FORMAS QUADRÁTICAS SOBRE LG-ANÉIS

Este exemplar corresponde à redação final da Tese defendida pela Srta. IRES DIAS, e aprovada pela comissão julgadora.

Campinas, 4 de outubro de 1988.

Prof. Dr. ANTONIO PAQUES
Orientador

Tese de Doutoramento apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do título de "Doutor em Ciências".

Outubro de 1988

A Alexandre e Junior

Agradeço ao Prof. Dr. Antonio Paques pela dedicada e precisa orientação; à FAPESP e CAPES pelo custeio parcial de meus estudos de Pós-Graduação; à minha família, pelo carinho, apoio e compreensão; aos professores e funcionários da Faculdade de Engenharia de Limeira - UNICAMP, pela colaboração na impressão deste trabalho, em especial ao Prof. Francisco A. Menezes e à Profª Gladis Camarini, e a todos aqueles que direta ou indiretamente colaboraram para a realização deste trabalho.

INTRODUÇÃO

Neste trabalho apresentamos um estudo sobre formas quadráticas sobre um LG-anel. Um LG-anel é um anel comutativo com elemento identidade que satisfaz o seguinte princípio local-global: "todo polinômio $f \in R[X_1,\ldots,X_n]$ que representa uma unidade em R_p, para todo ideal maximal p de R, também representa uma unidade em R". Tais anéis surgiram pela primeira vez na literatura nos trabalhos de D. Estes e R. Guralnick [E-G] e de B. R. McDonald e W. C. Waterhouse [McD-W], o nome LG-anel é devido à Estes e Guralnick. Como exemplos de LG-anel citamos os anéis semi-locais, os anéis Von Neumann regulares (ou absolutamente planos) ou, mais geralmente, os anéis que módulo seu radical de Jacobson são Von Neumann regulares.

Os resultados sobre formas quadráticas aqui apresentados são extensões aos LG-anéis de resultados obtidos por E. Witt [W], A. Pfister [Pf], C. Arf [A], J. Milnor [M] e C. H. Sah [Sa] no caso de corpos, por A. Micali e O. Villamayor [M-V] e D. G. James [J] no caso de anéis locais, por M. Knebush, A. Rosenberg e R. Ware [K-R-W]$_{1e2}$, M. Knebush [Kn]$_{1,2,3}$ e R. Baeza [B] no caso de anéis semi-locais e por B. H. Kirkwood [K], B. H. Kirkwood e B. R. McDonald [K-McD]$_{1,2,3}$ e H. Ishibashi [I] no caso de anéis sobre os quais todo polinômio primitivo quadrático representa uma unidade (os assim chamados "full-rings").

No Capítulo I, apresentamos a noção e exemplos de LG-anel e estudamos algumas de suas propriedades.

No Capítulo II, introduzimos as noções de espaços

bilinear e quadrático sobre um LG-anel. Os principais resultados aqui apresentados são os teoremas de estrutura para espaços bilinear e quadrático e o teorema do Cancelamento de Witt para espaços quadráticos.

No Capítulo III, fazemos um estudo dos anéis de Witt bilinear $W(R)$ e quadrático $W_q(R)$ de um LG-anel R. Especificamente, descrevemos os geradores e ideais primos de $W(R)$ e apresentamos alguns resultados sobre os elementos de torção e os elementos nilpotentes de $W(R)$ e $W_q(R)$, entre os quais o Princípio Local-Global de Pfister, para espaços bilineares, e o seu análogo quadrático.

Finalmente, no Capítulo IV, nos dedicamos ao estudo do grupo ortogonal $O(V)$ de um espaço quadrático (V,q) sobre um LG-anel R tal que $\dim_R V \geq 3$ e dimensão hiperbólica de $V \geq 1$. Apresentamos uma descrição completa dos geradores de $O(V)$ e exibimos uma caracterização dos subgrupos de $O(V)$ que são normalizados por $\Omega(V) = [O(V),O(V)]$.

ÍNDICE

CAPÍTULO I

LG - ANÉIS

No que segue e nos demais capítulos R denotará sempre um anel comutativo com elemento identidade 1. Indicamos por Spm(R) o conjunto dos ideais maximais de R, por J(R) o radical de Jacobson de R e por R^* o grupo das unidades de R. Assumiremos também, neste capítulo e nos demais, que todo R-módulo é unitário, que todo R-álgebra é associativa (não necessáriamente comutativa) com elemento identidade e que todo homomorfismo de anéis leva elemento identidade em elemento identidade.

§ 1 - Definições e Propriedades

(1.1) Definição - Um anel R é dito ser um *LG-anel* se satisfaz o seguinte princípio local-global: "Todo polinômio $f \in R[X_1,\ldots,X_n]$ que representa uma unidade em R_p, para todo $p \in Spm(R)$, também representa uma unidade em R".

(1.2) Lema - As seguintes condições são equivalentes:

(i) R é um LG-anel.

(ii) Todo $f \in R[X_1,\ldots,X_n]$ que satisfaz $\sum_{x\in R^n} f(x)R = R$ representa uma unidade em R.

Dem.: (i) → (ii). Se $f \in R[X_1,\ldots,X_n]$ é tal que $\sum_{x\in R^n} f(x)R = R$, então, para todo $\wp \in Spm(R)$, $\sum_{x\in R^n_\wp} f(x)R_\wp = R_\wp$ e, consequentemente, existem $r_1,\ldots,r_s \in R_\wp$ e $X^{(1)},\ldots,X^{(s)} \in R^n_\wp$, tais que, $1 = \sum_{i=1}^{s} f(X^{(i)})r_i$. Disto segue-se imediatamente que existe $1 \leq i \leq s$ tal que $f(X^{(i)}) \in R^*_\wp$. Logo, f representa uma unidade em $R_\wp$, para todo $\wp \in Spm(R)$. De (i) segue-se que f representa uma unidade em R.

(ii) → (i). Se $f \in R[X_1,\ldots,X_n]$ é tal que, para todo $\wp \in Spm(R)$, f representa uma unidade em $R_\wp$, então, o ideal de R, $I = \sum_{x\in R^n} f(x)R$, é tal que $I_\wp = R_\wp$ para todo $\wp \in Spm(R)$, o que implica que $I = R$ e, por (ii), f representa uma unidade em R, como queríamos■

A noção de LG-anel é preservada por homomorfismos.

(1.3) Proposição - Se R é um LG-anel e $I \subseteq R$ é um ideal, então R/I é um LG-anel.

Dem.: Se $\bar{f} \in R/I[X_1,\ldots X_n]$ é tal que $\sum_{x\in(R/I)^n} \bar{f}(x)R/I = R/I$, então existem $r_1,\ldots,r_t \in R$ e $X^{(1)},\ldots, X^{(t)} \in R^n$, tais que $\sum_{i=1}^{t} \overline{f(X^{(i)})}\bar{r}_i = \bar{1}$, ou seja $r_1f(X^{(1)}) +\ldots+ r_tf(X^{(t)}) = 1 + a$, para algum $a \in I$.

Desde que $\sum_{x\in(R/I)^n} \bar{f}(x)R/I = R/I$, temos que $\sum_{x\in(R/I)^{n+1}} \bar{h}(x)R/I = R/I$, onde $h(X_1,\ldots,X_n,X_{n+1}) =$

$= X_{n+1} f(X_1,\ldots,X_n)$. O polinômio $g(X_1,\ldots,X_{n+2}) = aX_{n+2} +$ $+ h(X_1,\ldots,X_{n+1})$ satisfaz $\bar{g}=\bar{h}$ e $\sum_{X\in R^{n+2}} g(X)R = R$, pois $1 =$ $= g(0,\ldots,0,-1) + \sum_{i=1}^{t} r_i g(X_1^{(i)},\ldots,X_n^{(i)},1,0)$. Mas, por hipótese, R é um LG-anel , logo g representa uma unidade em R, portanto $\bar{h} =$ $= \bar{g}$ representa uma unidade em R/I, o que implica que $\bar{f}$ representa uma unidade em R/I, como queríamos■

(1.4) **Observação** - Observemos que se R/I é um LG-anel, não necessariamente R é um LG-anel. Basta tomarmos $R = \mathbb{Z}$, $f(X) = X^2 +$ $+ 2 \in R[X]$ e $I = (p)$, para algum número primo p. Claramente $\mathbb{Z}/(p)$ é um LG-anel (pois é corpo) e, f representa unidade em $\mathbb{Z}_{(q)}$, para todo número primo q, e não representa em $\mathbb{Z}$, isto é, $\mathbb{Z}$ não é um LG-anel.

Contudo temos a seguinte proposição:

(1.5) **Proposição** - Sejam R um anel e $I \subseteq J(R)$ um ideal de R. Se R/I é um LG-anel, então R também o é.

Dem.: Tomando $f \in R[X_1,\ldots,X_n]$ tal que $\sum_{X\in R^n} f(X)R = R$, temos $\sum_{X\in(R/I)^n} \bar{f}(X)R/I = R/I$ e, desde que R/I é um LG-anel, temos que $\bar{f}$ representa uma unidade em R/I. Assim, existem $X \in (R/I)^n$ e $\bar{\lambda} \in$ $\in (R/I)^*$ tais que $\bar{f}(X) = \bar{\lambda}$, ou equivalentemente, existem $X \in R^n$ e $\lambda \in R^*$ tais que $f(X) = \lambda + a$, para algum $a \in I$. De $I \subseteq J(R)$ segue que $\lambda + a \in R^*$ o que mostra que R é um LG-anel■

O seguinte lema nos será útil no que se segue.

(1.6) Lema ([E-G]Lemma 2.1) - Seja S uma R-álgebra contendo R como sub-anel. Se S é finitamente gerada como R-módulo, então S é imagem homomórfica de uma R-subálgebra de $M_n(R)$ (= álgebra das matrizes nxn à coeficientes em R). Além disso, toda subálgebra de S, finitamente gerada como R-álgebra é também finitamente gerada como R-módulo.

Dem.: Desde que S é finitamente gerado como R-módulo, existem um R-módulo livre e finitamente gerado F e um homomorfismo sobrejetor de R-módulos, $\varphi: F \to S$. Logo $S = End_S(S)$ é a imagem homomórfica do subanel A de $End_R(F) \cong M_n(R)$, consistindo daqueles endomorfismos que induzem S-endomorfismos de S. Agora, toda R-subálgebra finitamente gerada de S é imagem homomórfica de uma R-subálgebra finitamente gerada de A (sua pré-imagem). Finalmente observando que cada elemento de $M_n(R)$ é raiz de seu polinômio característico vemos que toda R-subálgebra finitamente gerada de $M_n(R)$ e, em particular de A, é também finitamente gerada como R-módulo, o que mostra o lema ■

(1.7) Teorema ([E.G]Prop..2.2) - Sejam R um LG-anel, S uma R-álgebra finitamente gerada como R-módulo e $f \in R[X_1,\ldots,X_m,Y_1,\ldots,Y_n]$. Sejam $a \in S^m$ e $L \subseteq S^n$ um R-submódulo. Se para cada $\wp \in Spm(R)$ existe $c_\wp \in L_\wp$ tal que $f(a,c_\wp) \in S^*_\wp$, então existe $c \in L$ tal que $f(a,c) \in S^*$.

Dem.: Observemos primeiro que $c_\wp = d_\wp/\lambda$, onde $d_\wp \in L_\wp$ e $\lambda \in R-\wp$.

Trocando $c_{\mathfrak{p}}$ por $d_{\mathfrak{p}}\lambda'$ onde $\lambda\lambda' \equiv 1 \bmod \mathfrak{p}$, podemos assumir que $c_{\mathfrak{p}} \in L$, pois $c_{\mathfrak{p}} = d_{\mathfrak{p}} / \lambda = d_{\mathfrak{p}}\lambda' / \lambda\lambda' = d_{\mathfrak{p}}\lambda' / 1$ em $L_{\mathfrak{p}}$.

Trocando f por Zf, se necessário, podemos assumir ainda que $f(a,c_{\mathfrak{p}}) \in R-\mathfrak{p}$, pois se $f(a,c_{\mathfrak{p}}) = \alpha$, com $\alpha \in S^{*}_{\mathfrak{p}}$ e $\alpha \notin R-\mathfrak{p}$, então $\alpha^{-1}f(a,c_{\mathfrak{p}}) = 1 \in R-\mathfrak{p}$ e, f representa uma unidade, se, e somente se, Zf representa uma unidade.

Como S é finitamente gerada como R-módulo de (1.6) decorre que $S \cong A/I$ onde A é uma R-subálgebra de $M_k(R)$ e finitamente gerada como R-módulo. Consideremos uma pré-imagem $a' \in A^m$, de a e $L' \subseteq A^n$ de L.

Para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, $S_{\mathfrak{p}} \cong (A/I)_{\mathfrak{p}} \cong A_{\mathfrak{p}} / I_{\mathfrak{p}}$, logo existem $c'_{\mathfrak{p}} \in L'_{\mathfrak{p}}$ e $\alpha_{\mathfrak{p}} \in R^{*}_{\mathfrak{p}}$ tal que $\overline{f(a',c'_{\mathfrak{p}})\alpha_{\mathfrak{p}}} = \bar{1}$ em $A_{\mathfrak{p}}/I_{\mathfrak{p}}$, ou seja, $f(a',c'_{\mathfrak{p}})\alpha_{\mathfrak{p}} = 1 + i$ para algum $i \in I_{\mathfrak{p}}$, o que implica que $f(a',c'_{\mathfrak{p}})\alpha_{\mathfrak{p}} - i = 1$, ou ainda, $(f(a',c'_{\mathfrak{p}}) - i\alpha_{\mathfrak{p}}^{-1})\alpha_{\mathfrak{p}} = 1$.

Assim para cada $\mathfrak{p} \in \mathrm{Spm}(R)$, existem $c'_{\mathfrak{p}} \in L'_{\mathfrak{p}}$ e $i' = -i\alpha_{\mathfrak{p}}^{-1} \in I_{\mathfrak{p}}$ tais que $f(a',c'_{\mathfrak{p}}) + i' \in A^{*}_{\mathfrak{p}}$. Portanto, considerando $g(X_1,\ldots,X_m,Y_1,\ldots,Y_n,Z) = f(X_1,\ldots,X_m,Y_1,\ldots,Y_n) + Z$, $a' \in A^m$ e $L'' = L' \times I \subseteq A^{n+1}$, do que vimos acima segue que para todo $\mathfrak{p} \in \mathrm{Spm}(R)$ existe $\lambda_{\mathfrak{p}} \in L''_{\mathfrak{p}}$ tal que $g(a',\lambda_{\mathfrak{p}})$ é uma unidade em $A_{\mathfrak{p}}$. Logo é suficiente mostrarmos o resultado para A. Assumiremos então que $S = A$ e que $L \subseteq A^n$.

Observemos que $f(a,Y_1,\ldots,Y_n) \in S[Y_1,\ldots,Y_n] \subseteq M_k(R)[Y_1,\ldots,Y_n] \subseteq M_k(R[Y_1,\ldots,Y_n])$, o que implica que, $h(Y_1,\ldots,Y_n) = \det(f(a,Y_1,\ldots,Y_n)) \in R[Y_1,\ldots,Y_n]$. Agora, por hipótese existe $c_{\mathfrak{p}} \in L_{\mathfrak{p}}$ tal que $f(a,c_{\mathfrak{p}}) \in S^{*}_{\mathfrak{p}}$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, ou seja, h representa uma unidade localmente. Mas R é

um LG-anel, então h representa uma unidade em R, isto é, existe $c \in L \subseteq S^n$ tal que $\det(f(a,c)) \in R^*$, portanto $f(a,c) \in S^*$, o que mostra o teorema■

(1.8) Corolário ([E-G] Cor.2.3) - Seja $R \subseteq S$ uma extensão integral de anéis. Se R é um LG-anel, então S também o é.

Dem.: Seja $f \in S[X_1,\ldots,X_n]$ que representa uma unidade em S_q, para todo $q \in \mathrm{Spm}(S)$. Queremos mostrar que f representa uma unidade em S.

Observemos que, dado $p \in \mathrm{Spm}(R)$, existe $q \in \mathrm{Spm}(S)$, tal que $q \cap R = p$ e $T_1 = R-p$, $T_2 = S-q$ são dois subconjuntos multiplicativamente fechados de S com $T_1 \subseteq T_2$.

