P}$.

Dado $\mathcal{P}_{\sigma,p} \in \mathrm{Spec}(\mathcal{W}(A))$, $\sigma \in Ass(A)$ e p um número primo ímpar, para cada inteiro $i \geq 1$, denotaremos por $\mathcal{P}_{\sigma,p^i}$ o ideal de $\mathcal{W}(A)$

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

Com esta notação temos

Lema 4.6 *Para cada* $i \geq 1$, $(\mathcal{P}_{\sigma,p})^i = \mathcal{P}_{\sigma,p^i}$.

Dem.: É fácil ver que $(\mathcal{P}_{\sigma,p})^i \subseteq \mathcal{P}_{\sigma,p^i}$. Desde que $\mathcal{P}_\sigma \subseteq \mathcal{I}(A)$, de **(4.1)** e da definição de $\mathcal{P}_\sigma$, obtemos que $\mathcal{P}_\sigma$ é aditivamente gerado por elementos da forma $\langle 1, \alpha \rangle$, com $\alpha \in A^*$ tal que $\sigma(\langle \alpha \rangle) = -1$. Para um tal gerador $\langle 1, \alpha \rangle \in \mathcal{P}_\sigma$ e $s = \dfrac{(p-1)}{2} \in \mathbb{Z}$, temos que

$$\langle 1, \alpha \rangle = \langle 1, \alpha \rangle \cdot (\langle 1 \rangle \perp s \langle 1, -\alpha \rangle)^i,$$

para todo inteiro positivo i, pois $\langle 1, \alpha \rangle . \langle 1, -\alpha \rangle = 0$ em $\mathcal{W}(A)$. Mas $b = \langle 1 \rangle \perp s \langle 1, -\alpha \rangle \in \mathcal{P}_{\sigma,p}$, pois $\sigma(b) = p$. Assim, $\langle 1, \alpha \rangle \in (\mathcal{P}_{\sigma,p})^i$, o que mostra que $\mathcal{P}_\sigma \subseteq (\mathcal{P}_{\sigma,p})^i$. Desde que $p^i \langle 1 \rangle \in (\mathcal{P}_{\sigma,p})^i$, obtemos

$$\mathcal{P}_{\sigma,p^i} = \mathcal{P}_\sigma + p^i \langle 1 \rangle . \mathcal{W}(A) \subseteq (\mathcal{P}_{\sigma,p})^i,$$

o que mostra o lema. ∎

Teorema 4.7 *Sejam* $\mathcal{J} \subseteq \mathcal{W}(A)$ *um ideal,* p *um número primo ímpar e* $\sigma \in \mathcal{A}ss(A)$. *Então* $\mathcal{J}$ *é* $\mathcal{P}_{\sigma,p}$*-primário se, e somente se* $\mathcal{J} = (\mathcal{P}_{\sigma,p})^i$, *para algum inteiro* $i \geq 1$.

Dem.: Se $\mathcal{J} = (\mathcal{P}_{\sigma,p})^i$, para algum $i \geq 1$, então do lema anterior temos que $\mathcal{J} = \mathcal{P}_{\sigma,p^i}$. Seja $s : \mathcal{W}(A) \longrightarrow \mathbb{Z}/p^i\mathbb{Z}$ o homomorfismo sobrejetor de anéis obtido pela composta da assinatura σ com a projeção canônica $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/p^i\mathbb{Z}$, ou seja, $s(b) = \sigma(b) + p^i\mathbb{Z}$, para todo $b \in \mathcal{W}(A)$. Então $\dfrac{\mathcal{W}(A)}{\mathrm{Ker}(s)} \cong \dfrac{\mathbb{Z}}{p^i\mathbb{Z}}$ que é um anel onde cada divisor de zero é nilpotente o que mostra que $\mathrm{Ker}(s)$ é um ideal primário de $\mathcal{W}(A)$. Mas $\mathrm{Ker}(s) = \{b \in \mathcal{W}(A);\ s(b) = 0\} = \mathcal{P}_{\sigma,p^i}$. Logo $\mathcal{P}_{\sigma,p^i}$ é um ideal primário de $\mathcal{W}(A)$ para cada $\sigma \in \mathcal{A}ss(A)$, p número primo ímpar e $i \geq 1$ inteiro. Mais ainda, do lema anterior, temos que $r(\mathcal{P}_{\sigma,p^i}) = r((\mathcal{P}_{\sigma,p})^i) = \mathcal{P}_{\sigma,p}$, ou seja $\mathcal{P}_{\sigma,p^i}$ é $\mathcal{P}_{\sigma,p}$-primário.

Reciprocamente, seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal $\mathcal{P}_{\sigma,p}$-primário. Neste caso, temos que $\mathcal{P}_\sigma \subseteq \mathcal{J}$. De fato, dado $\alpha \in A^*$, com $\sigma(\langle \alpha \rangle) = -1$, temos que

$b = \langle 1 \rangle \perp s\langle 1, -\alpha \rangle \in \mathcal{P}_{\sigma,p}$, para $s = \dfrac{p-1}{2}$. Então, $b^m \in \mathcal{J}$ para algum inteiro positivo m, pois $\mathcal{P}_{\sigma,p} = \tau(\mathcal{J})$. Agora, como na demonstração do lema **(4.6)**, $\langle 1, \alpha \rangle = (1, \alpha).b^m \in \mathcal{J}$, o que mostra que de fato $\mathcal{P}_\sigma \subseteq \mathcal{J}$, quando $\mathcal{J}$ é $\mathcal{P}_{\sigma,p}$-primário.

Desde que $\mathcal{P}_\sigma \subseteq \mathcal{J}$, temos uma sobrejeção canônica $\pi : \dfrac{\mathcal{W}(A)}{\mathcal{P}_\sigma} \longrightarrow \dfrac{\mathcal{W}(A)}{\mathcal{J}}$. Mais ainda, dado $\sigma \in \mathcal{A}ss\,(A)$, temos que $\sigma : \mathcal{W}(A) \longrightarrow \mathbb{Z}$ é um homomorfismos sobrejetor de anéis que induz um isomorfismo $\overline{\sigma} : \dfrac{\mathcal{W}(A)}{\mathcal{P}_\sigma} \longrightarrow \mathbb{Z}$. Assim, obtemos uma seqüência de homomorfismos de anéis

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

onde τ é o isomorfismo inverso de $\overline{\sigma}$, isto é, $\tau(n) = n\langle 1 \rangle + \mathcal{P}_\sigma$, para todo $n \in \mathbb{Z}$. Claramente $\pi \circ \tau$ é sobrejetor e, com isso, temos que $\dfrac{\mathcal{W}(A)}{\mathcal{J}} \cong \dfrac{\mathbb{Z}}{\mathrm{Ker}\,(\pi \circ \tau)}$.

Usando o fato que um ideal não nulo $\mathcal{J}$ é um ideal primário de $\mathcal{W}(A)$ se, e somente se os divisores de zero de $\dfrac{\mathcal{W}(A)}{\mathcal{J}}$ são nilpotentes, juntamente com o isomorfismo acima, obtemos que $\mathrm{Ker}\,(\pi \circ \tau)$ é um ideal primário de $\mathbb{Z}$. Mais ainda, como $p\langle 1 \rangle \in \mathcal{P}_{\sigma,p} = \tau(\mathcal{J})$, temos que $p^k \langle 1 \rangle \in \mathcal{J}$ para algum inteiro positivo k e, consequentemente, p^k está em $\mathrm{Ker}\,(\pi \circ \tau)$ o que mostra que $\mathrm{Ker}\,(\pi \circ \tau)$ é um ideal primário de $\mathbb{Z}$ que contém uma potência de p, ou seja, $\mathrm{Ker}\,(\pi \circ \tau) = p^i\,\mathbb{Z}$ para algum inteiro $i \geq 1$. Observe que $p^k \in p^i\,\mathbb{Z}$ e, portanto, $i \geq k$, o que mostra que $p^i \langle 1 \rangle \in \mathcal{J}$.