Observemos ainda que dado q', ideal primo de S, se $q' \cap T_2 \neq \emptyset$, então $q' \cap T_1 \neq \emptyset$. De fato, se $q' \cap T_1 = \emptyset$, então $p' = q' \cap R$ é um ideal primo de R contido em p, e pelo teorema "going up", $q' \subseteq q$ que é uma contradição pois $q' \cap T_2 \neq \emptyset$. Logo,de [Bo] Prop.8, § 2, Chap 2, segue que os subconjuntos multiplicativos T_1 e T_2 tambem satisfazem o seguinte:

(*)"para todo $t \in T_2$, existe $s \in S$ tal que $st \in T_1$".

Observemos também que se $f \in S[X_1,\ldots,X_n]$ então $f \in R[Y_1,\ldots,Y_m,X_1,\ldots,X_n]$ onde os $Y_i \in S$ são os coeficientes de f. Podemos então nos restringir ao caso em que $S = R[Y_1,\ldots,Y_m]$, que é finitamente gerado como R-módulo. Agora, para todo $p \in \mathrm{Spm}(R)$, existe $q \in \mathrm{Spm}(S)$ tal que $q \cap R = p$, e f representa uma unidade em S_q, isto é, existe $c_q \in S^n_q$ tal que se $a = (Y_1,\ldots,Y_m) \in S^m$, $f(a,c_q) \in S^*_q$. De (*) decorre facilmente que

existe $c_{\mathfrak{p}} \in S_{\mathfrak{p}}^n$ tal que $f(a,c_{\mathfrak{p}}) \in S_{\mathfrak{p}}^*$ e, do teorema (1.7) segue que f representa uma unidade em S, como queríamos■.

(1.9) Teorema ([McD-W]Theorem) - Seja R um LG-anel. Se L é um R-módulo projetivo, finitamente gerado e de posto constante, então L é um R-módulo livre.

Dem.: Desde que L é projetivo e finitamente gerado existe $n \in \mathbb{N}$ tal que $R^n \cong L \oplus Q$, para algum R-módulo Q.

Sejam $\pi: R^n \to R^n$, a projeção em L com núcleo Q e M a matriz associada a π. Sejam $X = (X_{ij})$, $1 \leq i, j \leq n$, uma matriz de indeterminadas e X^c a matriz dos cofatores tal que $XX^c = \det(X)I_n$ onde I_n denota a matriz identidade nxn. Sejam m o posto de L, $g(X_{ij})$ o polinômio que é o determinante do bloco mxm superior à esquerda de XMX^c e $f(X_{ij}) = g(X_{ij})\det(X_{ij})$.

Dado $\mathfrak{p} \in \mathrm{Spm}(R)$, ambos os módulos $L_{\mathfrak{p}}$ e $Q_{\mathfrak{p}}$ são livres sobre o anel local $R_{\mathfrak{p}}$, $\dim L_{\mathfrak{p}} = m$ e $R_{\mathfrak{p}}^n \cong L_{\mathfrak{p}} \oplus Q_{\mathfrak{p}}$. Escolhendo uma base para $R_{\mathfrak{p}}^n$, compatível com esta decomposição, temos que a projeção sobre $L_{\mathfrak{p}}$ tem matriz $\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}$. Se (c_{ij}) é a matriz de mudança da base canônica para a base escolhida acima, então $g(c_{ij}) = (\det(c_{ij})^m)$ é uma unidade e, consequentemente, $f(c_{ij}) \in R_{\mathfrak{p}}^*$. Mostramos então que f representa uma unidade localmente e, desde que R é um LG-anel, f representa uma unidade em R, isto é, existe $(a_{ij}) \in M_n(R)$ tal que $f(a_{ij}) = g(a_{ij})\det(a_{ij}) \in R^*$. Então (a_{ij}) é inversível e o bloco mxm superior à esquerda de $M' = (a_{ij})M(a_{ij})^{-1}$ é inversível.

Fazendo a mudança de base de R^n dada pela matriz (a_{ij}), temos que a matriz da projeção sobre L é M'.

Sejam $F = R^m \times \{0\}$ e $p: R^n \to F$ a projeção com núcleo $\{0\} \times R^{n-m}$. Então $F \to R^n \xrightarrow{\pi} R^n \xrightarrow{p} F$, tem matriz inversível. Consequentemente $p|_{\pi(R^n)=L}: L \to F$ é sobrejetora e, desde que F é um R-módulo livre, a sequência exata curta $0 \to \mathrm{Ker}\, p|_L \to L \to F \to 0$ cinde. Portanto $L \cong F \oplus K$ para algum R-módulo K. Finalmente observemos que $L_\wp$ e $F_\wp$ são livres de dimensão m, o que implica que $K_\wp = 0$ para todo $\wp \in \mathrm{Spm}(R)$, ou seja $K = 0$ e $L \cong F$ que é livre ■

§ 2 - Exemplos

Podemos ver imediatamente, a partir da definição, que todo corpo ou mais geralmente todo anel local é um LG-anel.

No teorema seguinte mostraremos que todo anel Von Neumann regular é um LG-anel. Recordemos que um anel Von Neumann regular R é um anel caracterizado pelas seguintes condições equivalentes:

- "$R_\wp$ é corpo para todo $\wp \in \mathrm{Spm}(R)$".
- "Todo R-módulo é plano".

Observemos também que, se R é um anel Von Neumann regular, então as seguintes afirmações são verdadeiras:

- "Spm(R) é Hausdorff, compacto e totalmente desconexo (com a topologia de Zariski)".
- "Os abertos básicos de Spm(R) são também fechados".

-"Todo ideal primo é maximal".

-"R é isomorfo a um sub-produto direto de corpos".

(2.1) Teorema([G-W]Prop.3) - Todo anel Von Neumann regular é um LG-anel.

Dem.: Sejam R um anel Von Neumann regular (VN-regular) e f $\in$ $\in R[X_1,\ldots,X_n]$ um polinômio que representa unidade localmente. Assim, dado $p \in Spm(R)$ existem $a_i \in R$ e λ, c, $b_i \in R-p$, $1 \leq i \leq n$, tais que $f(\frac{a_1}{b_1},\ldots,\frac{a_n}{b_n}) = \frac{\lambda}{c} \in R_p^*$. Tomando $X_i = \frac{Y_i}{Z_i}$, $1 \leq i \leq n$, podemos escrever $(Z_1\ldots Z_n)^N f(X_1,\ldots,X_n) = g(Y_1,\ldots,Y_n,Z_1,\ldots,Z_n)$, para algum $N \in \mathbb{N}$. Desde que $b_1,\ldots,b_n \in R-p$, temos $(b_1\ldots b_n)^N \in$ $\in R_p^*$ e, consequentemente podemos afirmar que dado $p \in Spm(R)$, existem $a_1,\ldots,a_n \in R$, λ, c, $b_1,\ldots,b_n \in R-p$ tais que

(*) $cg(a_1,\ldots,a_n,b_1,\ldots,b_n) = \lambda$.

Considerando Spm(R) com a topologia de Zariski, indiquemos por X a família de abertos $\mathcal{A} \subseteq Spm(R)$ tais que existem $a_1,\ldots,a_n \in R$ e λ, c, $b_1,\ldots,b_n \in R - \bigcup_{p\in\mathcal{A}} p$ satisfazendo (*).

Desde que para cada $p \in Spm(R)$, existem $a_i \in R$, λ, c, $b_i \in R-p$, $1 \leq i \leq n$, satisfazendo (*), temos que $p \in \mathcal{A} \in X$, onde $\mathcal{A} = (p \in Spm(R);\ \lambda c b_1\ldots b_n \notin p)$, que é um aberto básico de Spm(R). Assim, X contém uma cobertura do Spm(R) por abertos básicos. Mas, Spm(R) é compacto. Logo, existem $\mathcal{A}_1,\ldots,\mathcal{A}_t$ em X, abertos básicos de Spm(R), tais que $Spm(R) = \bigcup_{i=1}^{t} \mathcal{A}_i$.

Considerando que os abertos básicos de Spm(X) são

também fechados, a diferença entre dois conjuntos abertos e fechados é um aberto, se $\mathcal{A} \in X$ e $\mathcal{A}' \subseteq \mathcal{A}$ é um aberto, então $\mathcal{A}' \in X$ e, escrevendo $\mathrm{Spm}(R) = \bigcup_{j=1}^{m} \left(\bigcap_{\substack{k=1 \\ i_1 < \ldots < i_j \\ i_k \in \{1,\ldots,j\}}}^{j} \mathcal{A}_{i_k} - \bigcup_{\substack{l=1 \\ l \neq i_k}}^{i} \mathcal{A}_l \right)$, temos que $\mathrm{Spm}(R)$ admite uma partição finita de abertos de X.

Seja $\{\mathcal{B}_i \,/\, 1 \leq i \leq m\}$, tal partição. Então existem idempotentes ortogonais, $e_1, \ldots, e_m \in R$, tais que $\sum_{i=1}^{m} e_i = 1$ e cada $\mathcal{B}_i = \{p \in \mathrm{Spm}(R);\ e_i \notin p\}$ (cf [Bo] Prop 15, §4, Chap. II).

Para cada $i = 1, \ldots, m$, existem $\alpha_{1i}, \ldots, \alpha_{ni} \in R$ e $\lambda_i,\ c_i,\ \beta_{1i}, \ldots, \beta_{ni} \in R - \bigcup_{p \in \mathcal{B}_i} p$ satisfazendo (*). Considerando, para $1 \leq j \leq n$, $\alpha'_j = \sum_{i=1}^{m} e_i \alpha_{ji}$, $\beta'_j = \sum_{i=1}^{m} e_i \beta_{ji}$, $c' = \sum_{i=1}^{m} e_i c_i$, $\lambda' = \sum_{i=1}^{m} e_i \lambda_i$ e, usando o fato que os e_i são idempotentes ortogonais, obtemos $c' g(\alpha'_1, \ldots, \alpha'_n, \beta'_1, \ldots, \beta'_n) = \lambda'$.

Notemos que $e_i,\ c_i \notin \bigcup_{p \in \mathcal{B}_i} p$, para $1 \leq i \leq m$, logo $e_i c' = e_i c_i \notin \bigcup_{p \in \mathcal{B}_i} p$ e, consequentemente $c' \notin \bigcup_{p \in \mathcal{B}_i} p$, pois $R - \bigcup_{p \in \mathcal{B}_i} p$ é multiplicativamente fechado. Desde que $\{\mathcal{B}_i \,/\, 1 \leq i \leq m\}$ é uma cobertura para $\mathrm{Spm}(R)$, temos $c' \notin p$ para todo $p \in \mathrm{Spm}(R)$ o que implica que $c' \in R^*$. De maneira análoga mostra-se que β'_j e $\lambda' \in R^*$, $1 \leq j \leq n$. Assim $\frac{\alpha'_j}{\beta'_j} \in R$ e, consequentemente $f\left(\frac{\alpha'_1}{\beta'_1}, \ldots, \frac{\alpha'_n}{\beta'_n}\right) = \frac{\lambda'}{c'} \in R^*$, isto é, f representa uma unidade em R. ■

(2.2) Corolário - (i) Todo anel semi-local é um LG-anel.

(ii) Todo anel de dimensão (de Krull) zero é um LG-anel.

Dem.: (i). Imediato, pois se R é um anel semi-local com ideais maximais $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, então $R/J(R) \cong R/\mathfrak{p}_1 \oplus \ldots \oplus R/\mathfrak{p}_r$ é Von Neumman regular. Logo (i) segue-se de (2.1) e (1.5).

(ii). Segue-se de (1.5) e (2.1) e do fato seguinte:

-"R é um anel de dimensão zero se, e somente se J(R) é nilpotente e R/J(R) é Von Neumman regular". ([G-W].Lem.1.(c)).

Mostremos então essa equivalência.

Se J(R) é nilpotente, então $J(R) \subseteq \mathfrak{p}$, para todo ideal primo $\mathfrak{p}$ de R. Logo R e R/J(R) têm a mesma dimensão e, desde que num anel Von Neumann regular todo ideal primo é maximal, temos que R tem dimensão zero.

Reciprocamente, se R tem dimensão zero, então todo ideal primo de R é também maximal e consequentemente J(R) coincide com o nilradical de R que é um ideal nilpotente. Para provarmos que R/J(R) é Von Neumann regular, podemos supor, sem perda de generalidade, que J(R) = 0.

Mostremos que $R_{\mathfrak{p}}$ é corpo, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$.

Desde que R tem dimensão zero, temos que $R_{\mathfrak{p}}$ também tem dimensão zero e, por conseguinte, $\mathfrak{p}R_{\mathfrak{p}}$ é nilpotente. Por outro lado, se $\frac{\lambda}{c} \in R_{\mathfrak{p}}$ é nilpotente, então existe $\alpha \in R-\mathfrak{p}$ tal que $\alpha\lambda^n = 0$, para algum $n > 0$, donde segue-se que $(\alpha\lambda)^n = \alpha^n\lambda^n = 0$, ou seja, $\alpha\lambda$ é nilpotente em R. Como assumimos que J(R) = 0 e R tem dimensão zero, temos $\alpha\lambda = 0$, o que mostra que $\frac{\lambda}{c} = 0$. Isto mostra que $\mathfrak{p}R_{\mathfrak{p}} = 0$ e, portanto, $R_{\mathfrak{p}}$ é corpo■

Outra classe de exemplos é obtida a partir da proposição seguinte.

(2.3) Proposição - Se R é um LG-anel, então R [[X]] também o é.

Dem.: Sejam $S = R[[X]]$ e $f(Y_1,\ldots,Y_n) \in S[Y_1,\ldots,Y_n]$ com $\sum_{Y\in S^n} f(Y)S = S$. Então, existem $(Y_{i1},\ldots,Y_{in}) \in S^n$, $1 \leq i \leq r$, e, $a_1,\ldots,a_r \in S$ tais que $\sum_{i=1}^{r} f(Y_{i1},\ldots,Y_{in})a_i = 1$. Desde que $S[Y_1,\ldots,Y_n] = R[Y_1,\ldots,Y_n][[X]]$, temos $f(Y_1,\ldots,Y_n) = \sum_{i=0}^{\infty} f_i(Y_1,\ldots,Y_n)X^i$, com $f_i \in R[Y_1,\ldots,Y_n]$.

Do fato que $\sum_{i=1}^{r} f(Y_{i1},\ldots,Y_{in})a_i = 1$, segue-se que o termo constante da série à esquerda na igualdade acima é igual a 1, isto é, $\sum_{i=1}^{r} f_o(Y^o_{i1},\ldots,Y^o_{in})a_{io} = 1$, onde Y^o_{ij} e a_{io} são os termos constantes das séries Y_{ij} e a_i respectivamente. Mas $f_o \in R[Y_1,\ldots,Y_n]$ e $a_{io} \in R$, então $\sum_{Y\in R^n} f_o(Y)R = R$, de onde segue que f_o representa uma unidade em R, ou seja, existe $(Y^o_1,\ldots,Y^o_n) \in R^n$ e $\lambda_o \in R^*$ tais que $f_o(Y^o_1,\ldots,Y^o_n) = \lambda_o$. Portanto, existe $(Y_1,\ldots,Y_n) = (Y^o_1,\ldots,Y^o_n) \in S^n$ tal que $f(Y_1,\ldots,Y_n) = \lambda_o + \sum_{i=1}^{\infty} f_i(Y^o_1,\ldots,Y^o_n)X^i \in S^*$, o que mostra que S é um LG-anel ■

Concluiremos este parágrafo fornecendo um método para a construção de um LG-anel à partir de um anel comutativo qualquer. Para tanto necessitaremos de alguns resultados

auxiliares.

(2.4) Definição - Sejam R um anel e $f(X) = \sum_{i=0}^{n} \lambda_i X^i \in R[X]$. Dizemos que f é um *polinômio primitivo* se o ideal c(f) gerado pelos coeficientes λ_i de f é igual a R. Dizemos que R satisfaz o *critério primitivo* se, todo polinômio primitivo de R[X] representa uma unidade em R.

(2.5) Lema ([McD-W]Lemma) -Seja R um anel que satisfaz o critério primitivo. Sejam $f_i(X) = \sum_{j=0}^{n} \lambda_{ij} X^j$, $1 \leq i \leq m$, polinômios tais que $\sum_{i,j} \lambda_{ij} R = R$. Então existe $\lambda \in R$ com $\sum_{i=1}^{m} f_i(\lambda) R = R$.

Dem.: Seja r um número inteiro maior que os graus de todas as f_i, $1 \leq i \leq m$. Considerando $g(X) = \sum_{i=1}^{m} f_i(X) X^{ri}$, temos que todos os λ_{ij} são coeficientes de g; logo g é um polinômio primitivo de R[X]. Consequentemente g representa uma unidade em R, isto é, existe $\lambda \in R$, tal que, $g(\lambda) = \sum_{i=1}^{m} f_i(\lambda)\lambda^{ri} \in R^*$, o que mostra que $\sum_{i=1}^{m} f_i(\lambda) R = R$■

(2.6) Lema ([McD-W] Lemma) - Seja R um anel que satisfaz o critério primitivo. Seja $f \in R[X_1,\ldots,X_n]$ tal que c(f) = R. Então f representa uma unidade em R.