Temos agora os isomorfismos de anéis

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

onde o segundo isomorfismo é o isomorfismo encontrado no início da demonstração.

Finalmente observamos que $\mathcal{P}_{\sigma,p^i} = \mathcal{P}_\sigma + (p^i\langle 1 \rangle)$, onde $(p^i\langle 1 \rangle)$ denota o ideal principal de $\mathcal{W}(A)$ gerado pelo elemento $p^i\langle 1 \rangle$. Assim, $\mathcal{P}_{\sigma,p^i} \subseteq \mathcal{J}$ que, juntamente com o isomorfismo $\dfrac{\mathcal{W}(A)}{\mathcal{J}} \cong \dfrac{\mathcal{W}(A)}{\mathcal{P}_{\sigma,p^i}}$, mostra que $\mathcal{J} = \mathcal{P}_{\sigma,p^i}$, como queríamos. ■

Resumimos estes resultados em

Teorema 4.8 *Se A é um anel semilocal formalmente real, então os ideais primários de $\mathcal{W}(A)$ são:*

(i) *Os $\mathcal{P}_\sigma$, para $\sigma \in Ass(A)$ são os $\mathcal{P}_\sigma$-primários;*

(ii) *Os $(\mathcal{P}_{\sigma,p})^i$, para $\sigma \in Ass(A)$, p um número primo ímpar e $i \geq 1$, são os $\mathcal{P}_{\sigma,p}$-primários;*

(iii) *Os ideais contendo $2^k\langle 1\rangle$, para algum inteiro $k \geq 1$, são todos os $\mathcal{J}(A)$-primários.*

4.2 Decomposição Primária em $\mathcal{W}(A)$

Um resultado clássico de álgebra comutativa, ver por exemplo **(7.13)** de **[01]**, diz que num anel noetheriano todo ideal admite uma decomposição primária, ou seja, é decomponível. Nesta seção, veremos que para anéis de Witt, vale um resultado mais forte, mais precisamente, apresentaremos condições necessárias e suficientes sobre o anel semilocal A para que todo ideal de $\mathcal{W}(A)$ seja decomponível e, existem muitos tais anéis de Witt que não são noetherianos, como por exemplo, os aneis de Witt de corpos globais, ver **[10]**. Antes de apresentarmos tal resultado, apresentaremos um refinamento do teorema de unicidade **(1.9)**, para o caso do anel de Witt de um anel semilocal formalmente real A.

Nesta seção, continuaremos assumindo que A é um anel semilocal formalmente real. O próximo resultado, de verificação imediata, será frequentemente usado nas demonstrações que seguem.

Lema 4.9 *Se σ, $\tau \in Ass(A)$ são distintas, então existe $\alpha \in A^*$ tal que $\sigma(\langle\alpha\rangle) = 1$ e $\tau(\langle\alpha\rangle) = -1$.*

Dem.: Imediata. ∎

Seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal. Recordemos que o conjunto dos ideais primos associados de $\mathcal{J}$, $Assoc(\mathcal{J})$, é precisamente o conjunto dos ideais primos que ocorrem como radicais de ideais da forma $(\mathcal{J} : b.\mathcal{W}(A))$, com $b \in \mathcal{W}(A)$. O próximo resultado caracteriza quando $\mathcal{I}(A)$ e/ou $\mathcal{P}_\sigma$, com $\sigma \in Ass(A)$, são ideais primos associados de $\mathcal{J}$.

Proposição 4.10 *Sejam $\mathcal{I} \subseteq \mathcal{W}(A)$ um ideal e $\sigma \in Ass(A)$. Temos então*

(i) *$\mathcal{I}(A) \in Assoc(\mathcal{J})$ se, e somente se existe $b \in \mathcal{W}(A) - \mathcal{J}$, tal que $2^k b \in \mathcal{J}$, para algum inteiro positivo k.*

(ii) *Se $\mathcal{J}$ é decomponível, então $\mathcal{P}_\sigma \in Assoc(\mathcal{J})$ se, e somente se $\mathcal{J} \subseteq \mathcal{P}_\sigma$.*

Dem.: Temos que $\mathcal{I}(A) \in Assoc(\mathcal{I})$ se, e somente se existe $b \in \mathcal{W}(A) - \mathcal{J}$ tal que $(\mathcal{J} : b.\mathcal{W}(A))$ é $\mathcal{I}(A)$-primário. Mas, de **(4.3)**, temos que isto ocorre se, e somente se $2^k \langle 1 \rangle \in (\mathcal{J} : b.\mathcal{W}(A))$ para algum inteiro positivo k. Assim $\mathcal{I}(A) \in Assoc(\mathcal{J})$ se, e somente se existe $b \in \mathcal{W}(A) - \mathcal{J}$ tal que $2^k b = 2^k \langle 1 \rangle \cdot b \in \mathcal{J}$, para algum inteiro positivo k, o que mostra (i).

Para mostrarmos **(ii)**, suponhamos que $\mathcal{J} \subseteq \mathcal{W}(A)$ é um ideal decomponível.

Se $\mathcal{P}_\sigma \in Assoc(\mathcal{J})$, então de **(1.8)** e da definição de $Assoc(\mathcal{J})$, temos que $\mathcal{J}$ está contido em algum ideal $\mathcal{P}_\sigma$-primário. Consequentemente, de **(4.8)**, temos que $\mathcal{J} \subseteq \mathcal{P}_\sigma$. Reciprocamente, seja $\mathcal{J} \subseteq \mathcal{P}_\sigma$. Suponhamos que $\mathcal{P}_\sigma \notin Assoc(\mathcal{J})$. Então, usando **(4.8)** e o fato de $\mathcal{J}$ ser decomponível, temos que $\mathcal{J}$ admite uma decomposição primária da forma

$$\mathcal{J} = \left(\bigcap_{\tau \in \Gamma} \mathcal{P}_\tau \right) \cap \left(\bigcap_{\gamma \in \Delta} \left(\bigcap_{p \in \Delta_\gamma} \mathcal{P}_{\gamma, p^{i(\gamma,p)}} \right) \right) \cap Q,$$

onde Γ, Δ são subconjuntos finitos de $Ass(A)$, com $\sigma \notin \Gamma$ e, para cada $\gamma \in \Delta$, Δ_γ é um conjunto finito de números primos ímpares, $i(\gamma, p)$ é um inteiro ≥ 1 para cada $\gamma \in \Delta$ e $p \in \Delta_\gamma$, e Q é um ideal $\mathcal{I}(A)$-primário de $\mathcal{W}(A)$ ou $Q = \mathcal{W}(A)$.