Dem.: Podemos escrever $f(X_1,\ldots,X_n) = \sum_{\alpha} f_\alpha(X_1) X_2^{\alpha_2} \ldots X_n^{\alpha_n}$, onde $\alpha = (\alpha_1,\ldots,\alpha_n)$. Todos os coeficientes de f aparecem como

coeficientes dos f_α, o que mostra que os polinômios f_α satisfazem as hipóteses do lema (2.5). Consequentemente existe $\lambda_1 \in R$ tal que $\sum_\alpha f_\alpha(\lambda_1)R = R$. Agora, $f(\lambda_1, X_2, \ldots, X_n)$ ainda satisfaz a hipótese, logo o resultado segue por indução sobre o número de variáveis.■

(2.7) Proposição ([McD-W]Prop.) - Para um anel R são equivalentes:

(i) R satisfaz o critério primitivo.

(ii) R é um LG-anel com corpos residuais infinitos.

Dem.: Se $p \in Spm(R)$ é tal que $|R/p| = m$ (isto é, a cardinalidade de R/p é m), então o polinômio primitivo $X^m - X \in R[X]$ é identicamente nulo em R/p e consequentemente não representa unidade em R. Logo (i) implica que os corpos residuais de R são infinitos. Agora, se $f \in R[X_1, \ldots, X_n]$ representa uma unidade localmente, então $c(f) = R$, pois $c(f)_p = R_p$ para todo $p \in Spm(R)$. De(i) e (2.6) segue-se que f representa uma unidade em R, ou seja, que R é um LG-anel.

Reciprocamente, se $f \in R[X]$ é primitivo então f é não trivial módulo p, para todo $p \in Spm(R)$ e, desde que os corpos residuais de R são infinitos, f representa um elemento não nulo em $R/p \cong R_p/pR_p$, para todo $p \in Spm(R)$. Consequentemente f representa uma unidade localmente e, desde que R é um LG-anel, f representa uma unidade em R.■

Consideremos agora um anel comutativo R e observemos que o conjunto T = {f ∈ R[X]; f é primitivo} é multiplicativamente fechado, isto é, para quaisquer f, g ∈ R[X] tais que c(f) = c(g) = R, tem-se também c(fg) = R. Para a verificação disto é suficiente nos restringirmos ao caso em que R é um anel local com ideal maximal $\mathcal{P}$.

Se $f(X) = \sum_{i=0}^{m} \alpha_i X^i$ e $g(X) = \sum_{i=0}^{n} \beta_i X^i$ são polinômios satisfazendo c(f) = c(g) = R, então existe algum $0 \leq i \leq m$ e algum $0 \leq j \leq n$ tais que $\alpha_i \beta_j \notin \mathcal{P}$. Sejam $r = \min\{0 \leq i \leq m;\ \alpha_i \notin \mathcal{P}\}$ e $s = \min\{1 \leq j \leq n;\ \beta_j \notin \mathcal{P}\}$. É fácil ver que o coeficiente c_{r+s}, do polinômio $(fg)(X) = \sum_{i=0}^{m+n} c_i X^i$, não pertence ao ideal maximal $\mathcal{P}$ e, por conseguinte, c_{r+s} é inversível em R, o que acarreta c(fg) = R.

(2.8) Proposição - O anel de frações $R(X) = T^{-1}(R[X])$ satisfaz o critério primitivo. Além disso a aplicação canônica $i: R \to R(X)$, dada por $i(\lambda) = \lambda/1$, é injetiva.

Dem.: Se $f(Y) = \sum_{i=0}^{n} \alpha_i(X) Y^i \in R(X)[Y]$ é tal que c(f) = R(X), então podemos supor, sem perda de generalidade, que $\alpha_i(X) \in R[X]$ para $0 \leq i \leq n$, pois o produto dos denominadores é uma unidade em R(X).

De c(f) = R(X), segue-se que existem elementos $c_i \in T$ e $\beta_i' \in R[X]$, $0 \leq i \leq n$, tais que $\sum_{i=0}^{m} \alpha_i(X) \beta_i'(X)/c_i(X) = 1$. Multiplicando esta igualdade por $\prod_{i=0}^{n} c_i(X)$, temos que existem $\beta_i \in$

$\in R[X]$, $0 \leq i \leq n$, tais que $h(X) = \sum_{i=0}^{n} \alpha_i(X)\beta_i(X) \in T$, ou seja, h é uma unidade em $R(X)$.

Observemos que $R = c(h) \subseteq (\bigcup_{i=0}^{n} c(\alpha_i))$ (= ideal gerado pela união dos $c(\alpha_i)$). Assim, tomando um número inteiro s, maior que o máximo dos graus dos $\alpha_i(X)$, $0 \leq i \leq n$, temos que $f(X^s) = \sum_{i=0}^{n} \alpha_i(X)X^{si}$ é tal que $c(f(X^s)) = (\bigcup_{i=0}^{n} c(\alpha_i)) = R$, isto é, $f(X^s)$ é primitivo. Portanto, existem $\lambda \in R$ e $Y = \frac{\lambda^s}{1} \in R(X)$ tal que $f(Y) \in R(X)^*$, o que mostra que $R(X)$ satisfaz o critério primitivo.

Finalmente mostremos que $i: R \to R(X)$ é injetiva. Dado $\alpha \in R$, se $\frac{\alpha}{1} = 0$ em $R(X)$, então existe $f(X) = \sum_{i=0}^{m} \beta_i X^i \in T$ tal que $f(X)\alpha = 0$ em $R[X]$. Disto segue-se que $\beta_i \alpha = 0$, $0 \leq i \leq m$ e, considerando que $c(f) = R$ obtemos $\alpha = 0$. ∎

CAPÍTULO II

Bil(R) e Quad(R)

Neste capítulo trataremos com espaços quadráticos e bilineares sobre um LG-anel R e apresentaremos alguns resultados básicos da teoria como os teoremas de decomposição e teorema do cancelamento para espaços quadráticos. Alguns resultados deste capítulo, sobretudo nos parágrafos 1,2,3 e 5 valem para um anel comutativo com elemento identidade **1** em geral, e estão demonstrados no texto de Baeza [B]; aqui somente os enunciaremos.

Baeza [B] define as noções de espaços quadráticos e bilineares sobre um anel R na categoria dos R-módulos projetivos finitamente gerados e de posto constante com as operações $\oplus$(soma direta) e $\otimes_R$ (produto tensorial). Como os principais resultados deste capítulo (que se encontram nos parágrafos 4 e 6) são sobre espaços quadráticos e bilineares sobre um LG-anel e, neste caso, todo R-módulo projetivo finitamente gerado de posto constante é livre (cf.(I,1.9)), por conveniência de redação, trabalharemos desde o início com a categoria dos R-módulos livres de dimensão finita sobre R. Denotaremos tal categoria por L(R). Exceto quando mencionado o contrário, $\otimes$ significando sempre $\otimes_R$. Para cada $V \in L(R)$, denotaremos por V^* o R-módulo dual $\mathrm{Hom}_R(V,R) \in L(R)$.

§ 1 - Definições

(1.1) Definição - O par (V,b) consistindo de um módulo $V \in L(R)$ e uma forma bilinear simétrica $b: V \times V \to R$ é chamado um *módulo bilinear sobre* R. Um módulo bilinear (V,b) é dito ser *não singular* ou simplesmente um *espaço bilinear*, se a função $d_b: V \to V^*$, dada por $d_b(x) = b(x, \ )$, para todo $x \in V$, for um isomorfismo de R-módulos. Uma *isometria* entre dois módulos bilineares (V_1,b_1) e (V_2,b_2) é um R-isomorfismo $\varphi: V_1 \cong V_2$, satisfazendo $b_1(x,y) = b_2(\varphi(x),\varphi(y))$ para todo $x,y \in V_1$. Quando existe uma isometria entre (V_1,b_1) e (V_2,b_2) dizemos que os módulos bilineares são *isométricos* e denotamos $(V_1,b_1) \simeq (V_2,b_2)$ ou simplesmente $b_1 \simeq b_2$.

Se (V,b) é um módulo bilinear sobre R e $(x_1,\ldots x_n)$ é uma base de V, então a forma bilinear b é determinada pela matriz $(b_{ij})=(b(x_i,x_j)), 1 \leq i,j \leq n$, pois $b(x,y) = \sum_{i,j=1}^{n} b_{ij}\alpha_i\beta_j$, onde $x = \sum_{i=1}^{n}\alpha_i x_i$ e $y = \sum_{j=1}^{n}\beta_j x_j$. Reciprocamente, para cada matriz simétrica n x n, (b_{ij}), sobre R, obtemos uma forma bilinear simétrica sobre V dada pela mesma fórmula descrita acima, e o módulo bilinear (V,b) é não singular se, e sòmente se, $\det(b_{ij})$ é uma unidade em R.

(1.2) Definição - Uma *forma quadrática* sobre um módulo $V \in L(R)$ é uma função $q: V \to R$ satisfazendo as seguintes propriedades:

(i) $q(\lambda x) = \lambda^2 q(x)$, para todo $x \in V$ e $\lambda \in R$.

(ii) $b_q(x,y) = q(x + y) - q(x) - q(y)$; $x,y \in V$ é uma

forma bilinear simétrica em V.

O par (V,q) é denominado um *módulo quadrático* sobre R e (V,b_q) denotará o módulo bilinear associado. Se (V,b_q) é não singular dizemos que (V,q) é *não singular* ou simplesmente, é um *espaço quadrático*. Uma *isometria* entre dois módulos quadráticos (V_1,q_1) e (V_2,q_2) é um R-isomorfismo $\varphi: V_1 \cong V_2$, satisfazendo $q_1(x) = q_2(\varphi(x))$ para todo x de V_1. Quando existe uma isometria entre (V_1,q_1) e (V_2,q_2), dizemos que os módulos quadráticos são *isométricos* e escrevemos $(V_1,q_1) \simeq (V_2,q_2)$, ou simplesmente $q_1 \simeq q_2$. Observamos que se $q_1 \simeq q_2$, então $b_{q_1} \simeq b_{q_2}$.

(1.3) Observação - Se $2 \in R^*$, existe uma correspondência um a um entre os módulos bilineares e os módulos quadráticos sobre R. Esta correspondência associa ao módulo bilinear (V,b) o módulo quadrático (V,q_b) onde $q_b(x) = \frac{1}{2}b(x,x)$; $x \in V$ e reciprocamente, ao módulo quadrático (V,q) corresponde o módulo bilinear (V,b_q). Ve-se imediatamente que $q_{b_q} = q$ e $b_{q_b} = b$.

Consideremos agora um módulo quadrático (V,q) sobre R e $(x_1,\ldots,x_n)$ uma base de V. A matriz (a_{ij}), $1 \leq i,j \leq n$, onde $a_{ij} = b_q(x_i,x_j)$ se $i \neq j$ e $a_{ii} = q(x_i)$ é chamada a matriz dos valores de q com respeito a base $(x_1,\ldots x_n)$ e determina completamente q, desde que para todo $x = \sum_{i=1}^{n} \alpha_i x_i \in V$, $q(x) = \sum_{1 \leq i,j \leq n} a_{ij}\alpha_i\alpha_j$. Por esta razão podemos identificar a forma quadrática q com sua matriz de valores (a_{ij}). Por exemplo se $V = Ru \oplus Rv$ com $q(u)=\alpha$, $q(v)=\beta$ e $b_q(u,v)=1$, temos $q=\begin{pmatrix}\alpha & 1\\ 1 & \beta\end{pmatrix}$. A matriz

dos valores de (V,b_q) é $\begin{pmatrix} 2\alpha & 1 \\ 1 & 2\beta \end{pmatrix}$, logo (V,q) é não singular se, e somente se $1-4\alpha\beta \in R^*$. Denotaremos este particular espaço quadrático por $[\alpha,\beta]$. Se $2=0$ em R, todos os espaços quadráticos $[\alpha,\beta]$ tem o mesmo espaço bilinear associado $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; isto mostra que em geral dois espaços quadráticos não isométricos podem ter o mesmo espaço bilinear associado.

(1.4) Observação - Se R tem característica 2, então $b_q(x,x) = 2q(x) = 0$, para toda forma quadrática q sobre R. Logo, se (V,q) é um espaço quadrático sobre R, então $\dim_R V$ é par.

Denotamos a categoria dos espaços bilineares sobre R por $Bil(R)$ e dos espaços quadráticos por $Quad(R)$, onde os morfismos destas categorias são as isometrias.

§ 2 - Operações em Bil(R) e Quad(R)

(2.1) Soma Ortogonal - Para $(V_i,b_i) \in Bil(R)$, respectivamente $(V_i,q_i) \in Quad(R)$, $i = 1, 2$, definimos:

$$(V_1,b_1) \perp (V_2,b_2) = (V_1 \oplus V_2,\ b_1 \perp b_2),$$

$$(V_1,q_1) \perp (V_2,q_2) = (V_1 \oplus V_2, q_1 \perp q_2),$$

onde $(b_1 \perp b_2)(x_1 + x_2, y_1 + y_2) = b_1(x_1,y_1) + b_2(x_2,y_2)$ e $(q_1 \perp q_2)(x_1 + x_2) = q_1(x_1) + q_2(x_2)$, para todo $x_i, y_i \in V_i$, $i = 1, 2$. É imediato que $b_1 \perp b_2 \in Bil(R)$ e $q_1 \perp q_2 \in Quad(R)$.

(2.2) Ação de Bil(R) sobre Quad(R) - Dados $(V,b) \in Bil(R)$ e

$(V',q) \in Quad(R)$, definimos um novo espaço quadrático

$$(V,b) \otimes (V',q) = (V \otimes V', b \otimes q),$$

onde $(b \otimes q)(x \otimes y) = b(x,x)q(y)$, para todo $x \in V$ e $y \in V'$. O espaço bilinear associado a este espaço quadrático é o produto tensorial $(V,b) \otimes (V',b_q)$ como definido a seguir.

(2.3) Produto Tensorial em Bil(R) e Quad(R) - Para $(V_i,b_i) \in$ $\in Bil(R)$, $i = 1, 2$ definimos:

$$(V_1,b_1) \otimes (V_2,b_2) = (V_1 \otimes V_2, b_1 \otimes b_2),$$

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 $x_i, y_i \in V_i$, $i = 1, 2$.

Para $(V_i,q_i) \in Quad(R)$, $i = 1, 2$, existe uma isometria $(V_1,b_{q_1}) \otimes (V_2,q_2) \simeq (V_1,q_1) \otimes (V_2,b_{q_2})$, a qual nos permite definir, a menos de isometrias o espaço quadrático

$$(V_1,q_1) \circ (V_2,q_2) = (V_1,b_{q_1}) \otimes (V_2,q_2).$$

As operações vistas em (2.2) e (2.3) denotamos, abreviadamente, por $b \otimes q$, $b_1 \otimes b_2$ e $q_1 \circ q_2$ respectivamente. É fácil ver que, para estas operações, valem (a menos de isometrias) a associatividade, a comutatividade e a distributividade. Por exemplo, para $b \in Bil(R)$, $q_1,q_2 \in Quad(R)$, vale $(b \otimes q_1) \circ q_2 \simeq q_1 \circ (b \otimes q_2) \simeq b \otimes (q_1 \circ q_2)$.

§ 3 - Extensão e Contração de Espaços

(3.1) Extensão de Escalares - Seja $\tau: R \to S$ um homomorfismo de anéis. Dados $(V,b) \in Bil(R)$ e $(V',q) \in Quad(R)$, vemos facilmente

que $V \otimes S$ e $V' \otimes S$ estão em $L(S)$. Sobre tais S-módulos definimos, respectivamente, uma forma bilinear $b \otimes S$ e uma forma quadrática $q \otimes S$ do seguinte modo:

$$(b \otimes S)(x \otimes r, y \otimes s) = \tau(b(x,y))rs,$$

$$(q \otimes S)(z \otimes s) = \tau(q(z))s^2, \text{ e}$$

$$b_{q\otimes S}(z \otimes s, w \otimes r) = \tau(b_q(z,w))rs,$$

para todo $x, y \in V$, $z, w \in V'$ e $r, s \in S$. Vemos facilmente que $b \otimes S \in Bil(S)$ e $q \otimes S \in Quad(R)$. Definimos, com isso, dois funtores aditivos e multiplicativos, $\tau^*: Bil(R) \to Bil(S)$ e $\tau^*: Quad(R) \to Quad(S)$ onde $\tau^*(b) = b \otimes S$ e $\tau^*(q) = q \otimes S$, para todo $b \in Bil(R)$ e $q \in Quad(R)$.

Em particular, temos:

(3.2) Localização - Dado $p \in Spm(R)$, consideremos $\tau: R \to R_p$, o homomorfismo canônico $\tau(a) = \frac{a}{1}$, para todo $a \in R$. Para $(V,b) \in Bil(R)$ e $(V,q) \in Quad(R)$ temos $(V_p, b_p) \in Bil(R_p)$ e $(V_p, q_p) \in Quad(R_p)$, onde $b_p(\frac{x}{r}, \frac{y}{s}) = \frac{b(x,y)}{rs}$ e $q_p(\frac{x}{s}) = \frac{q(x)}{s^2}$, para todo $x, y \in V$ e $r, s \in R - p$. Os espaços b_p e q_p sao chamados as localizações de b e q em p, respectivamente.

(3.3) Redução módulo p - Para $p \in Spm(R)$ e $\tau: R \to R/p$ a projeção canônica, temos que para todo $(V,b) \in Bil(R)$ e $(V,q) \in Quad(R)$, $\tau^*(b) = b(p) \in Bil(R/p)$ e $\tau^*(q) = q(p) \in Quad(R/p)$, onde $b(p)(\bar{x}, \bar{y}) = \overline{b(x,y)} = \tau(b(x,y))$ e $q(p)(\bar{x}) = \overline{q(x)} = \tau(q(x))$, para todo $x, y \in V$. Os espaços $b(p)$ e $q(p)$ são chamados as *reduções módulo* p de b e q, respectivamente. Esta redução pode ser

definida módulo um ideal I, qualquer, de R.

Considerando o fato que um módulo bilinear sobre um anel R é não singular se, e somente se suas localizações em ideais máximais de R ou, equivalentemente, suas reduções módulo ideais maximais de R são não singulares, deduzimos:

(3.4) Proposição - Seja (V,b) um módulo bilinear sobre R. São equivalentes:

(i) (V,b) $\in$ Bil(R)

(ii) $(V_{\wp}, b_{\wp}) \in$ Bil(R), para todo $\wp \in$ Spm(R)

(iii) (V($\wp$), b($\wp$)) $\in$ Bil(R), para todo $\wp \in$ Spm(R)

Vale um resultado análogo para o caso quadrático.

(3.5) Proposição - Seja (V,q) um módulo quadrático sobre R. São equivalentes:

(i) (V,q) $\in$ Quad(R)

(ii) $(V_{\wp}, q_{\wp}) \in$ Quad(R), para todo $\wp \in$ Spm(R)

(iii) (V($\wp$),q($\wp$)) $\in$ Quad(R), para todo $\wp \in$ Spm(R)

Vejamos agora uma maneira de fazermos a contração de espaços.

(3.6) O homomorfismo transfer - Seja i:R$\to$S um homomorfismo de anéis tal que S é um R-módulo (com respeito a i), livre de

dimensão finita n. Dizemos que S é uma *extensão de Frobenius* de R (de grau n), se existe uma função R-linear, $s: S \to R$ (chamada *função traço*) com a seguinte propriedade: a forma bilinear simétrica, $\bar{s}: S \times S \to R$, definida por $\bar{s}(x,y) = s(xy)$, para todo $x,y \in S$ é não singular, isto é $(S,\bar{s}) \in Bil(R)$.

Consideremos agora S uma extensão de Frobenius de R com função traço s. Dado $V \in L(S)$, consideremos V como um R-módulo via o homomorfismo $i: R \to S$, e o denotemos por V_R. Desde que $S \in L(R)$ segue-se que $V_R \in L(R)$. Agora definimos, para cada $(V,b) \in Bil(S)$. (resp. $(V,q) \in Quad(S)$), o módulo bilinear $s_*(V,b) = (V_R, sob)$, (resp. o módulo quadrático $s_*(V,q) = (V_R, soq)$). Temos então:

(3.7) Proposição - $s_*(V,b) \in Bil(R)$ (resp. $s_*(V,q) \in Quad(R)$).

Dem.: Ver [B] Prop. (2.8), Chap. I■

De (3.7) segue-se que $s_*: Bil(S) \to Bil(R)$ e $s_*: Quad(S) \to Quad(R)$, onde $s_*(V,b) = (V_R, sob)$ e $s_*(V,q) = (V_R, soq)$, são dois funtores aditivos que dão a contração dos espaços (V,b) e (V,q) respectivamente.

§ 4 - Subespaços

(4.1) Definições - Seja (V,q) (resp. (V,b)) um módulo quadrático (resp. um módulo bilinear) sobre um anel R. Para cada subconjunto

E de V, consideremos o submódulo de V, $E^{\perp_q} = \{x \in V;\ b_q(x,y)=0,$ para todo $y \in E\}$. (resp. $E^{\perp}=\{x \in V;\ b(x,y)=0,$ para todo $y \in E\}$). Dizemos que dois subconjuntos E, U de V são *ortogonais* se $E \subseteq U^{\perp}$ (ou equivalente $U \subseteq E^{\perp}$). O subconjunto E de V é dito ser *totalmente isotrópico* se $E \subseteq E^{\perp}$ e, no caso quadrático se além disso $q(E) = 0$. Um submódulo $E \subseteq V$ é um *subespaço* de (V,q) (resp. de (V,b)) se E é um somando direto de V.

Se temos $V = E \oplus U$, com $U \subseteq E^{\perp}$, escrevemos $V = E \perp U$ e dizemos que V é uma *soma ortogonal* de E e U. A restrição da forma quadrática q (resp. da forma bilinear b) ao subespaço $E \subseteq V$, será denotada por $(E, q|_E)$ (resp. $(E, b|_E)$). É claro que se $V = E \perp U$, então $(V,q) \simeq (E, q|_E) \perp (U, q|_U)$ (resp. $(V,b) \simeq (E,b|_E) \perp (U,b|_U)$). Um elemento $x \in V$ é dito ser *estritamente isotrópico* se Rx é um subespaço totalmente isotrópico de V. Um elemento $y \in V$ é dito ser *estritamente anisotrópico* se Ry é um subespaço de V com $q(y) \in R^*$ (resp. $b(y,y) \in R^*$).

(4.2) Proposição - Seja $V \in L(R)$ um módulo quadrático (resp. bilinear).

(i) Se V é não singular e $E \subseteq V$ é um subespaço, então $E^{\perp}$ é um subespaço e $E=E^{\perp\perp}$.

(ii) Se $E \subseteq V$ é um submódulo tal que $(E,q|_E)$ (resp. $(E,b|_E)$) é não singular, então E é um subespaço de V e $V = E \perp E^{\perp}$.

Dem.: Ver [B], Prop. (3.2), Chap. I■

Seja (V,b) um espaço bilinear sobre R. Consideremos o ideal de R gerado pelo conjunto $\{b(x,x);\ x \in V\}$. Se este ideal é todo o anel R, dizemos que (V,b) é *próprio*, caso contrário dizemos que (V,b) é *impróprio*.

(4.3) Teorema - Seja (V,b) um espaço bilinear sobre um LG - anel R.

(i) Se (V,b) é próprio, então (V,b) é uma soma ortogonal de subespaços de dimensão 1.

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

Dem.: Se $\dim_R V = 1$. nada há a demonstrar.

Podemos então supor que $\dim_R V \geq 2$. Consideremos uma base $(x_1,\ldots,x_n)$ de V sobre R. Mostraremos, primeiramente, que existem $w_1 = \sum_{i=1}^{n} \alpha_i x_i$ e $w_2 = \sum_{i=1}^{n} \beta_i x_i$, elementos de V, tais que $\det(b(w_i,w_j)) \in R^*$ e que, quando (V,b) é próprio, também é possível escolher w_1, tal que $b(w_1,w_1) \in R^*$. Desde que R é um LG-anel, basta mostrarmos a existência de tais elementos localmente.

Dado $p \in \mathrm{Spm}(R)$, seja (V_p,b_p) a localização de (V,b) em p (cf.(3.2)). Consideraremos separadamente os casos próprio e impróprio.

Caso 1: (V_p,b_p) é próprio.

De (V_p,b_p) ser próprio segue-se que existe $x \in V_p$ tal que

$b_{\mathfrak{p}}(x,x) \in R_{\mathfrak{p}}^{*}$. De (4.2)(i), $(V_{\mathfrak{p}},b_{\mathfrak{p}}) \simeq (R_{\mathfrak{p}}x,b_{\mathfrak{p}}) \perp (V_1,b_{\mathfrak{p}})$, onde $V_1=(R_{\mathfrak{p}}x)^{\perp}$. Por simplicidade denotamos também por $b_{\mathfrak{p}}$ as suas restrições aos subespaços $R_{\mathfrak{p}}x$ e V_1. Se $(V_1,b_{\mathfrak{p}})$ é próprio, de maneira análoga, existe $x' \in V_1$ tal que $b_{\mathfrak{p}}(x',x') \in R_{\mathfrak{p}}^{*}$. Neste caso, $w_1 = x$ e $w_2 = x'$ satisfazem o requerido. Agora, se $(V_1,b_{\mathfrak{p}})$ não é próprio, existem $y, z \in V_1$ tais que $b_{\mathfrak{p}}(y,z) \in R_{\mathfrak{p}}^{*}$, pois $(V_1,b_{\mathfrak{p}})$ é não singular. Basta então tomarmos $w_1 = x + y$ e $w_2 = x + \lambda z$, com $\lambda = -\frac{b(x,x)}{b(y,z)}$

Caso 2: $(V_{\mathfrak{p}},b_{\mathfrak{p}})$ é impróprio.

Seja $b_{ij} = b(x_i,x_j)$. Desde que a matriz $\left(\frac{b_{ij}}{1}\right)$ é inversível sobre $R_{\mathfrak{p}}$, cada linha ou cada coluna de $\left(\frac{b_{ij}}{1}\right)$ gera $R_{\mathfrak{p}}$ e, como $\frac{b_{ii}}{1} \in \mathfrak{p}R_{\mathfrak{p}}$, para todo $i = 1,\ldots,n$ e $R_{\mathfrak{p}}$ é local, cada linha de $\left(\frac{b_{ij}}{1}\right)$ contém pelo menos uma unidade de $R_{\mathfrak{p}}$ do tipo $\frac{b_{ij}}{1}$, com $i \neq j$. Assim, podemos reordenar as linhas de (b_{ij}) de maneira a termos $\begin{pmatrix} \frac{b_{11}}{1} & \frac{b_{12}}{1} \\ \frac{b_{21}}{1} & \frac{b_{22}}{1} \end{pmatrix}$ inversível sobre $R_{\mathfrak{p}}$. Isto mostra que existe uma matriz mudança de base M (que reordena as linhas de $\left(\frac{b_{ij}}{1}\right)$ tal que para $w_1 = M\left(\frac{x_1}{1}\right)$ e $w_2 = M\left(\frac{x_2}{1}\right)$, temos $\det(b(w_i,w_j)) \in R_{\mathfrak{p}}^{*}$.

Agora, se (V,b) é próprio, então $(V_{\mathfrak{p}},b_{\mathfrak{p}})$ é próprio para todo $\mathfrak{p} \in \mathrm{Spm}(R)$. Pelo *Caso* 1, existem w_1, w_2 em V, tais que $b(w_1,w_1)\det(b(w_i,w_j)) \in R^{*}$, o que mostra que $(V,b) \simeq (Rw_1+Rw_2,b) \perp (V_2,b)$ onde $V_2 = (Rw_1 + Rw_2)^{\perp}$ (cf. (4.2)(ii)). Mas $b(w_1,w_1) \in R^{*}$ e $(Rw_1 + Rw_2,b)$ é não singular, então existem

u_1, $u_2 \in Rw_1+Rw_2$ tais que $b(u_1,u_1)b(u_2,u_2) \in R^*$ e $b(u_1,u_2) = 0$ o que mostra que $(V,b) \simeq (Rw_1,b) \perp (V_1,b)$, com (V_1,b) próprio. Aplicando indução sobre $\dim_R V$ temos (i).

Se (V,b) é impróprio, do *Caso* 1 e 2 segue-se que $(V,b) \simeq (V_1,b) \perp (V_2,b)$, com $\dim_R V_1 = 2$. Considerando que se (V,b) é impróprio, então todo subespaço de (V,b) também o é, temos por indução sobre $\dim_R V$ que $(V,b) \simeq (V_1,b) \perp \ldots \perp (V_r,b)$ com $\dim_R V_i = 2$, $1 \leq i \leq r$. Isto mostra também, em particular, que se (V,b) é impróprio, então $\dim_R V$ é par.

Para provarmos completamente (ii) resta mostrar que cada subespaço de dimensão 2 pode ser escrito na forma $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$, com $1-\alpha\beta \in R^*$. Para tanto, consideremos w_1, $w_2 \in V$, com $\det(c_{ij}) \in R^*$, onde $c_{ij} = b(w_i,w_j)$, $1 \leq i, j \leq 2$. Desde que (c_{ij}) é inversível temos que o ideal gerado por uma linha de (c_{ij}) é o anel todo, em particular $(c_{21}, c_{22}) = R$, o que é equivalente a $(c_{21}, c_{22})_p = R_p$, para todo $p \in \mathrm{Spm}(R)$. Logo c_{21} ou c_{22} é uma unidade em R_p, o que significa que o polinômio $h(X) = c_{21} + c_{22}X$ representa uma unidade em R_p, para todo $p \in \mathrm{Spm}(R)$. Então existe $y \in R$, tal que $c_{21} + c_{22}\, y \in R^*$.

Temos então:

$$\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = \begin{pmatrix} c_{11} + 2c_{12}y + c_{22}y^2 & c_{21}+c_{22}y \\ c_{21}+c_{22}y & c_{22} \end{pmatrix}$$

ou seja, via uma mudança de base obtemos uma nova base (w_1', w_2') de $Rw_1 + Rw_2$, com $b(w_1', w_2') = c \in R^*$. Tomando $w_1'' = w_1'$ e $w_2'' = c^{-1}w_2'$ temos $(Rw_1 + Rw_2,b) \simeq \begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$ com $1-\alpha\beta \in R^*$, como queríamos ■

Para o caso quadrático temos o seguinte teorema de decomposição:

(4.4) Teorema - Seja (V,q) um espaço quadrático sobre um LG-anel R, com $\dim_R V = n$.

(i) Se $2 \in R^*$, então existem $\lambda_1,\ldots,\lambda_n \in R^*$, tais que $(V,q) \simeq [\lambda_1] \perp \ldots \perp [\lambda_n]$ (isto é, (V,q) tem uma base ortogonal $(x_1,\ldots,x_n)$, com $q(x_i) = \lambda_i \in R^*$).

(ii) Se $2 \notin R^*$, então $n = 2m$ e existem $\alpha_i, \beta_i \in R$, $1 \leq i \leq m$, tais que $1-4\alpha_i\beta_i \in R^*$ e $(V,q) \simeq [\alpha_1,\beta_1] \perp \ldots \perp [\alpha_m,\beta_m]$ isto é, (V,q) tem uma base $(x_i, y_i, 1 \leq i \leq m)$, com $q(x_i) = \alpha_i$, $q(y_i) = \beta_i$, $b_q(x_i,y_i) = 1$ e $1 - 4\alpha_i\beta_i \in R^*$, $1 \leq i \leq m$).

Dem.: (i) Se $2 \in R^*$, então (V,b_q) é próprio. De fato, se (V,b_q) é impróprio, existe $\wp \in \mathrm{Spm}(R)$ tal que $(V_\wp,(b_q)_\wp)$ é impróprio, o que implica que $b_q(x,x) \in \wp R_\wp$, para todo $x \in V$. Mas $b_q(x,x) = 2q(x)$ e $2 \in R^*$, logo $q(x) \in \wp R_\wp$, para todo $x \in V$. Portanto $b_q(x,y) = q(x+y) - q(x) - q(y) \in \wp R_\wp$, para todo $x,y \in V$, o que é uma contradição, pois $(V_\wp,(b_q)_\wp)$ é não singular (cf. (3.4)).

De (4.3)(i) segue-se que existe $x \in V$ tal que $b_q(x,x) \in R^*$, isto é, $2q(x) \in R^*$. Desde que $2 \in R^*$, segue-se que $q(x) = \alpha_1 \in R^*$ e, consequentemente $q \simeq [\alpha_1] \perp [\alpha_1]^\perp$. Agora (i) segue-se por indução sobre n.