Seja $m_1 = \prod_{\gamma \in \Delta} \left(\prod_{p \in \Delta_\gamma} p^{i(\gamma,p)} \right)$. Usando **(4.3)** se necessário, podemos afirmar que existe um inteiro positivo m_2 tal que $2^{m_2} \langle 1 \rangle \in Q$. Seja $m = 2^{m_2} m_1 \in \mathbb{Z}$. Agora, desde

que $\sigma \notin \Gamma$, do lema anterior, temos que para cada $\tau \in \Gamma$, existe $\alpha_\tau \in A^*$ tal que $\sigma(\langle \alpha_\tau \rangle) = 1$ e $\tau(\langle \alpha_\tau \rangle) = -1$. Considere

$$b = m \prod_{\tau \in \Gamma} \langle 1, \alpha_\tau \rangle \in \mathcal{W}(A).$$

Pela escolha de m_1 e m_2 feita acima, temos que $b \in Q$ e $b \in \mathcal{P}_{\gamma, p^{i(\gamma,p)}}$, para todo $\gamma \in \Delta$ e $p \in \Delta_\gamma$. Mais ainda, da escolha de $\alpha_\tau \in A^*$, temos que $b \in \mathcal{P}_\tau$, para todo $\tau \in \Gamma$, ou seja,

$$b \in \left(\bigcap_{\tau \in \Gamma} \mathcal{P}_\tau \right) \cap \left(\bigcap_{\gamma \in \Delta} \left(\bigcap_{p \in \Delta_\gamma} \mathcal{P}_{\gamma, p^{i(\gamma,p)}} \right) \right) = \mathcal{J}.$$

Mas $\sigma(b) = 2m \neq 0$, o que contradiz a hipótese de $\mathcal{J} \subseteq \mathcal{P}_\sigma$. Logo $\mathcal{P}_\sigma \in Assoc(\mathcal{J})$, como queríamos. ■

Teorema 4.11 *Seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal com uma decomposição primária reduzida $Q_1 \cap Q_2 \cap \ldots \cap Q_n$.*

(i) *Se $r(Q_i) = \mathcal{P}_\sigma$ ou $\mathcal{P}_{\sigma,p}$, para algum $\sigma \in Ass(A)$ e p um primo ímpar, então Q_i é unicamente determinado, isto é, Q_i aparece em toda decomposição primária reduzida de $\mathcal{J}$.*

(ii) *Todos Q_i's são unicamente determinados se $\mathcal{J} \not\subseteq \mathcal{P}_\sigma$, para todo $\sigma \in Ass(A)$ ou $2^k b \notin \mathcal{J}$ para todo $b \notin \mathcal{J}$ e todo inteiro positivo k.*

Dem.: De **(1.9)** temos que, para mostrarmos (i), é suficiente provarmos que $r(Q_i)$ é um elemento minimal em $Assoc(\mathcal{J})$.

Se $r(Q_i) = \mathcal{P}_\sigma$, para algum $\sigma \in Ass(A)$, então de **(3.15)** temos que $r(Q_i)$ é um elemento minimal em $\mathcal{W}(A)$. Consequentemente, também o é em $Assoc(\mathcal{J})$. Se $r(Q_i) = \mathcal{P}_{\sigma,p}$, para algum $\sigma \in Ass(A)$ e p primo ímpar, e $r(Q_i)$ não é minimal em $Assoc(\mathcal{J})$, então de **(3.15)** temos que $\mathcal{P}_\sigma$ também é associado de $\mathcal{J}$. Trocando a ordem, se necessário, de **(4.8)** podemos assumir que $Q_1 = \mathcal{P}_{\sigma,p^i}$, para algum inteiro $i \geq 1$ e

$Q_2 = \mathcal{P}_\sigma$. Assim, $(Q_1 \cap Q_2) \subseteq \mathcal{P}_\sigma \subseteq Q_1$ o que contradiz o fato de $Q_1 \cap \ldots \cap Q_n$ ser uma decomposição primária reduzida de $\mathcal{J}$. Consequentemente, se $\mathcal{P}_{\sigma,p} \in Assoc(\mathcal{J})$, então ele é minimal em $Assoc(\mathcal{J})$, o que completa a demonstração de (i).

Suponhamos agora que Q_i não é unicamente determinado, para algum $i = 1, \ldots, n$. Então, de **(1.9)**, temos que $Assoc(\mathcal{J})$, tem um elemento que não é minimal. Do ítem (i) acima, temos que isto ocorre somente se existe $\sigma \in Ass(A)$, tal que $\mathcal{I}(A)$ e $\mathcal{P}_\sigma$ estão ambos em $Assoc(\mathcal{J})$. Assim, $\mathcal{J} \subseteq \mathcal{P}_\sigma$, para algum $\sigma \in Ass(A)$ e, de **(4.10)**, existe $b \in \mathcal{W}(A) - \mathcal{J}$ tal que $2^k b \in \mathcal{J}$, para algum inteiro positivo k, o que mostra a negação de (ii). ■

Para apresentarmos condições necessárias e suficientes para que cada ideal do anel de Witt seja decomponível, necessitaremos de dois resultados auxiliares.

Lema 4.12 *Sejam $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ ideais de um anel R, com $\mathfrak{C} \subseteq \mathfrak{B}$. Então $\mathfrak{C} = \mathfrak{B} \cap (\mathfrak{C}+\mathfrak{D})$ se, e somente se $(\mathfrak{B} \cap \mathfrak{D}) \subseteq \mathfrak{C}$.*

Dem.: Se $\mathfrak{C} = \mathfrak{B} \cap (\mathfrak{C} + \mathfrak{D})$ e $x \in \mathfrak{B} \cap \mathfrak{D}$, então claramente x está em $\mathfrak{B} \cap (\mathfrak{C} + \mathfrak{D}) = \mathfrak{C}$. Reciprocamente, se $\mathfrak{B} \cap \mathfrak{D} \subseteq \mathfrak{C}$, como $\mathfrak{C} \subseteq \mathfrak{B}$ e $\mathfrak{C} \subseteq (\mathfrak{C} + \mathfrak{D})$, temos que $\mathfrak{C} \subseteq (\mathfrak{B} \cap (\mathfrak{C} + \mathfrak{D}))$. Agora, dado $x \in (\mathfrak{B} \cap (\mathfrak{C} + \mathfrak{D}))$, podemos escrever $x = y + z$, com $y \in \mathfrak{C}$ e $z \in \mathfrak{D}$. Temos então $z = x - y$, onde $x \in \mathfrak{B}$ e $y \in \mathfrak{C} \subseteq \mathfrak{B}$, ou seja, $z \in \mathfrak{B} \cap \mathfrak{D} \subseteq \mathfrak{C}$. Assim $x = y + z \in \mathfrak{C}$, o que conclui a demonstração. ■

Lema 4.13 *Sejam m um inteiro positivo e A um anel semilocal tal que $Ass(A)$ tem $m+1$ elementos. Então para todo $\sigma \in Ass(A)$ existe uma forma bilinear $b_\sigma \in Bil(A)$, tal que $\sigma(b_\sigma) = 2^m$ e $\tau(b_\sigma) = 0$, para toda assinatura $\tau \in Ass(A)$ com $\tau \neq \sigma$.*

Dem.: Dado $\sigma \in Ass(A)$ fixo, para cada uma das m assinaturas τ de A distintas de σ, do lema **(4.9)** podemos encontrar $\alpha_\tau \in A^*$ tal que $\sigma(\langle \alpha_\tau \rangle) = 1$ e $\tau(\langle \alpha_\tau \rangle) = -1$.