(ii) Se $2 \notin R^*$, então (V,b_q) é impróprio, pois caso contrário existiria $x \in V$ tal que $b_q(x,x) = 2q(x) \in R^*$, (cf. (4.3)(i)). Logo, segue de (4.3) (ii) que (V,b_q) é soma de subespaços de

dimensão 2 do tipo $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$ com $1-\alpha\beta \in R^*$. Considerando que $b_q(x,x) = 2q(x)$, para todo $x \in V$, o resultado segue-se■

Deste teorema segue-se facilmente que qualquer espaço quadrático (V,q) sobre um LG-anel R tem a forma $V \cong \overset{n}{\underset{i=1}{\perp}} (Rx_i \oplus Ry_i)$, ou $V \cong \left(\overset{n}{\underset{i=1}{\perp}} (Rx_i \oplus Ry_i) \right) \perp (Rg)$, onde $b_q(x_i,y_i) = 1$, $(1 - 4q(x_i)q(y_i))q(g) \in R^*$. Além disso, podemos supor que $q(x_i)$ ou $q(y_i)$ é uma unidade para $1 \leq i \leq n$; pois caso contrário, existem x_i', $y_i' \in (Rx_i \oplus Ry_i)$ tais que $(Rx_i \oplus Ry_i) \cong (Rx_i' \oplus Ry_i')$ e $q(x_i') \in R^*$, $1 \leq i \leq n$. Observemos que, para que isto aconteça, é necessário e suficiente, que para cada $1 \leq i \leq n$ o polinômio $f(X_1, X_2, Y_1, Y_2) = (X_1Y_2 - X_2Y_1)(X_1Y_2 + X_2Y_1 + 2(q(x_i)X_1X_2 + q(y_i)Y_1Y_2))(q(x_i)X_1^2 + X_1Y_1 + q(y_i)Y_1^2)$ represente uma unidade em R, pois se $f(\lambda_1,\lambda_2,\gamma_1,\gamma_2) \in R^*$, então $x_i' = \lambda_1 x_i + \gamma_1 y_i$ e $y_i' = \lambda_2 x_i + \gamma_2 y_i$ satisfazem o requerido. Agora, com simples cálculos mostra-se que f representa um elemento não nulo em $R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, consequentemente f representa uma unidade em R. Uma base desta forma é chamada de *base canônica* para V. Se $q(x_i)q(y_i) \in R^*$, $1 \leq i \leq n$, dizemos que a base é *estritamente canônica*.

(4.5) Proposição - Se R é um LG-anel tal que $|R/\mathfrak{p}| \geq 4$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, então todo espaço quadrático sobre R admite uma base estritamente canônica.

Dem.: Usando (4.4) observamos que basta mostrarmos o resultado

para $(V,q) \in Quad(R)$ tal que $\dim_R V = 2$. Suponhamos então que $V = (Rx_1 \oplus Rx_2)$ com $q(x_1) = \alpha \in R^*$, $q(x_2) = \beta \notin R^*$ e $b_q(x_1,x_2) = 1$, ou seja, que $q = [\alpha,\beta]$. Se encontrarmos $x \in V$ tal que $q(x)b_q(x_1,x) \in R^*$ e (x_1, x) forme uma base para V, então a base $(x_1, x/b_q(x_1,x))$ é estritamente canônica.

Tomando $x = x_1 + \lambda x_2$, temos que (x_1, x) é uma base de V se, e somente se, $\lambda \in R^*$.

Considerando $h(X) = X(\alpha + X + \beta X^2)(2\alpha + X) \in R[X]$, temos que $h(X)$ representa uma unidade em R_p para todo $p \in Spm(R)$ tal que $|R/p| > 4$, pois $R_p/pR_p \cong R/p$ e o grau de h é ≤ 4. Se $|R/p| = 4$, então $2 = 0$ em R/p e, consequentemente h representa uma unidade em R_p se, e somente se $g(X) = X(\alpha + X + \beta X^2)$ representa.

Como grau de $g \leq 3$ concluímos que h representa uma unidade em R_p para todo $p \in Spm(R)$ com $|R/p| \geq 4$, ou seja h representa uma unidade em R. Logo existe $\lambda \in R^*$ tal que $(x_1, x_1 + \lambda x_2)$ é uma base de V, com $q(x_1 + \lambda x_2)b_q(x_1, x_1 + \lambda x_2) = \frac{h(\lambda)}{\lambda} \in R^*$ como queríamos■

§ 5 - Espaços Hiperbólicos

(5.1) Definição - Seja $U \in L(R)$. Definimos em $U \oplus U^*$ a forma quadrática q_U, por $q_U(x + x^*) = x^*(x)$, para todo $x \in U$ e $x^* \in U^*$. A forma bilinear associada é dada por $b_U(x + x^*, y + y^*) = x^*(y) + y^*(x)$ para todo $x,y \in U$ e $x^*, y^* \in U^*$. De (4.4) Chap I de [B] temos que $(U \oplus U^*, q_U)$ é não singular. O espaço quadrático

$(U \oplus U^*, q_U)$ é chamado o *espaço hiperbólico* associado a $U \in L(R)$ e é denotado por $H(U)$.

De maneira similar podemos construir espaços bilineares hiperbólicos. Consideremos (V,b) um módulo bilinear sobre R. Definimos no módulo $V \oplus V^*$ uma forma bilinear simétrica b_V, por $b_V(x + x^*, y + y^*) = b(x,y) + x^*(y) + y^*(x)$, para todo $x, y \in V$ e $x^*, y^* \in V^*$. De (4.4), Chap I de [B], temos que $(V \oplus V^*, b_V) \in Bil(R)$. O espaço bilinear $(V \oplus V^*, b_V)$, é chamado o *espaço metabólico* associado à (V,b) e denotado por $M(V)$. Mas, no caso especial em que $b = 0$, escrevemos $H(V)$ no lugar de $M(V)$. O espaço $H(V)$ é também chamado o *espaço bilinear hiperbólico* associado a $V \in L(R)$.

Observe que em $H(U)$ existem dois subespaços totalmente isotrópicos U e U^* tais que $U = U^\perp$ e $U^* = (U^*)^\perp$. Em $M(V)$, em geral, somente V^* é totalmente isotrópico.

Se $U = Rx$, então $H(U) = [0,0]$. Similarmente, se $b = \langle\alpha\rangle$, $\alpha \in R$, é uma forma bilinear, então $M(\langle\alpha\rangle) = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$. Mais geralmente, se $U = Rx_1 \oplus \ldots \oplus Rx_n$, então $H(U) = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ onde $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_{n \times n}$, isto é, $H(U) = [0,0] \perp \ldots \perp [0,0]$ (n-vezes). Denotaremos o plano hiperbólico $[0,0]$ por H. Analogamente, temos para o módulo bilinear $(V,b) = \langle\alpha_1\rangle \perp \langle\alpha_2\rangle \perp \ldots \perp \langle\alpha_n\rangle = \langle\alpha_1, \ldots, \alpha_n\rangle$, $M(\langle\alpha_1, \ldots, \alpha_n\rangle) = \begin{pmatrix} \alpha_1 & 1 \\ 1 & 0 \end{pmatrix} \perp \ldots \perp \begin{pmatrix} \alpha_n & 1 \\ 1 & 0 \end{pmatrix}$.

(5.2) Proposição ([B], Prop. (4.5), Chap I) - Para $U, V \in L(R)$ temos $H(U \oplus V) \simeq H(U) \perp H(V)$ e, para qualquer módulo bilinear (U,b),

com $U = U_1 \perp U_2$, temos $\mathbb{H}(U) \simeq \mathbb{H}(U_1) \perp \mathbb{H}(U_2)$.

Dem.: Imediata■

O próximo teorema dá uma caracterização dos espaços hiperbólicos e metabólicos.

(5.3) Teorema ([B], Th(4.6), Chap. I) - Seja V um espaço quadrático ou bilinear sobre R. Então V é hiperbólico (resp. metabólico) se, e somente se, V contém um subespaço totalmente isotrópico U, com $U = U^{\perp}$. Além disso, no caso quadrático, $V \simeq \mathbb{H}(U)$.

Dem.: Provaremos o teorema para espaços quadráticos. O caso bilinear pode ser tratado de maneira análoga.

Se (V,q) é hiperbólico, segue-se da definição de espaços hiperbólicos, que existe U como requerido. Agora, se (V,q) é um espaço quadrático com um subespaço U, tal que $q(U) = 0$ e $U = U^{\perp}$, então por [B] Cor(3.8), Chap I, existe $E \subseteq V$, com $q(E) = 0$, $d_q : E \to U^*$ um isomorfismo e $V \cong U \oplus E$. Definimos $\varphi : V \to \mathbb{H}(U) = U \oplus U^*$, por $\varphi(u + v) = u + d_q(v)$, para todo $u \in U$ e $v \in E$. Claramente φ é um isomorfismo de R-módulos. Mais ainda, φ é uma isometria de espaços quadráticos, pois $q(u) = q(v) = 0$ e $q_U(\varphi(u + v)) = q_U(u + d_q(v)) = d_q(v)(u) = b_q(u,v) = q(u + v)$, para todo $u \in U$ e $v \in E$, o que prova o teorema■

(5.4) Carolário ([B] Cor.(4.7), Chap. I) - (i) Para $(V,q) \in Quad(R)$, tem-se $(V,q) \perp (V,-q) \simeq \mathbb{H}(V)$.

(ii) Para $(U,b) \in Bil(R)$, tem-se $(U,b) \perp (U,-b) \simeq \mathbb{H}(U)$.

(iii) Para $P \in L(R)$, $(V,q) \in Quad(R)$, $(E,b) \in Bil(R)$ e (U,b') um módulo bilinear qualquer, tem-se:

$$\mathbb{M}(U) \otimes (V,q) \simeq \mathbb{H}(U \otimes V)$$

$$(E,b) \otimes \mathbb{H}(P) \simeq \mathbb{H}(E \otimes P)$$

$$\mathbb{H}(P) \circ (V,q) \simeq \mathbb{H}(P \otimes V)$$

$$\mathbb{M}(U) \otimes (E,b) \simeq \mathbb{M}(U \otimes E)$$

Dem.: Imediata■

§ 6 - O Teorema do Cancelamento de Witt

O nosso objetivo, neste parágrafo, é provar o teorema do cancelamento de Witt para espaços quadráticos sobre um LG-anel. Para tanto, introduziremos alguns resultados auxiliares.

Seja (V,q) um espaço quadrático sobre um anel R. Para quaisquer $x, y \in V$, tais que $q(x) = 0$ e $b_q(x,y) = 0$ (isto é, $y \in (Rx,q)^{\perp}$), indiquemos por $E(x,y)$ a aplicação R-linear, $E(x,y): V \to V$, dada por:

$E(x,y)(z) = z - b_q(z,x)y + b_q(z,y)x - q(y)b_q(z,x)x$, para todo $z \in V$.

Se V tem uma decomposição $V \simeq (Ru \oplus Rv) \perp V_o$, onde $(Ru \oplus Rv)$ é um plano hiperbólico e $V_o \neq 0$, para qualquer $\lambda \in R^*$, indiquemos por $\phi(\lambda)$ a aplicação R-linear $\phi(\lambda): V \to V$, dada por: $\phi(\lambda)(u) = \lambda u$, $\phi(\lambda)(v) = \lambda^{-1}v$ e $\phi(\lambda)(x) = x$, para todo $x \in V_o$.

Com simples cálculos mostra-se que $E(x,y)$ e $\phi(\lambda)$

são isometrias de V. A aplicação $E(x,y)$ é chamada a *transvecção de Siegel*.

(6.1) Lema - Sejam R um LG-anel e $(V,q) \in Quad(R)$ com uma decomposição $V \simeq (Ru \oplus Rv) \perp V_o$, onde $(Ru \oplus Rv)$ é um plano hiperbólico e $V_o \neq 0$. Seja $x = \alpha u + \beta v + z$; $\alpha, \beta \in R$ e $z \in V_o$, um vetor unimodular de V; isto é, $b_q(x,V) = R$. Assumamos uma das seguintes condições:

(i) $|R/\mathfrak{p}| \geq 3$, para todo $\mathfrak{p} \in Spm(R)$

(ii) x é isotrópico.

Então, existe $y \in V_o$ tal que $E(u,y)(x) = \alpha' u + \beta v + z'$ com $\alpha' \in R^*$ e $z' \in V_o$.

Dem.: Seja $(x_1,\ldots,x_n)$ uma base de V_o. Temos então $b_q(u,x_i) = b_q(v,x_i) = 0$ para $1 \leq i \leq n$. Queremos encontrar $y = \sum_{i=1}^{n} \lambda_i x_i \in V_o$ tal que $(\alpha + b_q(y,z) - q(y)\beta) \in R^*$, pois $E(u,y)(x) = (\alpha + b_q(y,z) - q(y)\beta)u + \beta v + (z - \beta y)$. Ou seja, queremos mostrar que $f(Y_1,\ldots,Y_n) = \alpha + \sum_{i=1}^{n} b_q(z,x_i)Y_i - \beta \sum_{i,j=1}^{n} b_q(x_i,x_j)Y_iY_j \in R[Y_1,\ldots,Y_n]$, representa uma unidade em R.

Inicialmente, assumamos (i) e observemos que, do fato de x ser unimodular, temos que x é *primitivo*, isto é os coeficientes de x não são todos nulos em $R/\mathfrak{p}$, para todo $\mathfrak{p} \in Spm(R)$, o que implica que f é um polinômio não nulo localmente. Desde que f tem grau ≤ 2 e $|R/\mathfrak{p}| \geq 3$, para todo $\mathfrak{p} \in Spm(R)$, segue-se que f representa uma unidade em $R_{\mathfrak{p}}$, para todo $\mathfrak{p} \in$

$\in$ Spm(R), o que mostra o lema no caso (i).

Assumamos agora (ii), ou seja que x é isotrópico, e mostremos que f representa uma unidade localmente.

Seja $p \in$ Spm(R). Se $\frac{\alpha}{1} \notin pR_p$, então $f(0,\ldots,0) = \alpha \in R_p^*$. Se $\frac{\alpha}{1} \in pR_p$, procuremos determinar $y \in V_o$ tal que $b_q(y,z) - \beta q(y) \notin pR_p$. Observemos que x é isotrópico, o que acarreta $\alpha\beta + q(z) = 0 \in pR_p$ e, desde que $\alpha \in pR_p$, temos $q(z) \in pR_p$, o que mostra que $\bar{z} = 0$ ou $\bar{z}$ é isotrópico em $(V_o(p), q(p))$. Desde que $(V_o(p), q(p)) \in Quad(R/p)$, (cf.(3.5)), se $\bar{z}$ é isotrópico temos que existe $y \in V_o$ tal que $\overline{q(y)} = 0$ e $\overline{b_q(y,z)} = 1$ em R/p, ou seja, existe $y \in V_o$ tal que $q(y) \in pR_p$ e $b_q(y,z) \notin pR_p$ ($R/p \cong Rp/pR_p$). Assim, existe $y \in V_o$ tal que $f(y) = \alpha + b_q(y,z) - \beta q(y) \in R_p^*$. Se $\bar{z} = 0$, então $\bar{\beta} \neq 0$, pois x é primitivo. Neste caso, considerando que $(V_o(p), q(p))$ é não singular (cf.(3.5)), existe $y \in V_o$ tal que $q(y) \neq 0$, ou seja, $q(y) \notin pR_p$ e desde que $\beta \notin pR_p$, temos que $f(y) \in R_p^*$. Disto segue-se o lema no caso (ii)■

Sejam $(V,q) \in Quad(R)$ e $(E, q|_E)$ um subespaço de (V,q). Uma *isometria*, $\varphi: E \to V$, é um monomorfismo de R-módulo tal que $q(\varphi(x)) = q(x)$, para todo $x \in E$ e, $\varphi(E)$ é um subespaço de V.

(6.2) Lema - Seja R um LG-anel, sejam $(V,q) \in Quad(R)$, com uma decomposição como em (6.1), e $\mathbb{H} \leq V$ um plano hiperbólico. Então existe uma isometria, $\varphi: V \to V$, que leva $(Ru \oplus Rv)$ em $\mathbb{H}$.

Dem.: Seja (i,j) uma base para $\mathbb{H}$, com $q(i) = q(j) = 0$ e $b_q(i,j) = 1$. O elemento i é da forma $\alpha u + \beta v + z$; $\alpha, \beta \in R$ e $z \in V_o$. Usando o fato de i ser unimodular e isotrópico de (6.1) podemos supor que $\alpha \in R^*$.

Observemos que $E(v,\alpha^{-1}z)(u) = u - \alpha^{-1}z - \alpha^{-2}q(z)v$, e $q(i) = \alpha\beta + q(z) = 0$, o que implica que $\beta = -\alpha^{-1}q(z)$ e, consequentemente $E(v, \alpha^{-1}z)(u) = \alpha^{-1}(\alpha u - \alpha^{-1}q(z)v + z) = \alpha^{-1}i$. Tomando a isometria $\psi = E(v, \alpha^{-1}z)\phi(\alpha)$, temos $\psi(u) = i$, ou seja, ψ leva $(Ru \oplus Rv)$ em $(Ri \oplus R\psi(v))$ que é um plano hiperbólico de V.

Considerando $w = \psi(v)$ e a decomposição $V \simeq (Ri \oplus \oplus Rw) \perp V_1$, temos que o elemento $j \in V$ pode ser escrito na forma $j = \lambda i + \gamma w + z'$ com $\lambda, \gamma \in R$ e $z' \in V_1$. Desde que $b_q(i,w) = b_q(i,j) = 1$ e j é isotrópico, temos que $\gamma = 1$ e $\lambda = -q(z')$. Então $E(i,z')(w) = w - q(z')i + z' = j$ e $E(i,z')(i) = i$. Logo $\varphi = E(i,z')\psi$ satisfaz o requerido.

A demonstração do principal teorema deste parágrafo, que veremos a seguir, foi feita por Knebush no caso de um anel semi-local e posteriormente reproduzida por Baeza em [B].

(6.3) Teorema - Seja R um LG-anel, sejam $(V,q) \in Quad(R)$ e $(E,q|_E)$ um subespaço não singular de (V,q). Cada isometria $\varphi: E \to V$ pode ser estendida a uma isometria $\phi: V \to V$.

Dem.: Desde que $(E,q|_E)$ é um subespaço não singular de (V,q), temos de (4.2)(ii), que $V = E \perp E^{\perp}$. Consideremos o espaço $V \perp$

$\perp -E \simeq E \perp -E \perp E^{\perp} \simeq \mathbb{H}(E) \perp E^{\perp}$.

A isometria $\varphi: E \to V$ induz uma isometria $\varphi' = \varphi \perp id_{(-E)}: \mathbb{H}(E) \to V \perp -E$ e, cada extensão $\tilde{\varphi}'$ de φ' à $V \perp -E$ nos dá uma extensão de φ à V. De fato, basta observarmos que $(-E)^{\perp} = V$ em $V \perp -E$ e que $\tilde{\varphi}'|_{(-E)} = \varphi'|_{(-E)} = id_{(-E)}$ donde segue-se que $\tilde{\varphi}': (-E)^{\perp} \simeq (-E)^{\perp}$, ou seja $\tilde{\varphi}'|_{V}$ é uma extensão de φ a V. Assim podemos supor que E é hiperbólico, ou seja, que $E = \mathbb{H}_1 \perp \ldots \perp \mathbb{H}_n$, onde $\mathbb{H}_i = Ru_i \oplus Rv_i$ são planos hiperbólicos. A demonstração segue-se agora, por indução sobre n.

Se $n = 1$ o lema (6.2) garante a existência da extensão de φ. Suponhamos então que $n > 1$.

Consideremos a restrição de φ, $\varphi_1: \mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1} \to V$. Por hipótese de indução existe uma isometria, $\sigma: V \to V$, que estende φ_1. Então $\sigma^{-1}\varphi: E \to V$ é uma isometria que é a identidade em $\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1}$. Logo a restrição de $\sigma^{-1}\varphi$ à $\mathbb{H}_n$ é uma isometria $\sigma^{-1}\varphi: \mathbb{H}_n \to (\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1})^{\perp}$.

Como $\mathbb{H}_n \subseteq (\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1})^{\perp}$, do que vimos acima segue-se que $\sigma^{-1}\varphi$ se estende a um isometria τ de $(\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1})^{\perp}$, logo $\psi = id|_{\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1}} \perp \tau: V \to V$ é uma extensão de τ à V tal que $\psi|_{\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1}} = id_{\mathbb{H}_1 \perp \ldots \perp \mathbb{H}_{n-1}}$. Agora, é imediato ver que $\phi = \sigma\psi: V \to V$ é uma extensão de φ requerida■

(6.4) Carolário (Teorema do Cancelamento de Witt) - Sejam (V_i, q_i), $1 \leq i \leq 3$, espaços quadráticos sobre um LG-anel R tais que $V_1 \perp V_2 \simeq V_1 \perp V_3$. Então $V_2 \simeq V_3$ (ou seja, se $q_1 \perp q_2 \simeq q_1 \perp q_3$,

então $q_2 \simeq q_3$).

Dem.: Sejam $\sigma: V_1 \perp V_2 \to V_1 \perp V_3$ uma isometria e $i: V_1 \to V_1 \perp V_2$ a inclusão. Do teorema (6.3) segue-se que $\sigma i: V_1 \to V_1 \perp V_3$ admite uma extensão à uma isometria $\psi: V_1 \perp V_3 \to V_1 \perp V_3$. Portanto a isometria $\varphi = \sigma^{-1}\psi: V_1 \perp V_3 \to V_1 \perp V_2$ satisfaz $\varphi|_{V_1} = id_{V_1}$, o que mostra que $\varphi|_{V_3}$ é uma isometria de V_3 em V_2, isto é, $V_2 \simeq V_3$, como queríamos■

(6.5) Observação - O teorema do cancelamento de Witt não vale em geral para espaços bilineares sobre um LG-anel R, pois se, por exemplo, R é um corpo de característica 2, temos $\langle 1,1,1,1\rangle \simeq \langle 1,1\rangle \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e $\langle 1,1\rangle$ não é isométrico a $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Mas, se $2 \in R^*$ decorre de (1.3) que, o teorema do cancelamento de Witt vale em Bil(R).

CAPÍTULO III

OS ANÉIS W(R) e $W_q(R)$

Neste capítulo faremos um estudo da estrutura do anel de Witt dos espaços bilineares, W(R), e do anel de Witt dos espaços quadráticos, $W_q(R)$, sobre um LG-anel. Mais especificamente, daremos uma descrição dos ideais primos e dos geradores de W(R) e apresentaremos alguns resultados sobre os elementos nilpotentes e os elementos de torção de W(R) e $W_q(R)$. Em todo este capítulo, salvo menção contrária, R significará sempre um LG-anel.

Às categorias Bil(R) e Quad(R) associamos seus correspondentes anéis de Grothendieck, $K_o(Bil(R))$ e $K_o(Quad(R))$ (cf.[Ba]), os quais são chamados, respectivamente, *anel de Witt - - Grothendieck dos espaços bilineares sobre R e anel Witt-Grothendieck dos espaços quadráticos sobre R*. Tais anéis são denotados, respectivamente por, $\hat{W}(R)$ e $\hat{W}_q(R)$.

O anel $\hat{W}(R)$ tem um elemento identidade que é representado pelo espaço bilinear $\langle 1 \rangle$, enquanto que, se $2 \in R^*$, o anel $\hat{W}_q(R)$ não tem elemento identidade. Se $2 \in R^*$ podemos identificar $\hat{W}(R)$ e $\hat{W}_q(R)$ (cf.(II.1.3)). Em geral $\hat{W}_q(R)$ é uma W(R)-álgebra.

Se [q] denota a classe de isometria do espaço quadrático q, então os elementos de de $\hat{W}_q(R)$ são as diferenças

formais $[q_1] - [q_2]$, de classes $[q_1]$ e $[q_2]$, onde por definição $[q_1] - [q_2] = [q_1'] - [q_2']$ se, e somente se, existe $q \in$ $\in Quad(R)$ tal que $q_1 \perp q_2' \perp q \cong q_1' \perp q_2 \perp q$. Respectivamente, temos o mesmo fato em $\hat{W}(R)$. Observemos que, no caso quadrático, vale o teorema do cancelamento de Witt e consequentemente, $[q_1] - [q_2] = [q_1'] - [q_2']$ se, e somente se, $q_1 \perp q_2' \simeq q_1' \perp q_2$.

Sejam $\hat{M}(R) = \{[b] - [b'] \in \hat{W}(R);$ b e b' são metabólicos$\}$ e $\hat{H}(R) = \{[q] - [q'] \in \hat{W}_q(R);$ q e q' são hiperbólicos$\}$. De (II,5.4,(iii)), decorre que $\hat{M}(R)$ e $\hat{H}(R)$ são ideais de $\hat{W}(R)$ e $\hat{W}_q(R)$, resp. Assim, definimos, $W(R) = \hat{W}(R)/\hat{M}(R)$, o *anel de Witt dos espaços bilineares sobre R* e, $W_q(R) = \hat{W}_q(R)/\hat{H}(R)$, *o anel de Witt dos espaços quadráticos sobre R*.

§ 1 - Geradores e Ideais Primos de W(R)

Os resultados deste parágrafo e do seguinte foram originariamente demonstrados por Knebush $[Kn]_3$ no caso de um anel semi-local.

Para o estudo dos geradores de W(R) utilizaremos o grupo $G = R^*/(R^*)^2$ e denotaremos por $\langle a \rangle$; $a \in R^*$ a classe de a em G.

(1.1) Proposição - W(R) é aditivamente gerado por G.

Dem.: Seja $[b] \in W(R)$. O espaço bilinear $b \perp \langle 1 \rangle$ é próprio e, consequentemente existem $\alpha_1, \ldots, \alpha_r \in R^*$ tais que $b \perp \langle 1 \rangle \simeq$

$\simeq \langle \alpha_1,\ldots,\alpha_r\rangle$ (cf.(II,4.3)). Assim $[b] = [b \perp \langle 1,-1\rangle] = [\langle \alpha_1,\ldots,\alpha_r,-1\rangle] = [\langle \alpha_1\rangle] \perp\ldots\perp [\langle \alpha_r\rangle] \perp [\langle -1\rangle]$ em $W(R)$■

De acordo com esta proposição, existe um homomorfismo de anéis sobrejetor, $\varphi: \mathbb{Z}[G]\to W(R)$, tal que $\varphi(\langle a\rangle) = [\langle a\rangle]$, para todo $\langle a\rangle \in G$. Se K é o núcleo de φ, então $W(R) \cong \mathbb{Z}[G]/K$. A próxima proposição caracteriza os elementos de K.

(1.2) Proposição- O ideal K é aditivamente gerado pelos elementos $\langle 1\rangle + \langle -1\rangle$ e todos os elementos da forma $z = \sum_{i=1}^{n}\langle \alpha_i\rangle - \sum_{i=1}^{n}\langle \beta_i\rangle$, para algum inteiro 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 K. Agora, seja $z = \sum_{i=1}^{r}\langle \alpha_i\rangle - \sum_{i=1}^{s}\langle \beta_i\rangle$ um elemento K. Trocando z por -z, se necessário, assumiremos 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 $W(R)$, ou seja, existem U_1, $U_2 \in$ $\in Bil(R)$ tais que $\langle \alpha_1,\ldots,\alpha_r\rangle \perp M(U_1) \simeq \langle \beta_1,\ldots,\beta_s\rangle \perp M(U_2)$. Mas, $\dim_R M(U_1)$ e $\dim_R M(U_2)$ são números pares, o que implica que $r - s$ é um número par 2t.

Sejam $E_1 = \langle \alpha_1,\ldots,\alpha_r\rangle$ e $E_2 = \langle \beta_1,\ldots,\beta_s\rangle \perp$ $\perp t\langle 1,-1\rangle$. Desde que $[E_1] = [E_2]$ em $W(R)$, temos que $[E_1] - [E_2] \in$ $\in \hat{M}(R)$ o que implica que existe $V \in Bil(R)$ tal que $[E_1] - [E_2] =$ $= [M(V)]$ em $\hat{W}(R)$, isto é, exite $V' \in Bil(R)$ tal que $E_1 \perp V' \simeq E_2 \perp$ $\perp M(V) \perp V'$. Mas $\dim_R E_1 = \dim_R E_2$ e, consequentemente, $\dim_R M(V) = 0$, isto é, $M(V) = 0$. Assim, existe $V' \in Bil(R)$ tal que $\langle \alpha_1,\ldots,\alpha_r\rangle \perp V' \simeq \langle \beta_1,\ldots,\beta_s\rangle \perp t\langle 1,-1\rangle \perp V'$. Somando $\langle 1\rangle$ em

ambos os lados, se necessário, podemos assumir que V' é próprio, ou seja $V' \simeq \langle \lambda_1, \ldots, \lambda_k \rangle$; $\lambda_i \in R^*$, $1 \leq i \leq k$ (cf.(II,4.3)). Tomando $\alpha_{r+1} = \lambda_1, \ldots, \alpha_{r+k} = \lambda_k$; $n = r + k$; $\beta_i = \pm 1$, $s < i \leq r$ e $\beta_i = \alpha_i$, $r < i \leq n$, temos $\langle \alpha_1, \ldots, \alpha_n \rangle \simeq \langle \beta_1, \ldots, \beta_n \rangle$ e $z = t(\langle 1 \rangle + \langle -1 \rangle) + \sum_{i=1}^{n} \langle \alpha_i \rangle - \sum_{i=1}^{n} \langle \beta_i \rangle$, como queríamos■

(1.3) Teorema - $W(R)$ é aditivamente gerado por $\{\langle \alpha \rangle;\ \alpha \in R^*\}$ com as seguintes relações:

(i) $\langle \alpha\lambda^2 \rangle = \langle \alpha \rangle$, para todo $\alpha, \lambda \in R^*$.

(ii) $\langle \alpha_1 \rangle + \ldots + \langle \alpha_n \rangle = \langle \beta_1 \rangle + \ldots + \langle \beta_n \rangle$ se, e somente se, $\langle \alpha_1, \ldots, \alpha_n \rangle \simeq \langle \beta_1, \ldots, \beta_n \rangle$

(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 $\alpha + \beta \in R^*$

(v) $\langle \alpha \rangle \langle \beta \rangle = \langle \alpha\beta \rangle$

Dem.: Para mostrarmos que (i), (ii), (iii) e (v) valem para $W(R)$ basta observarmos que $W(R) \cong \mathbb{Z}[G]/K$. Para vermos que (iv) vale, consideremos o espaço bilinear $(V,b) = \langle \alpha, \beta \rangle$ com uma base $\{x,y\}$ tal que, $b(x,y) = 0$, $b(x,x) = \alpha$ e $b(y,y) = \beta$. Então $b(x+y,x+y) = \alpha + \beta \in R^*$, o que implica que existe $z \in V$ tal que $\{x+y,z\}$ é uma base ortogonal para V, (cf.(II,4.2)), isto é, $b \simeq \langle \alpha+\beta \rangle \perp \perp \langle \gamma \rangle$, onde $b(z,z) = \gamma \in R^*$. Agora, comparando os determinantes, temos $\alpha\beta \equiv (\alpha+\beta)\gamma \bmod (R^*)^2$, isto é, $\gamma \equiv \alpha\beta(\alpha+\beta) \bmod (R^*)^2$ pois $(\alpha+\beta) \equiv (\alpha+\beta)^{-1} \bmod (R^*)^2$. Assim, por (i) e (ii) temos: $\langle \alpha \rangle + \langle \beta \rangle \simeq \langle \alpha+\beta \rangle + \langle \alpha\beta(\alpha+\beta) \rangle$■

Na demonstração da proposição (1.2) mostramos parte da seguinte proposição:

(1.4) Proposição - Sejam E_1, $E_2 \in Bil(R)$. $[E_1] = [E_2]$ em $\hat{W}(R)$ se, e somente se $[E_1] = [E_2]$ em $W(R)$, e $\dim_R E_1 = \dim_R E_2$.

Dem.: Se $[E_1] = [E_2]$ em $\hat{W}(R)$, então existe $V \in Bil(R)$ tal que $E_1 \perp V \simeq E_2 \perp V$ e, consequentemente, $\dim_R E_1 = \dim_R E_2$. Além disso, temos $E_1 \perp V \perp -V \simeq E_2 \perp V \perp -V$ o que implica que $E_1 \perp \mathbb{H}(V) \simeq E_2 \perp \perp \mathbb{H}(V)$ (conforme(II.5.4)), o que mostra que $[E_1] = [E_2]$ em $W(R)$. A recíproca esta demonstrada em (1.2)■

Caracterizaremos, agora, os ideais primos de $W(R)$ usando o fato que $W(R) \cong \mathbb{Z}[G]/K$, onde $G \cong R^*/(R^*)^2$ e K é bem determinado em (1.2); ou seja, usaremos o fato que os ideais primos de $W(R)$ estão em correspondência 1-1 com os ideais primos de $\mathbb{Z}[G]$ que contém K.