Consideremos $b_\sigma = \prod_{\tau \neq \sigma} \langle 1, \alpha_\tau \rangle \in \mathcal{B}il\,(A)$. Temos então

$$\sigma(b_\sigma) = \prod_{\tau \neq \sigma} \sigma(\langle 1, \alpha_\tau \rangle) = \prod_{\tau \neq \sigma} (1+1) = 2^m \text{ e } \tau(b_\sigma) = \prod_{\tau \neq \sigma} \tau(\langle 1, \alpha_\tau \rangle) = \prod_{\tau \neq \sigma} (1-1) = 0,$$

como queríamos. ■

Dado um inteiro positivo $n \geq 2$ e $\sigma \in \mathcal{A}ss\,(A)$, denotamos por

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

É facil ver que se $n = p_1^{i_1} \ldots p_k^{i_k}$, com $p_1, \ldots, p_k$ números primos distintos, então $\mathcal{P}_{\sigma,n} = \bigcap_{j=1}^{k} (\mathcal{P}_{\sigma,p_j})^{i_j}$. Para formalizar a notação, escrevemos $\mathcal{P}_{\sigma,0} = \mathcal{P}_\sigma$ e $\mathcal{P}_{\sigma,1} = \mathcal{W}(A)$.

Dado um anel semilocal A, sabemos de **(3.18)** e **(3.22)** que A tem somente 2-torção. Assim, faz sentido definirmos a *altura de* A, como sendo $h(A) = 2^m$, onde $m = \min\{k \in \mathbb{Z};\ k \geq 0 \text{ e } 2^k\,\mathcal{W}_t\,(A) = 0\}$ se tal número inteiro existir, caso contrário diremos que A tem altura infinita e escrevemos $h(A) = \infty$. Com esta noção temos

Teorema 4.14 *Todo ideal de $\mathcal{W}(A)$ é decomponível se,e somente se A tem altura finita e $\mathcal{A}ss\,(A)$ é um conjunto finito.*

Dem.: Suponhamos inicialmente que A é um anel semilocal com $h(A) \leq 2^k$ e $\mathcal{A}ss\,(A) = \{\sigma_0, \sigma_1, \ldots, \sigma_m\}$.

Seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal próprio. Queremos mostrar que $\mathcal{J}$ é decomponível. Para tanto, para cada $i = 0, 1, \ldots, m$, considere $\mathfrak{B}_i = \{\sigma_i(b);\ b \in \mathcal{J}\} \subseteq \mathbb{Z}$. É fácil ver que $\mathfrak{B}_i$ é um ideal de $\mathbb{Z}$, gerado por digamos $2^{r_i}\,n_i$, com $r_i \geq 0$ e n_i um inteiro ímpar ou $n_i = 0$. Sejam $b_i' \in \mathcal{J};\ i = 0, 1, \ldots, m$, tais que $\sigma_i(b_i') = 2^{r_i}\,n_i$. Para $r = \max\{r_0, r_1, \ldots, r_m\}$ e $b_i = 2^{r-r_i}\,b_i'$, $i = 0, 1, \ldots, m$, vamos mostrar que

$$\mathcal{J} = \left(\bigcap_{i=0}^{m} \mathcal{P}_{\sigma_i,n_i}\right) \cap \left(\mathcal{J} + 2^{k+m+r}\,\mathcal{W}(A)\right).$$

Se $b \in \mathcal{J}$, então para cada $i = 0, 1, \ldots, m$, temos que $\sigma_i(b) \in \mathfrak{B}_i$, o que implica que $\sigma_i(b)$ é um múltiplo de $2^{r_i} n_i$ e portanto, $\sigma_i(b) \equiv 0 \bmod n_i$. Assim $b \in \mathcal{P}_{\sigma_i,n_i}$, o que mostra que $\mathcal{J} \subseteq \left(\bigcap_{i=0}^{m} \mathcal{P}_{\sigma_i,n_i}\right)$. Agora, considerando $\mathfrak{B} = \bigcap_{i=0}^{m} \mathcal{P}_{\sigma_i,n_i}$, $\mathfrak{C} = \mathcal{J}$ e $\mathfrak{D} = 2^{k+m+r}\,\mathcal{W}(A)$ no lema **(4.12)**, temos que é suficiente mostrar que

$$\left(\bigcap_{i=0}^{m} \mathcal{P}_{\sigma_i,n_i}\right) \cap \left(2^{k+m+r}\,\mathcal{W}(A)\right) \subseteq \mathcal{J}.$$

Seja $b \in \left(\bigcap_{i=0}^{m} \mathcal{P}_{\sigma_i,n_i}\right) \cap \left(2^{k+m+r}\,\mathcal{W}(A)\right)$. Escrevendo $b = 2^{k+m+r}\,b_0$, com $b_0 \in \mathcal{W}(A)$, temos que $\sigma_i(b) = 2^{k+m+r}\,\sigma_i(b_0) \equiv 0 \bmod n_i$, para cada $i = 0, 1, \ldots, m$. Desde que n_i é ímpar ou zero, temos que $\sigma_i(b_0) = s_i\, n_i$, para algum inteiro s_i. Do lema anterior temos que, para cada $i = 0, 1, \ldots, m$, existe uma forma bilinear q_i tal que $\sigma_i(q_i) = 2^m$ e $\sigma_j(q_i) = 0$ se $j \neq i$.

Considere $b' = \perp_{i=0}^{m} s_i\, q_i \cdot b_i$. Observe que $b' \in \mathcal{J}$, pois cada $b_i \in \mathcal{J}$. Mais ainda, da construção dos b_i's, temos que para cada $i = 0, 1, \ldots, m$,

$$\sigma_i(b') = \sum_{j=0}^{m} s_j\,\sigma_i(q_j)\,\sigma_i(b_j) = s_i\,2^m\,\sigma_i(2^{r-r_i}\,b_i') = 2^{m+r}\,s_i\,n_i.$$

Logo $2^{m+r}\,b_0 - b' \in \mathcal{W}(A)$ é tal que $\sigma_i(2^{m+r}\,b_0 - b') = 0$, para todo $i = 0, 1, \ldots, m$, o que implica que $2^{m+r}\,b_0 - b' \in$
$mathscrW_t(A)$ pelo Princípio Local-Global de Pfister. Assim, desde que $h(A) \leq 2^k$, obtemos $b - 2^k\,b' = 2^k\,(2^{m+r}\,b_0 - b') = 0$, ou seja, $b = 2^k\,b' \in \mathcal{J}$. Consequentemente, da definição de $\mathcal{P}_{\sigma_i,n_i}$ e de **(4.6)** e **(4.8)** temos que

$$\left(\bigcap_{i=0}^{m} P_{\sigma_i,n_i}\right) \cap \left(\mathcal{J} + 2^{k+m+r}\,\mathcal{W}(A)\right)$$

é uma decomposição primária de $\mathcal{J}$.

Para a recíproca, consideremos que A é um anel semilocal tal que todo ideal de $\mathcal{W}(A)$ é decomponível. Queremos mostrar que $h(A) < \infty$ e $Ass\,(A)$ é um conjunto finito.

Suponhamos que A admita infinitas assinaturas. Considere o ideal de torção $\mathcal{W}_t(A)$ que por hipótese é decomponível. Logo $\mathcal{W}_t(A)$ se escreve como uma intersecção finita de ideais primários de $\mathcal{W}(A)$. Do Princípio Local-Global de Pfister, temos que $\mathcal{W}_t(A) \subseteq \mathcal{P}_\sigma$, para toda $\sigma \in Ass(A)$. Como, $\mathcal{P}_\sigma \subseteq \mathcal{P}_{\sigma,p^i}$, podemos assumir que nenhum ideal primário da forma $\mathcal{P}_{\sigma,p^i}$, onde $\sigma \in Ass(A)$, p primo ímpar e $i \geq 1$, ocorre na decomposição de $\mathcal{W}_t(A)$. Assim, usando **(4.8)**, temos que existem $\sigma_1, \ldots, \sigma_l \in Ass(A)$ tais que

$$\mathcal{W}_t(A) = \left(\bigcap_{i=1}^{l} \mathcal{P}_{\sigma_i}\right) \cap Q,$$

onde Q é um ideal $\mathcal{I}(A)$-primário, ou $Q = \mathcal{W}(A)$. De **(4.3)** temos que existe um inteiro positivo r tal que $2^r\langle 1\rangle \in Q$ e, como $Ass(A)$ é um conjunto infinito, existe $\gamma \in Ass(A)$, com $\gamma \neq \sigma_i$, para todo $i = 1, \ldots, l$. Para cada $i = 1, \ldots, l$, considere $\alpha_i \in A^*$ tal que $\gamma(\langle\alpha_i\rangle) = 1$ e $\sigma_i(\langle\alpha_i\rangle) = -1$, que existem pelo lema **(4.9)**. Tomando $b = 2^r\langle 1, \alpha_1\rangle \otimes (1, \alpha_2\rangle \otimes \ldots \otimes \langle 1, \alpha_l\rangle$, temos que $b \in \left(\bigcap_{i=1}^{l} \mathcal{P}_{\sigma_i}\right) \cap Q = \mathcal{W}_t(A)$. Mas $\gamma(b) = 2^{r+l} \neq 0$, o que contradiz o Princípio Local-Global de Pfister. Consequentemente, se todo ideal de $\mathcal{W}(A)$ é decomponível, então $Ass(A)$ é um conjunto finito.

Finalmente, suponhamos que $Ass(A)$ é um conjunto finito e $h(A) = \infty$. Como $h(A) = \infty$, temos que $\mathcal{W}_t(A) \neq 0$. Seja $b \in \mathcal{W}_t(A)$, com $b \neq 0$. O ideal principal $\mathfrak{B} = b \cdot \mathcal{W}(A)$ está contido em $\mathcal{P}_\sigma$, para toda $\sigma \in Ass(A)$. Assim, de **(4.8)** podemos assumir que $\mathfrak{B}$ tem uma decomposição primária da forma

$$\mathfrak{B} = \left(\bigcap_{\sigma \in Ass(A)} \mathcal{P}_\sigma\right) \cap Q,$$

onde Q é $\mathcal{I}(A)$-primário ou $Q = \mathcal{W}(A)$. Agora, como b é um elemento de torção de $\mathcal{W}(A)$, de **(3.22)** temos que existe um inteiro $m \geq 1$ tal que $2^m b = 0$. Mais ainda, de **(4.3)** temos que existe um inteiro positivo k tal que $2^k\langle 1\rangle \in Q$. Logo o ideal Q contém os ideais $\mathfrak{B}$ e $2^k\mathcal{W}(A)$ e, sem perda de generalidade, podemos assumir $k \geq m$.

Temos então

$$\mathfrak{B} \subseteq \left(\bigcap_{\sigma \in Ass(A)} \mathcal{P}_\sigma \right) \cap (\mathfrak{B} + (2^k \mathcal{W}(A))) \subseteq \left(\bigcap_{\sigma \in Ass(A)} \mathcal{P}_\sigma \right) \cap Q = \mathfrak{B},$$

ou seja,

$$\mathfrak{B} = \left(\bigcap_{\sigma \in Ass(A)} \mathcal{P}_\sigma \right) \cap (\mathfrak{B} + 2^k \mathcal{W}(A)) = \mathcal{W}_t(A) \cap (\mathfrak{B} + 2^k \mathcal{W}(A)),$$

onde a última igualdade segue do Princípio Local-Global de Pfister. Em particular, temos $2^k \mathcal{W}_t(A) = \mathcal{W}_t(A) \cap (2^k \mathcal{W}(A)) \subseteq \mathfrak{B}$.

Agora, desde que $h(A) = \infty$, temos que existe $b_0 \in \mathcal{W}_t(A)$ tal que $2^{2k} b_0 \neq 0$ em $\mathcal{W}(A)$. Mas $2^k b_0 \in 2^k \mathcal{W}_t(A) \subseteq \mathfrak{B} = b.\mathcal{W}(A)$. Então $2^k b_0 = b.b_1$, para algum $b_1 \in \mathcal{W}(A)$, o que implica que $2^{2k} b_0 = 2^k b.b_1 = 0$, o que é uma contradição. Portanto, $h(A) < \infty$ o que completa a demonstração do teorema. ■

4.3 Ideais contendo uma forma de dimensão ímpar

Nesta seção assumiremos que A é um anel semilocal formalmente real, com $h(A) < \infty$ e com um conjunto finito de assinaturas. Sob tais condições apresentaremos alguns resultados sobre ideais de $\mathcal{W}(A)$ que contém uma forma de dimensão ímpar, ou seja, ideais que não estão contidos em $\mathcal{J}(A)$. Encontraremos também condições equivalentes para que formas de dimensão ímpar tenham fatoração única como produto de irredutíveis.

Seja $\mathcal{J} \subseteq \mathcal{W}(A)$ um ideal contendo uma forma de dimensão ímpar. Desde que, de **(3.15)**, $\mathcal{P}_\sigma \subseteq \mathcal{J}(A)$, para todo $\sigma \in Ass(A)$ e $\mathcal{J} \not\subseteq \mathcal{J}(A)$, temos que $\mathcal{J} \not\subseteq \mathcal{P}_\sigma$, para todo $\sigma \in Ass(A)$. Usando a caracterização dos ideais primários de $\mathcal{W}(A)$, apresentada em **(4.8)**, temos que $\mathcal{J}$ pode ser escrito como uma intersecção finita de ideais da forma $\mathcal{P}_{\sigma,p^i}$, com $\sigma \in Ass(A)$, p primos ímpares e $i \geq 1$. Além disso, de **(4.11)**, temos que esta decomposição primária reduzida é unicamente determinada.

Proposição 4.15 *Se $\mathcal{J} \subseteq \mathcal{W}(A)$ é um ideal contendo uma forma de dimensão ímpar então, para todo $b \in \mathcal{W}(A) - \mathcal{J}$, temos que $2^k b \notin \mathcal{J}$, para todo inteiro $k \geq 0$.*

Dem.: Desde que todo ideal primário está contido em seu radical e $\mathcal{J} \not\subseteq \mathfrak{I}(A)$, temos que nenhum ideal $\mathfrak{I}(A)$-primário de $\mathcal{W}(A)$ está contido em $\mathcal{J}$. Assim, da definição de $Assoc(\mathcal{J})$, temos que $\mathfrak{I}(A) \notin Assoc(\mathcal{J})$. Agora, a demonstração segue de **(4.10)**. ■

Proposição 4.16 *Se $\mathcal{J}$ é um ideal de $\mathcal{W}(A)$ contendo uma forma de dimensão ímpar, então $\mathcal{W}_t(A) \subseteq \mathcal{J}$.*

Dem.: Pelo Princípio Local-Global de Pfister, obtemos que $\mathcal{W}_t(A) \subseteq \mathcal{P}_{\sigma,p^i}$, para todo $\sigma \in Ass(A)$, p primo ímpar e $i \geq 1$. Logo, o resultado segue da observação feita no início desta seção. ■

Proposição 4.17 *Se b_1 e b_2 são formas bilineares de dimensão ímpar tais que $b_1 - b_2 \in \mathcal{W}_t(A)$, então os ideais principais $b_1.\mathcal{W}(A)$ e $b_2.\mathcal{W}(A)$ são iguais.*