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

Seja G um grupo arbitrário de expoente 2, isto é, $g^2 = 1$ para todo $g \in G$. Se P é um ideal primo de $\mathbb{Z}[G]$, então $g \equiv \pm 1 \bmod P$, para cada $g \in G$. Logo $\mathbb{Z}[G]/P$ é isomorfo a $\mathbb{Z}$ ou a $\mathbb{F}_p$, onde $\mathbb{F}_p$ denota o corpo finito com p elementos. Desde que os anéis $\mathbb{Z}$ e $\mathbb{F}_p$ não tem automorfismos não triviais, obtemos:

(1.5) Lema - Para cada ideal primo P de $\mathbb{Z}[G]$, com $P \cap \mathbb{Z} = (0)$,

existe um único homomorfismo de anéis, $\varphi: \mathbb{Z}[G] \to \mathbb{Z}$, tal que $\mathrm{Ker}\varphi = P$. Similarmente, para cada ideal primo P de $\mathbb{Z}[G]$, com $P \cap \mathbb{Z} = p\mathbb{Z}$, p um número primo, existe um único homomorfismo de anéis $\psi: \mathbb{Z}[G] \to \mathbb{F}_p$, tal que $\mathrm{Ker}\psi = P$.

Assim, necessitamos somente descrever os homomorfismos φ e ψ. Cada homomorfismo de anéis de $\mathbb{Z}[G]$ em $\mathbb{Z}$ leva G em $\langle \pm 1 \rangle$. Logo, a restrição $\varphi|_G$ de φ a G, é um caracter $\chi: G \to \langle \pm 1 \rangle$. Reciprocamente, cada caracter, $\chi: G \to \langle \pm 1 \rangle$, se extende de maneira única a um homomorfismo de anéis , $\varphi: \mathbb{Z}[G] \to \mathbb{Z}$. Assim, identificamos φ e χ. Agora, seja p um número primo impar. O grupo $\langle \pm 1 \rangle \leq \mathbb{F}_p$, é o subgrupo de todos os elementos de $\mathbb{F}_p^*$ de ordem 2. Logo, a restrição de um homomorfismo de anéis, $\psi: \mathbb{Z}[G] \to \mathbb{F}_p$, a G é também um caracter $\chi: G \to \langle \pm 1 \rangle$.

Finalmente, consideremos p = 2. Cada homomorfismo de $\mathbb{Z}[G]$ em $\mathbb{F}_2$, leva todo $g \in G$ em 1. Logo, existe um único homomorfismo de anéis $\psi_o: \mathbb{Z}[G] \to \mathbb{F}_2$, que é obtido da composição de algum caracter, $\chi: G \to \mathbb{Z}$, com projeção canônica sobre $\mathbb{F}_2$.

Destas observações e do lema (1.5) temos:

(1.6) Proposição - (i) Para cada ideal primo P de $\mathbb{Z}[G]$, com $P \cap \mathbb{Z} = \langle 0 \rangle$, existe um único caracter χ de G, tal que $P = P_\chi$ é o núcleo de $\varphi_\chi: \mathbb{Z}[G] \to \mathbb{Z}$ (φ_χ é a extensão de χ).

(ii) Para cada ideal primo P de $\mathbb{Z}[G]$, com $P \cap \mathbb{Z} = p\mathbb{Z}$, onde p é um número primo impar, existe um único caracter χ de G tal que $P = P_{\chi,p} = p\mathbb{Z} + \mathrm{Ker}\varphi_\chi = p\mathbb{Z} + P_\chi$, que é o conjunto de todos os elementos z de $\mathbb{Z}[G]$, tais que $\varphi_\chi(z) \equiv 0 \bmod p$.

(iii) Existe um único ideal primo P_o de $\mathbb{Z}[G]$ com $P_o \cap \mathbb{Z} = 2\mathbb{Z}$ e, $P_o = (\varphi_\chi)^{-1}(2\mathbb{Z}) = 2\mathbb{Z} + P_\chi$, para cada caracter χ de G.

Claramente os P_χ são os ideais primos minimais de $\mathbb{Z}[G]$ e os ideais $P_{\chi,p}$ e P_o são os maximais.

Consideremos agora, $G = R^*/(R^*)^2$ e olhemos para os ideais primos de $W(R) \cong \mathbb{Z}[G]/K$.

Denotemos por I(R) o núcleo da função dimensão módulo 2, $d: W(R) \to \mathbb{F}_2$. Da parte (iii) da proposição (1.6), obtemos:

(1.7) Proposição - I(R) é o único ideal primo de W(R) que contém $2.1_{W(R)} = 2.[\langle 1\rangle]$.

No que se segue, todo homomorfismo de anéis, $\sigma: W(R) \to \mathbb{Z}$, sera' chamado *assinatura de R*. Denotamos $\ker\sigma = P_\sigma$ e, do que já vimos, temos $W(R)/P_\sigma \cong \mathbb{Z}$, para toda assinatura σ de R.

O próximo resultado segue-se de (1.6),(1).

(1.8) Proposição - Para cada ideal primo P de W(R), que não contém $p[\langle 1\rangle]$, para todo primo impar p, existe uma única assinatura σ de R tal que $P = P_\sigma$.

Para analisarmos os ideais primos de W(R) que contém $p[\langle 1\rangle]$, para algum primo impar p, necessitamos mais informações sobre o ideal K que veremos a seguir.

(1.9) Lema - Para cada caracter χ de G, temos $\varphi_\chi(K) = 0$ ou

$\varphi_{\mathcal{H}}(K) = 2^n\mathbb{Z}$, para algum $n \geq 1$.

Dem.: Para cada caracter χ de G, temos $\varphi((1) + (-1)) = 0$ ou 2, pois $\varphi_{\mathcal{H}}((1)) = 1$. Seja $z = \sum_{i=1}^{n} \langle \alpha_i \rangle - \sum_{i=1}^{n} \langle \beta_i \rangle \in \mathbb{Z}[G]$, tal que $\langle \alpha_1, \ldots, \alpha_n \rangle \simeq \langle \beta_1, \ldots, \beta_n \rangle$. Dado um caracter χ de G qualquer, sejam s o número de elementos $\langle \alpha_i \rangle$, $1 \leq i \leq n$, com $\varphi_{\mathcal{H}}(\langle \alpha_i \rangle) = -1$ e r o número dos $\langle \beta_i \rangle$, $1 \leq i \leq n$, tais que $\varphi_{\mathcal{H}}(\langle \beta_i \rangle) = -1$. Temos então $\varphi_{\mathcal{H}}(z) = 2(r-s)$. Mas $\langle \alpha_1, \ldots, \alpha_n \rangle \simeq \langle \beta_1, \ldots, \beta_n \rangle$ o que implica que $\prod_{i=1}^{n} \langle \alpha_i \rangle = \prod_{i=1}^{n} \langle \beta_i \rangle$ e, assim $(-1)^s = \varphi_{\mathcal{H}}(\prod_{i=1}^{n} \langle \alpha_i \rangle) = \varphi_{\mathcal{H}}(\prod_{i=1}^{n} \langle \beta_i \rangle) = (-1)^r$, isto é, $r - s$ é um número par, consequentemente $\varphi_{\mathcal{H}}(z) \equiv 0 \bmod 4$. Agora a demonstração segue-se de (1.2) ■

Deste lema segue-se facilmente que, se $\varphi_{\mathcal{H}}(K) \subseteq p\mathbb{Z}$ para algum número primo ímpar p, então $\varphi_{\mathcal{H}}(K) = 0$. Obtemos agora da proposição (1.6),(ii) o seguinte:

(1.10) Proposição - Seja p um número primo ímpar. Para cada ideal primo P de W(R) com $p[(1)] \in P$, existe uma única assinatura σ de R, tal que $P = P_{\sigma,p} = p\mathbb{Z} + P_{\sigma}$, que é o conjunto de todos os elementos $z \in W(R)$, tais que $\sigma(z) \equiv 0 \bmod p$.

Concluímos então que os P_{σ}, os $P_{\sigma,p}$ e I(R) são todos os ideais primos de W(R).

Dizemos que o anel R é *real* (ou *formalmente real*), se R tem pelo menos uma assinatura, ou seja, o conjunto das assinaturas de R, Ass(R), é não vazio. Caso contrário dizemos que

R é *não real*. Pela nossa descrição dos ideais primos de W(R), temos:

(1.11) Corolário - Se Ass(R) ≠ ∅, então:

(i) os P_σ, com $\sigma \in Ass(R)$, são os ideais primos minimais de W(R);

(ii) os $P_{\sigma,p}$, com $\sigma \in Ass(R)$ e p um primo ímpar e I(R) são todos os ideais primos máximais de W(R);

(iii) cada $P_{\sigma,p}$,,contém um único ideal primo minimal, a saber P_σ;

(iv) o ideal I(R) contém todos os ideais primos minimais.

No caso em que Ass(R) = ∅ temos:

(1.12) Proposição - São equivalentes:

(i) Ass(R) = ∅

(ii) I(R) é o único ideal primo de W(R)

(iii) $2^n W(R) = 0$, para algum número natural n.

Dem: (i) ↔ (ii). É imediato pela descrição dos ideais primos de W(R).

(ii) → (iii). Desde que I(R) é o único ideal primo de W(R), temos que I(R) é o nilradical de W(R). Em particular, 2[⟨1⟩] é nilpotente, assim existe n ≥ 1, tal que $2^n[\langle 1\rangle] = (2[\langle 1\rangle])^n = 0$ e, consequentemente $2^n W(R) = 0$.

(iii) → (i). Se Ass(R) ≠ ∅, então existe um ideal primo P de

W(R), tal que $P \cap \mathbb{Z} = \langle 0 \rangle$, o que implica que $W(R)/P \cong \mathbb{Z}$ que é livre de torção. Isto é uma contradição pois $2^n W(R) = 0$. Portanto $Ass(R) = \emptyset$ ■

§ 2 - $W(R)_t$ e Nil(W(R))

Neste parágrafo analisaremos os elementos nilpotentes e de torção de W(R). Denotamos o subgrupo dos elementos de torção de W(R) por $W(R)_t$, e o dos nilpotentes por Nil(W(R)).

Se Ass(R) =∅, decorre de (1.12) que Nil(W(R)) = = I(R), $W(R)_t$ = W(R) e, todo elemento de W(R) é anulado por uma potência de 2, isto é W(R) tem sómente 2-torção.

Vamos assumir que $Ass(R) \neq \emptyset$. Desde que os P_σ; $\sigma \in$ $\in Ass(R)$, são todos os ideais primos minimais de W(R), temos:

(2.1) Proposição - Um elemento $z \in W(R)$ é nilpotente se, e somente se, $\sigma(z) = 0$ para toda $\sigma \in Ass(R)$, isto é, $Nil(W(R)) = \bigcap_{\sigma \in Ass(R)} Ker\sigma$.

Os elementos de torção de W(R) são analizados na próxima proposição.

(2.2) Proposição - $W(R)_t = Nil(W(R))$

Dem.: Seja $z \in W(R)_t$. Existe $n \in \mathbb{N}$, $n \geq 1$, tal que $nz = 0$. Então

$\sigma(nz) = n\sigma(z) = 0$, o que implica que $\sigma(z) = 0$, para toda $\sigma \in$ Ass(R), ou seja $z \in Nil(W(R))$, o que mostra que $W(R)_t \subseteq$ $\subseteq Nil(W(R))$.

Reciprocamente, se $z \in Nil(W(R))$, então existe um subgrupo finito $H \subseteq G = R^*/(R^*)^2$, tal que z está no subanel $A = \mathbb{Z}[H]/(K \cap \mathbb{Z}[H])$, de W(R) gerado por H. Desde que H é finito e a característica, car($\mathbb{Q}$), do corpo dos números racionais $\mathbb{Q}$, é zero, temos que car($\mathbb{Q}$) não divide a ordem de nenhum elemento de H e, então, pelo teorema de Maschke (cf. [P]Th.3.6), o anel de grupo $\mathbb{Q}[H]$ é semi-simples (artiniano com nilradical zero).

O produto tensorial $\mathbb{Q} \otimes_{\mathbb{Z}} A$ é uma imagem homomórfica de $\mathbb{Q}[H]$ ($\cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[H]$), logo também é semi-simples (cf. [P] Corolário da Prop.3.1, b). Temos então $Nil(\mathbb{Q} \otimes_{\mathbb{Z}} A) = 0$. Mas $1 \otimes z \in \mathbb{Q} \otimes_{\mathbb{Z}} Nil(A) \cong Nil(\mathbb{Q} \otimes_{\mathbb{Z}} A) = 0$, $\mathbb{Q} \otimes_{\mathbb{Z}} A$ pode ser identificado com o anel de frações $T^{-1}(A)$, onde $T = \mathbb{Z} - (0)$ e $0 = 1 \otimes z = \frac{z}{1} \in T^{-1}(A)$, o que é equivalente a existir $n \in T$, $n \geq 1$, tal que $nz = 0$. Então $z \in A_t \subseteq W(R)_t$, o que mostra que $Nil(W(R)) \subseteq$ $\subseteq W(R)_t$, como queríamos ■

(2.3) Observação - (i) Se $Ass(R) \neq \emptyset$, de (2.1) e (2.2) temos $NIL(W(R)) = W(R)_t \cap I(R)$. Se $Ass(R) = \emptyset$, então $W(R)_t = W(R)$, $Nil(W(R)) = I(R)$ e, consequentemente, $Nil(W(R)) = W(R)_t \cap I(R)$. Assim, podemos concluir que $Nil(W(R)) = W(R)_t \cap I(R)$.

(ii) Se $Ass(R) = \emptyset$, então $W(R)_t = W(R) = \bigcap_{\sigma \in Ass(R)} Ker\sigma$. Se $Ass(R) \neq \emptyset$, então $W(R)_t = Nil(W(R)) = \bigcap_{\sigma \in Ass(R)} Ker\sigma$. Portanto podemos também concluir que $W(R)_t = \bigcap_{\sigma \in Ass(R)} Ker\sigma$, isto é, que

vale o Princípio Local - Global de Pfister para espaços bilineares.

(2.4) Teorema - $W(R)$ tem sómente 2-torção.

Dem.: Se $Ass(R) = \emptyset$, então o teorema segue de (1.12). Assumiremos então que $Ass(R) \neq \emptyset$.

Seja $z \in W(R)_t$. De (2.2) temos que $z \in Nil(W(R))$ e então existe um subgrupo finito $H \leq G = R^*/(R^*)^2$, tal que z está no subanel A de $W(R)$, gerado por H.

Seja p um número primo impar qualquer. O anel A/pA é uma imagem homomórfica do anel de grupos $\mathbb{F}_p[H]$ e, desde que $H \leq G$ os elementos de H tem ordem 2. Como $car(\mathbb{F}_p) = p$ temos pelo teorema de Maschke que A/pA é semi-simples.

O elemento z é nilpotente, então $\bar{z} = z + pA$ é zero em A/pA, o que implica que existe $y \in A$, tal que $z = py$. Desta forma mostramos também que A_t é divisível por cada número primo impar p, isto é, $pA_t = A_t$, para cada número primo impar p. Assim os elementos de A_t tem ordem potência de 2 ou ∞. Mas, A é um $\mathbb{Z}$-módulo finitamente gerado e $\mathbb{Z}$ é noetheriano, então A_t é um $\mathbb{Z}$-módulo finitamente gerado.

Sejam $x_1, \ldots, x_k$ os geradores de A_t. Então os x_i, $1 \leq i \leq k$, são de torção e todo $z' \in A_t$ é da forma $z' = \sum_{i=1}^{k} n_i x_i$, onde cada n_i é menor do que a ordem de x_i, o que mostra que A_t é finito e consequentemente todo elemento de A_t tem ordem potência de 2. Em particular $z \in A_t$ e, portanto z possue 2-torção, como

queríamos■

Como consequência deste teorema temos:

(2.5) Corolário - Os divisores de zero de W(R) tem dimensão par.

Dem.: O conjunto dos divisores de zero de W(R) é uma união de ideais primos. De (2.4) temos que p[<1>] não é um divisor de zero, para todo número primo impar p. De (1.11) segue que cada ideal primo que aparece na união é minimal ou I(R) e, desde que $P_\sigma \subseteq I(R)$, para todo $\sigma \in Ass(R)$, temos o corolário■

§ 3 - $W_q(R)_t$ e Nil($W_q(R)$)

Consideramos agora o anel, $W_q(R)$, dos espaços quadráticos sobre R.

Para estudarmos os elementos de torção e os elementos nilpotentes de $W_q(R)$, usaremos o módulo quadrático E_8, cuja matriz da forma bilinear associada é:

$$E_8 = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

O módulo quadrático E_8 é um espaço quadrático e $b_{E_8} \simeq 8\langle 1\rangle$ (cf. [S] pag. 89).