Dem.: Como $b_1 - b_2 \in \mathcal{W}_t(A)$, pelo Principio Local-Global de Pfister, temos que $\sigma(b_1) = \sigma(b_2)$, para todo $\sigma \in Ass(A)$. Assim, para todo primo ímpar p, $b_1 \in \mathcal{P}_{\sigma,p^i}$ se, e somente se $b_2 \in \mathcal{P}_{\sigma,p^i}$, onde $\sigma \in Ass(A)$ e $i \geq 1$. Consequentemente, os ideais primários que aparecem nas decomposições primárias reduzidas dos ideais $b_1.\mathcal{W}(A)$ e $b_2.\mathcal{W}(A)$ são os mesmos e, portanto, $b_1.\mathcal{W}(A) = b_2.\mathcal{W}(A)$. ■

Dados $\alpha_1, \alpha_2, \ldots, \alpha_n \in A^*$, dizemos que a forma bilinear não singular

$$b = \langle 1, \alpha_1 \rangle \otimes \langle 1, \alpha_2 \rangle \otimes \ldots \otimes \langle 1, \alpha_n \rangle$$

é uma n-forma de Pfister e, denotamos por $b = \langle\langle \alpha_1, \ldots, \alpha_n \rangle\rangle$. Para $\sigma \in Ass(A)$, temos que $\sigma(\langle \alpha \rangle) = \pm 1$, para cada $\alpha \in A^*$. Assim se b é uma n-forma de Pfister,

então $\sigma(b) = 0$ ou $\sigma(b) = 2^n = \dim(b)$, para cada $\sigma \in Ass(A)$. Mais ainda, se b é uma n-forma de Pfister, então $b = \langle 1 \rangle \perp b'$, para algum $b' \in Bil(A)$. Outra notação que usaremos no próximo resultado é que dado $b \in Bil(A)$, o conjunto dos elementos de A^* representados por b são denotados por $\mathcal{D}(b)$, ou seja, se M é um A-módulo livre de dimensão finita e (M, b) é um espaço bilinear sobre A, então

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

Com estas notações temos a seguinte conseqüência da proposição anterior

Corolário 4.18 *Sejam $b_1 = \langle 1 \rangle \perp b_1'$ e $b_2 = \langle 1 \rangle \perp b_2'$ duas n-formas de Pfister sobre A. Se $\mathcal{D}(b_1') = \mathcal{D}(b_2')$, então existe uma unidade $b \in \mathcal{W}(A)$ tal que $b_1' = b.b_2'$.*

Dem.: Sejam $\alpha_i,\ \beta_i \in A^*,\ i = 1, \ldots, n$, tais que $b_1 = \langle\langle \alpha_1, \ldots, \alpha_n \rangle\rangle$ e $b_2 = \langle\langle \beta_1, \ldots, \beta_n \rangle\rangle$. Dado $\sigma \in Ass(A)$, afirmamos que $\mathcal{D}(b_1') = \mathcal{D}(b_2')$, implica que $\sigma(b_1) = 2^n$ se, e somente se $\sigma(b_2) = 2^n$. De fato, se $\sigma(b_1) = 2^n$ e $\sigma(b_2) = 0$, então temos que $\sigma(\langle\langle \alpha_i \rangle\rangle) = 1$, para todo $i = 1, \ldots, n$ e existe $j \in \{1, \ldots, n\}$ tal que $\sigma(\langle\langle \beta_j \rangle\rangle) = -1$. Mas $\beta_j \in \mathcal{D}(b_2') = \mathcal{D}(b_1')$. Assim, de **(2.8)** temos que existe $b_3 \in Bil(A)$ tal que $b_1' \simeq \langle \beta_j \rangle \perp b_3$. Como $b_1 = \langle 1 \rangle \perp b_1'$ e $\sigma(b_1) = 2^n = \dim(b_1)$, temos que $\sigma(b_1') = 2^n - 1 = \dim(b_1')$. Consequentemente, $\dim(b_1') = \sigma(b_1') = \sigma(\langle \beta_j \rangle \perp b_3) = -1 + \sigma(b_3) \leq \dim(b_3) - 1 = (\dim(b_1') - 1) - 1 < \dim(b_1')$, o que é uma contradição.

Usando o fato que $\sigma(b_i) = 1 + \sigma(b_i')$, para $i = 1, 2$ e $\sigma \in Ass(A)$, e a afirmação acima, temos que, para cada $\sigma \in Ass(A)$, $\sigma(b_1') = \sigma(b_2')$, o que mostra que $b_1' - b_2'$ está em $\mathcal{W}_t(A)$ pelo Princípio Local-Global de Pfister. Como $\dim(b_i') = 2^n - 1$ é ímpar, para $i = 1, 2$ temos da proposição anterior que $b_1'.\mathcal{W}(A) = b_2'.\mathcal{W}(A)$, ou seja, existe um elemento inversível $b \in \mathcal{W}(A)$ tal que $b_1' = b.b_2'$, como queríamos. ■

Observação 4.19 Ainda é um problema em aberto se as hipóteses de **(4.18)**, de fato implicam que $b_1 \simeq b_2$.

O próximo teorema mostra condições equivalentes para que os ideais de $\mathcal{W}(A)$ que não estão contidos em $\mathcal{I}(A)$ sejam ideais principais.

Teorema 4.20 *As seguintes afirmações são equivalentes:*

(i) $\mathcal{P}_{\sigma,3}$ *é um ideal principal, para todo* $\sigma \in Ass(A)$;

(ii) *Para cada* $\sigma \in Ass(A)$, *existe uma forma bilinear* b *sobre* A, *tal que* $\sigma(b) = 3$ *e* $\tau(b) = -1$, *para todo* $\tau \in Ass(A)$, *com* $\tau \neq \sigma$;

(iii) *Para cada* $\sigma \in Ass(A)$, *existe uma forma bilinear* b *sobre* A, *tal que* $\sigma(b) = 4$ *e* $\tau(b) = 0$, *para todo* $\tau \in Ass(A)$, *com* $\tau \neq \sigma$;

(iv) *Todo ideal de* $\mathcal{W}(A)$ *contendo uma forma de dimensão ímpar é um ideal principal.*

Dem.: É evidente que (iv) $\Longrightarrow$ (i). Mostremos então as implicações (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv).
(i) $\Longrightarrow$ (ii). Dado $\sigma \in Ass(A)$, temos que $\sigma(\mathcal{P}_{\sigma,3}) = 3\mathbb{Z}$. Logo existe um gerador b_1 do ideal principal $\mathcal{P}_{\sigma,3}$ tal que $\sigma(b_1) = 3$. De **(3.15)** temos que $\mathcal{P}_{\sigma,3}$ contém um único ideal primo minimal, que é $\mathcal{P}_\sigma$. Assim, se $\tau \in Ass(A)$ é tal que $\tau \neq \sigma$, então $\mathcal{P}_\tau \not\subseteq \mathcal{P}_{\sigma,3}$ e, como $\mathcal{P}_{\sigma,3}$ é um ideal maximal de $\mathcal{W}(A)$, temos que $\mathcal{P}_{\sigma,3} + \mathcal{P}_\tau = \mathcal{W}(A)$. Usando que $\mathcal{P}_{\sigma,3} = b_1.\mathcal{W}(A)$ e que $\mathcal{P}_\tau = \mathrm{Ker}(\tau)$, temos que $\mathbb{Z} = \tau(\mathcal{W}(A)) = \tau(\mathcal{P}_{\sigma,3}) = \tau(b_1.\mathcal{W}(A)) = \tau(b_1)\mathbb{Z}$, o que mostra que $\tau(b_1) = \pm 1$, para todo $\tau \in Ass(A)$ com $\tau \neq \sigma$.

Agora, do fato que $\sigma(b_1) = 3$, obtemos que $\dim(b_1)$ é ímpar. Usando **(3.3)** e o fato que $\tau(b_1) = \pm 1$ e $\sigma(b_1) = 3$, para cada $\tau \in Ass(A)$, com $\tau \neq \sigma$, temos que $b_1 = \langle \alpha_1, \ldots, \alpha_{2n+1} \rangle$ em $\mathcal{W}(A)$, com $\alpha_i \in A^*$ tais que

$$\tau(\langle \alpha_i \rangle) = \begin{cases} 1 & \text{se } 1 \leq i \leq n \\ -1 & \text{se } n+1 \leq i \leq 2n \\ \tau(b) & \text{se } i = 2n+1 \end{cases}$$

e,

$$\sigma(\langle\alpha_i\rangle) = \begin{cases} -1 & \text{se } 1 \leq i \leq n-1 \\ 1 & \text{se } n \leq i \leq 2n+1. \end{cases}$$

Seja $e = (-1)^n \alpha_1 \dots \alpha_{2n+1} \in A^*$. Então,

$$\tau(\langle e\rangle) = (-1)^n \prod_{i=1}^{2n+1} \tau(\langle\alpha_i\rangle) = (-1)^n (-1)^n \tau(\langle\alpha_{2n+1}\rangle) = \tau(b_1),$$

para cada $\tau \in \mathcal{A}ss(A)$, com $\tau \neq \sigma$ e,

$$\sigma(\langle e\rangle) = (-1)^n \prod_{i=1}^{2n+1} \sigma(\langle\alpha_i\rangle) = (-1)^n (-1)^{n-1} = -1.$$

Assim, $b = \langle -e\rangle \otimes \langle \alpha_1, \alpha_2, \dots, \alpha_{2n+1}\rangle$ é uma forma bilinear não singular sobre A, tal que

$$\sigma(b) = \sigma(\langle -e\rangle) \sum_{i=1}^{2n+1} \sigma(\langle\alpha_i\rangle) = -\sigma(\langle e\rangle)\, 3 = 3$$

e, para cada $\tau \in \mathcal{A}ss(A)$, com $\tau \neq \sigma$,

$$\tau(b) = \tau(\langle -e\rangle) \sum_{i=1}^{2n+1} \tau(\langle\alpha_i\rangle) = -\tau(b_1)^2 = -1,$$

pois $\tau(b_1) = \pm 1$, o que mostra (ii).

(ii) $\Longrightarrow$ (iii). Se b é uma forma bilinear satisfazendo a condição (ii), então $b \perp \langle 1\rangle$ satisfaz (iii).

(iii) $\Longrightarrow$ (iv). Para $\sigma \in \mathcal{A}ss(A)$, seja b_σ a forma bilinear satisfazendo (iii), ou seja, $\sigma(b_\sigma) = 4$ e $\tau(b_\sigma) = 0$, para todo $\tau \in \mathcal{A}ss(A)$, com $\tau \neq \sigma$. Multiplicando b_σ por algum $\alpha \in \mathcal{D}(b_\sigma)$, com $\sigma(\langle\alpha\rangle) = 1$, se necessário, podemos assumir que $1 \in \mathcal{D}(b_\sigma)$. Então, de **(2.8)** temos que $b_\sigma \simeq \langle 1\rangle \perp q_\sigma$, para algum $q_\sigma \in \mathcal{B}il(A)$. Observe que, neste caso, para $\tau \in \mathcal{A}ss(A)$,

$$\tau(q_\sigma) = \begin{cases} 3 & \text{se } \tau = \sigma \\ -1 & \text{se } \tau \neq \sigma \end{cases}$$

Para mostrarmos a conclusão apresentada em (iv), usando a observação feita no início desta seção, é suficiente mostrarmos que os ideais $\mathcal{J} = \bigcap_{i \in \Gamma} \mathcal{P}_{\sigma,p^i}$ são principais, onde Γ é um conjunto finito de pares (σ, p^i), com $\sigma \in Ass(A)$, p primos ímpares e $i \geq 1$ inteiro.

Para cada $\sigma \in Ass(A)$, seja $n_\sigma = \prod_{(\sigma,p^i)\in\Gamma} p^i$, com $n_\sigma = 1$ se este produto for vazio e $\mathcal{P}_{\sigma,1} = \mathcal{W}(A)$. Com esta notação, desde que $Ass(A)$, é um conjunto finito, temos que $\mathcal{J} = \bigcap_{\sigma \in Ass(A)} \mathcal{P}_{\sigma,n_\sigma}$. Agora, o resultado segue da seguinte afirmação

Afirmação - *Existe uma forma bilinear* $b \in \mathcal{B}il(A)$, *tal que* $|\sigma(b)| = n_\sigma$, *para todo* $\sigma \in Ass(A)$.

De fato, se tal forma bilinear b existe, então $b.\mathcal{W}(A) \subseteq \mathcal{P}_{\sigma,n_\sigma}$, para todo $\sigma \in Ass(A)$, o que implica que $b.\mathcal{W}(A) \subseteq \bigcap_{\sigma \in Ass(A)} \mathcal{P}_{\sigma,n_\sigma} = \mathcal{J}$. Observe que para cada $\sigma \in Ass(A)$, n_σ é um número inteiro ímpar e, $\sigma(b) = n_\sigma$ implica que b é uma forma de dimensão ímpar. Portanto, os únicos ideais primários contendo b são os ideais $\mathcal{P}_{\sigma,p^i}$, com $(\sigma, p^i) \in \Gamma$ e ideais contendo estes. Desde que a decomposição primária reduzida de $b.\mathcal{W}(A)$ é uma intersecção finita de ideais primários contendo b, temos que $\mathcal{J} \subseteq b.\mathcal{W}(A)$, ou seja, $\mathcal{J} = b.\mathcal{W}(A)$, o que mostra (iv).

Finalmente, mostremos a afirmação. Se $n_\sigma = 1$, para todo $\sigma \in Ass(A)$, então $b = \langle 1 \rangle$ satisfaz a afirmação. Podemos então assumir que $n_\sigma \neq 1$, para pelo menos um $\sigma \in Ass(A)$. Como n_σ é um inteiro ímpar, para cada $\sigma \in Ass(A)$, temos que existe pelo menos um $\sigma \in Ass(A)$ tal que $n_\sigma \geq 3$.

Desde que $Ass(A)$ é um conjunto finito, temos que $n = \sum_{\sigma \in Ass(A)} n_\sigma \geq r + 2$, onde r é o número de elementos de $Ass(A)$. Mostraremos agora a afirmação por indução sobre n.

Se $n = r + 2$, então existe exatamente um $\sigma \in Ass(A)$ tal que $n_\sigma = 3$ e $n_\tau = 1$, para todo $\tau \in Ass(A)$ com $\tau \neq \sigma$. Neste caso, $b = q_\sigma$ satisfaz o requerido.

Se $n > r + 2$, consideremos dois casos separadamente:

Caso 1 - Existe $\sigma \in Ass(A)$, tal que $n_\sigma \geq 5$.

Considere o ideal de $W(A)$, $\mathcal{J}_0 = \mathcal{P}_{\sigma,n_\sigma-4} \cap \left(\bigcap_{\tau \neq \sigma} \mathcal{P}_{\tau,n_\tau} \right)$. Neste caso, $n_0 = (n_\sigma - 4) + \sum_{\tau \neq \sigma} n_\tau < n$ e, por hipótese de indução, existe $b_0 \in Bil(A)$ tal que

$$|\tau(b_0)| = \begin{cases} n_\sigma - 4 & \text{se } \tau = \sigma \\ n_\tau & \text{se } \tau \neq \sigma \end{cases}$$

Tomando $e = \pm 1$, de acordo com o sinal de $\sigma(b_0) = \pm(n_\sigma - 4)$, temos que $b = b_0 \perp \langle e \rangle \otimes b_\sigma$ satisfaz a afirmação pois

$$|\sigma(b)| = |\sigma(b_0) + \sigma(\langle e \rangle \otimes b_\sigma)| = (n_\sigma - 4) + 4 = n_\sigma$$
$$|\tau(b)| = |\tau(b_0) + \tau(\langle e \rangle \otimes b_\sigma)| = |\tau(b_0)| = n_\tau,$$

para todo $\tau \neq \sigma$.

Caso 2 - Para todo $\sigma \in Ass(A)$, $n_\sigma \leq 3$.

Desde que $n > r + 2$, temos que pelo menos dois n_σ's são iguais a 3. Digamos que $\sigma, \gamma \in Ass(A)$ são tais que $n_\sigma = n_\gamma = 3$. Seja

$$\mathcal{J}_0 = \mathcal{P}_{\sigma,1} \cap \mathcal{P}_{\gamma,1} \cap \left(\bigcap_{\tau \neq \sigma,\gamma} P_{\tau,n_\tau} \right) \subseteq W(A).$$

Para este ideal $\mathcal{J}_0$, temos $n_0 = 1 + 1 + \sum_{\tau \neq \sigma,\gamma} n_\tau < n$. Então, por hipótese de indução, existe $b_0 \in Bil(A)$ tal que

$$|\tau(b_0)| = \begin{cases} 1 & \text{se } \tau = \sigma \text{ ou } \gamma \\ n_\tau & \text{se } \tau \neq \sigma,\ \gamma. \end{cases}$$

Para cada $\tau \in Ass(A)$, seja $e_\tau = \dfrac{\tau(b_0)}{|\tau(b_0)|} = \pm 1$, de acordo com o sinal de $\tau(b_0)$. Sem perda de generalidade, podemos assumir que $e_\sigma = 1$, pois caso contrário, $b_0' = \langle -1 \rangle \otimes b_0 \in Bil(A)$ é tal que $|\tau(b_0')| = |\tau(b_0)|$, para todo $\tau \in Ass(A)$, e $e_\sigma = \dfrac{\sigma(b_0')}{\sigma(b_0')} = 1$. Mais ainda, podemos também assumir que $e_\gamma = 1$, pois se $e_\sigma =$

1 e $e_\gamma = -1$, escolhemos $\alpha \in A$ tal que $\sigma(\langle\alpha\rangle) = 1$ e $\gamma(\langle\alpha\rangle) = -1$, que existe por **(4.9)**. Neste caso, $b'_0 = \langle\alpha\rangle \otimes b_0 \in \mathcal{B}il(A)$ é tal que $|\tau(b'_0)| = |\tau(b_0)|$, para todo $\tau \in \mathcal{A}ss(A)$ e $e_\sigma = e_\gamma = 1$.

Para cada $\tau \in \mathcal{A}ss(A)$, com $\tau \neq \sigma,\ \gamma$, podemos escrever $n_\tau = 2m'_\tau + 1$, pois cada n_τ é ímpar. Considerando $m_\tau = m'_\tau$ se $e_\tau = 1$ e $m_\tau = -(m'_\tau + 1)$ se $e_\tau = -1$, temos que

$$b = b_0 \perp q_\sigma \perp q_\gamma \perp (\perp_{\tau \neq \sigma,\gamma} (-m_\tau)\, b_\tau)$$

satisfaz a afirmação. De fato:

$$\begin{cases} \sigma(b) = \sigma(b_0) + \sigma(q_\sigma) + \sigma(q_\gamma) - \displaystyle\sum_{\tau \neq \sigma,\gamma} m_\tau\, \sigma(b_\tau) = 1 + 3 - 1 = 3 = n_\sigma \\ \gamma(b) = \gamma(b_0) + \gamma(q_\sigma) + \gamma(b_\gamma) - \displaystyle\sum_{\tau \neq \sigma,\gamma} m_\tau\, \gamma(b_\tau) = 1 - 1 + 3 = n_\gamma. \end{cases}$$

Se $\tau \in \mathcal{A}ss(A) - \{\sigma,\ \gamma\}$ e $e_\tau = 1$, então

$$\begin{aligned} \tau(b) &= \tau(b_0) + \tau(q_\sigma) + \tau(q_\gamma) - m_\tau\, \tau(b_\tau) = \\ &= n_\tau - 1 - 1 - 4\, m'_\tau = \\ &= 2\, m'_\tau + 1 - 2 - 4\, m'_\tau = \\ &= -2\, m'_\tau - 1 = -n_\tau. \end{aligned}$$

Se $\tau \in \mathcal{A}ss(A) - \{\sigma,\ \gamma\}$ e $e_\tau = -1$, então

$$\begin{aligned} \tau(b) &= \tau(b_0) + \tau(q_\sigma) + \tau(q_\gamma) - m_\tau \tau(b_\tau) = \\ &= -n_\tau - 2 - 4(-(m'_\tau + 1)) = \\ &= n_\tau. \end{aligned}$$

Assim, $|\tau(b)| = n_\tau$, para todo $\tau \in \mathcal{A}ss(A)$, como queríamos. ∎

Corolário 4.21 *Se valem as condições equivalentes do teorema anterior, então vale a fatoração única em irredutíveis para formas de dimensão ímpar em* $\mathcal{W}(A)$.

Dem.: Mostra-se de maneira análoga a demonstração canônica de que todo domínio de ideais principais é um domínio fatorial, veja por exemplo [11]. ■

Referências Bibliográficas

[01] **ATIYAH, M.F. e MACDONALD, I.G.**; *Introduction to Commutative Algebra*, University of Oxford, 1969.

[02] **BAEZA, R.**; *Quadratic Forms over Semilocal Ring*, Lecture Notes in Mathematics 655, 1978.

[03] **BRUSAMARELLO, R.**; *Ideais Primos do Anel de Witt sobre um Anel Local*, Tese de Mestrado, ICMSC-USP, 1991.

[04] **DIAS, I.**; *Formas Quadráticas sobre LG-anéis*, Tese de Doutorado, IMECC-UNICAMP, 1988.

[05] **FITZGERALD, R.W.**; *Primary Ideals in Witt Rings*, Communication in Algebra 96, 368-385 (1985).

[06] **FITZGERALD, R.W.**; *Ideal Class Groups of Witt Rings*, Journal of Algebra 124, 506-520 (1989).

[07] **KAPLANSKY, I.**; *Commutative Rings*, Allyn an Bacon, Boston, 1970.

[08] **KNEBUSH, M.;ROSENBERG, A.; WARE,R.**; *Struture of Witt Rings, Quotients of Abelian Group Rings, and Orderings of Fields*, Bull. Amer. Math. Soc. 77, 208-210, (1971).

[09] **KNEBUSCH, M.; ROSENBERG, A.; WARE, R.**; *Struture of Witt Ring and Quotients of Abelian Group Rings*, Amer. J. of Math. 94, 119-155, (1972).

[10] **LAM, T. Y.**; *The Algebric Theory of Quadratic* .
California, 1973.

[11] **LANG, S.**; *Algebra*, Addison-Wesley P.C., Inc., 1993.

[12] **MCDONALD,B.R.**; *Linear Algebra over Commutative Rings*; Pure and Applied Math, 87, Marcel Dekker,INC., 1984.

[13] **PIERCE, R.**; *Associative Algebras*, G. T. M. 88, Springer Verlag, 1982.