(3.1) Proposição - São equivalentes:

(i) $W(R)$ tem somente 2-torção.

(ii) $W_q(R)$ tem somente 2-torção.

Dem.: (i) $\Rightarrow$ (ii). Seja $[q] \in W_q(R)_t$. Consideremos o homomorfismo de anéis, $\beta: W_q(R) \to W(R)$, dado por $\beta([q]) = [b_q]$.

Desde que $[q] \in W_q(R)_t$, temos que $[b_q] \in W(R)_t$ e, consequentemente, existe um número inteiro $r>0$ tal que $2^r[b_q] = 0$, ou seja, $2^r[q] \in Ker\beta$.

Mas, $8Ker\beta = 0$. De fato, desde que $[b_{E_8}] = 8[\langle 1\rangle]$ e $b_q \otimes E_8 \simeq b_{E_8} \otimes q$ (cf. (II, 2.3)), temos $[b_{E_8} \otimes q] = 8[q]$, para todo $[q] \in W_q(R)$. Agora, se $[q] \in Ker\beta$, então $8[q] = [b_q \otimes E_8] = \beta([q])[E_8] = 0$. Assim, se $[q] \in W_q(R)_t$, então existe um número inteiro $r > 0$, tal que $2^{r+3}[q] = 0$, ou seja, $[q]$ tem ordem potência de 2.

(ii) $\Rightarrow$ (i). Se $[b] \in W(R)_t$, então $[b \otimes E_8] \in W_q(R)_t$ e, de (ii), existe $r > 0$ tal que $2^r[b \otimes E_8] = 0$, o que implica que $0 = \beta(2^r[b \otimes E_8]) = 2^r 8[b] = 2^{r+3}[b]$, o que mostra (i) ■

De (2.4) e (3.1) temos:

(3.2) Teorema - $W_q(R)$ tem somente 2-torção.

Usando o homomorfismo $\beta: W_q(R) \to W(R)$, associamos a cada $\sigma \in Ass(R)$ um homomorfismo de anéis, não nulo, $\bar{\sigma} = \beta: W_q(R) \to \mathbb{Z}$. Observemos que, para todo $[b] \in W(R)$ e $[q] \in W_q(R)$, vale $\bar{\sigma}([b][q]) = \bar{\sigma}([b \otimes q]) = \sigma([b \otimes b_q]) = \sigma([b])\bar{\sigma}([q])$, logo $Ker\bar{\sigma}$ é um $W(R)$-submódulo de $W_q(R)$.

Reciprocamente, mostremos que, para todo homomorfismo não nulo de anéis, $\bar{\sigma}: W_q(R) \to \mathbb{Z}$, tal que $Ker\bar{\sigma}$ é um $W(R)$-submódulo de $W_q(R)$, temos $\bar{\sigma} = \sigma\beta$, para algum $\sigma \in Ass(R)$ e, mais ainda que a correspondência, $\sigma \longleftrightarrow \bar{\sigma}$, é 1-1.

Seja então $\bar{\sigma}: W_q(R) \to \mathbb{Z}$, um homomorfismo não nulo de anéis tal que $Ker\bar{\sigma}$ é um $W(R)$-submódulo de $W_q(R)$. Desde que $\bar{\sigma}$ é não nulo, $\bar{\sigma}(W_q(R)) = n\mathbb{Z}$, para algum número inteiro $n \geq 1$. Seja $[q_o] \in W_q(R)$. tal que $\bar{\sigma}([q_o]) = n$. Então, para todo $[b] \in W(R)$, definimos: $\sigma([b]) = (1/n)\bar{\sigma}([b \otimes q_o]) \in \mathbb{Z}$. Mostremos que $\sigma: W(R) \to \mathbb{Z}$, definimos dessa forma é um homomorfismo de anéis tal que $\bar{\sigma} = \sigma\beta$.

Claramente σ está bem definido. Além disso, σ não depende da escolha de $[q_o]$. De fato, considerando que $\bar{\sigma}$ é um homomorfismo de anéis e $(b \otimes q) \circ q_o \simeq q \circ (b \otimes q_o)$ (cf. (II, 2.3)), temos que, para todo $[q] \in W_q(R)$, com $\bar{\sigma}([q]) \neq 0$, e para todo $[b] \in W(R)$, $\bar{\sigma}([b \otimes q])/\bar{\sigma}([q]) = \bar{\sigma}([b \otimes q_o])/\bar{\sigma}([q_o])$.

Sejam $[b_1]$ e $[b_2] \in W(R)$. Se $\sigma([b_1])\sigma([b_2]) \neq 0$, então $\sigma([b_1][b_2]) = \sigma([b_1 \otimes b_2]) = (1/n)\bar{\sigma}([b_1 \otimes b_2 \otimes q_o]) =$
$= \left(\bar{\sigma}([b_1 \otimes (b_2 \otimes q_o)])/\bar{\sigma}([b_2 \otimes q_o])\right)\left(\bar{\sigma}([b_2 \otimes q])/n\right) = \sigma([b_1])\sigma([b_2])$.

Agora. se $\sigma([b_2]) = 0$, isto é $\bar{\sigma}([b_2 \otimes q_o]) = 0$, temos $[b_2 \otimes q_o] \in Ker\bar{\sigma}$, o que implica que $[b_1][b_2 \otimes q_o] \in Ker\bar{\sigma}$, pois $Ker\bar{\sigma}$ é um $W(R)$-módulo. De maneira análoga, se $\sigma([b_1]) = 0$,

então $[b_1 \otimes b_2 \otimes q_o] \in \mathrm{Ker}\bar{\sigma}$. Isto mostra que $\sigma([b_1][b_2]) = \sigma([b_1])\sigma([b_2])$, quando $\sigma([b_1])\sigma([b_2]) = 0$. Ou seja, σ é um homomorfismo de anéis.

Finalmente, $\bar{\sigma} = \sigma\beta$, pois para todo $[q] \in W_q(R)$, $\sigma\beta([q]) = \sigma([b_q]) = \bar{\sigma}([b_q \otimes q_o])/\bar{\sigma}([q_o]) = \bar{\sigma}([qoq_o])/\bar{\sigma}([q_o]) = \bar{\sigma}([q])\bar{\sigma}([q_o])/\bar{\sigma}([q_o]) = \bar{\sigma}([q])$.

Seja $\overline{\mathrm{Ass}(R)}$ o conjunto dos homomorfismos não nulos, de anéis, $\bar{\sigma}: W_q(R) \to \mathbb{Z}$, cujo núcleo é um $W(R)$-submódulo de $W_q(R)$. Definimos uma função de $\overline{\mathrm{Ass}(R)}$ em $\mathrm{Ass}(R)$, $\bar{\sigma} \longmapsto \sigma$ que é, obviamente, a inversa da função, $\sigma \longmapsto \sigma\beta$. Logo temos uma correspondência 1-1 entre os elementos de $\overline{\mathrm{Ass}(R)}$ e as assinaturas de R.

(3.3) Proposição - São equivalentes:

(i) $W(R)_t = \bigcap_{\sigma \in \mathrm{Ass}(R)} \mathrm{Ker}\sigma$.

(ii) $W_q(R)_t = \bigcap_{\bar{\sigma} \in \overline{\mathrm{Ass}(R)}} \mathrm{Ker}\bar{\sigma}$.

Dem.: (i) → (ii). Claramente $W_q(R)_t \subseteq \bigcap_{\bar{\sigma} \in \overline{\mathrm{Ass}(R)}} \mathrm{Ker}\bar{\sigma}$. Reciprocamente, se $[q] \in \bigcap_{\bar{\sigma} \in \overline{\mathrm{Ass}(R)}} \mathrm{Ker}\bar{\sigma}$, então $[b_q] \in \bigcap_{\sigma \in \mathrm{Ass}(R)} \mathrm{Ker}\sigma = W(R)_t$, o que implica que $[q] \in W_q(R)_t$, pois, da demostração de (3.1), $8\mathrm{Ker}\beta = 0$.

(ii) → (i). É imediato que $W(R)_t \subseteq \bigcap_{\sigma \in \mathrm{Ass}(R)} \mathrm{Ker}\sigma$. Seja $[b] \in \bigcap_{\sigma \in \mathrm{Ass}(R)} \mathrm{Ker}\sigma$. Então $[b \otimes E_8] \in \bigcap_{\bar{\sigma} \in \overline{\mathrm{Ass}(R)}} \mathrm{Ker}\bar{\sigma} = W_q(R)_t$, pois $\bar{\sigma}([b \otimes E_8]) = \sigma([b])\bar{\sigma}([E_8]) = 0$, para todo $\bar{\sigma} \in \overline{\mathrm{Ass}(R)}$. Logo

$\beta([b \otimes E_\beta] = \delta[b] \in W(R)_t$, ou seja, $[b] \in W(R)_t$, como queríamos.■

Da proposição acima e de (2.3),(ii), temos o seguinte teorema:

(3.4) Teorema (Análogo Quadrático do Princípio Local-Global de Pfister) - $W_q(R)_t = \bigcap_{\sigma \in Ass(R)} Ker\bar{\sigma}$.

Um resultado análogo a (2.2) ou, mais precisamente à (2.3) (i), pode ser provado no caso quadrático. Para prová-lo, necessitamos do seguinte resultado auxiliar.

(3.5) Lema - Para qualquer espaço quadrático $[1,\alpha]$ sobre R, temos $[1,\alpha] \perp [1,\alpha] \simeq 2[1,\alpha]$.

Dem.: Suponhamos, inicialmente que $|R/\wp| \geq 4$, para todo $\wp \in Spm(R)$. Neste caso, existe $\beta \in R$, tal que $(1 - 2\beta)(1 - 4\beta) \in R^*$ e $[1,\alpha] \simeq [1,\beta]$. De fato, basta observarmos que R é um LG-anel, e que o polinômio $f(X) = (1 - 2(X^2 + X + \alpha))(1 - 4(X^2 + X + \alpha))$ representa uma unidade localmente. Consequentemente existe $\lambda \in R$ talque $f(\lambda) \in R^*$, tomamos então $\beta = \lambda^2 + \lambda + \alpha$.

Observamos também que:

$\begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \perp \langle -1 \rangle \simeq \langle 1, 2\beta - 1, \gamma \rangle$, para algum $\gamma \in R^*$, pois se (x_1, x_2, x_3) é uma base canônica para o espaço $\begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \perp \langle -1 \rangle$, então $(x_1 + x_3, x_2 + x_3)$ é uma base para o subespaço não singular $\langle 1, 2\beta - 1 \rangle$.

Agora, comparando os determinantes em $\begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \perp \langle -1 \rangle \simeq \langle 1, 2\beta - 1, \gamma \rangle$, temos $\gamma \equiv (1 - 4\beta)(2\beta - 1) \bmod (R^*)^2$.

Portanto obtemos:

$$\begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \perp \langle 1, -1 \rangle \simeq \langle 1, 1, 2\beta - 1, (1 - 4\beta)(2\beta - 1) \rangle$$

Para $q = [1, \beta]$, temos:

$(qoq) \perp 2\mathbb{H} \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \otimes q \perp 2\mathbb{H} \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \otimes q \perp \langle 1, -1 \rangle \otimes q \simeq$
$\simeq \left[\begin{pmatrix} 2 & 1 \\ 1 & 2\beta \end{pmatrix} \perp \langle 1, -1 \rangle \right] \otimes q \simeq \langle 1, 1, 2\beta - 1, (2\beta - 1)(1 - 4\beta) \rangle \otimes q \simeq$
$\simeq \langle 1, 1, 2\beta - 1, -(2\beta - 1) \rangle \otimes q$, pois $4\beta - 1$ é representado por q, e q é um espaço quadrático redondo (cf. [B] Ex.(1.2),Chap IV). Cancelando $2\mathbb{H}$, obtemos $qoq \simeq 2q$ (cf.(II,6.4)).

Agora suponhamos que R é um LG-anel qualquer e consideremos a extensão cúbica de Frobenius $S = R[X]/(X^3 + 6X^2 - X + 1)$, com a função traço s definida por $s(1) = 1$ e $s(X) = s(X^2) = 0$.

Então sobre S temos que $qoq \simeq 2q$, pois $|S/\mathfrak{p}| \geq 7$, para todo $\mathfrak{p} \in \mathrm{Spm}(S)$ (cf. [B] Rem.(2.3), Chap.IV). Mas $qoq \simeq 2q$, implica que $s_*(qoq) \simeq 2s_*(q)$, ou seja, $qoq \perp 4\mathbb{H} \simeq 2q \perp 4\mathbb{H}$, pois $s_*(q \otimes S) = s_*(i^*(q) \otimes \langle 1 \rangle) = s_*(\langle 1 \rangle) \otimes q$ (cf. [B] Prop.(2.12), Chap. I) e $s_*(\langle 1 \rangle) \simeq \langle 1 \rangle \perp \begin{pmatrix} 0 & 1 \\ 1 & 6 \end{pmatrix} \simeq \langle 1 \rangle \perp \mathbb{H}$. Assim, $qoq \simeq 2q$ (cf.(II,6.4)), como queríamos■

(3.6) Corolário - Seja $q = \langle\langle \alpha_1, \ldots, \alpha_n, \beta]]$, um espaço de Pfister sobre R, isto é, $q = \langle\langle \alpha_1, \ldots, \alpha_n \rangle\rangle \otimes [1, \beta]$, onde $\langle\langle \alpha_1, \ldots, \alpha_n \rangle\rangle = \bigotimes_{i=1}^{n} \langle 1, \alpha_i \rangle$. Então para todo número inteiro $m \geq 1$, temos $q^m \simeq 2^{(n+1)(m-1)} q$.

Dem.: Sejam $b = \langle\langle \alpha_1, \ldots, \alpha_n \rangle\rangle$ e $q_o = [1, \beta]$, ou seja, $q = b \otimes q_o$.

Então $b_q \simeq b \otimes b_{q_o}$ e, consequentemente $qoq \simeq b \otimes b \otimes (q_o o q_o)$. Desde que $\langle 1, \alpha\rangle \otimes \langle 1, \alpha\rangle \simeq 2\langle 1, \alpha\rangle$, para todo $\alpha \in R^*$ e $q_o o q_o \simeq 2q_o$ temos por indução sobre n que $q o q \simeq 2^{n+1}q$. Agora, por indução sobre m, obtemos $q^m \simeq qoq^{m-1} \simeq qo(2^{(n+1)(m-2)}q) \simeq 2^{(n+1)(m-1)}q$, como queríamos■

(3.7) **Teorema** - $Nil(W_q(R)) = W_q(R)_o \cap W_q(R)_t$, onde $W_q(R)_o = \{[q] \in W_q(R);\ \dim_R q$ é par$\}$.

Dem.: Se $[q] \in W_q(R)_o \cap W_q(R)_t$, então podemos escrever $q = \langle a_1\rangle \otimes [1, \lambda_1] \perp \ldots \perp \langle a_n\rangle \otimes [1, \lambda_n]$, onde $a_i \in R^*$, $\lambda_i \in R$ e $1 - 4\lambda_i \in R^*$, $1 \le i \le n$, (cf. Chap. II, § 4) e, $[q]$ é de torção.

Considerando $q_i = \langle a_i\rangle \otimes [1, \lambda_i]$, $1 \le i \le n$, temos $q = q_1 \perp \ldots \perp q_n$. Para $N > n$, obtemos $q^N = (q_1 \perp \ldots \perp q_n)^N = \perp_{i_1+\ldots+i_n=N} \lambda_{i_1\ldots i_n} q_1^{i_1} o \ldots o q_n^{i_n}$, onde $\lambda_{i_1\ldots i_n} \in \mathbb{N}$. Generalizando o lema (3.5) segue-se que para $1 \le k \le n$, $q_k^{i_k} \simeq 2^{i_k - 1}\langle \gamma_k\rangle \otimes q_k$, onde $\gamma_k = a_k$ ou 1. Logo $q_1^{i_1} o \ldots o q_n^{i_n}$ é um múltiplo de $2^{\sum i_k - n} = 2^{N-n}$, ou seja $q^N \simeq 2^{N-n}q'$, para algum espaço quadrático q', o que implica que $q^{N+1} \simeq q' o (2^{N-n}q)$ e desde que $[q]$ é de torção, de (3.2) obtemos que $[q]^{N+1} = 0$ em $W_q(R)$, para algum $N > n$, o que mostra que $W_q(R)_o \cap W_q(R)_t \le Nil(W_q(R))$.

Reciprocamente, se $[q] \in Nil(W_q(R))$, então existe um número inteiro $m \ge 1$, tal que $[q]^m = [q^m] = 0$. Logo $0 = \beta([q]^m) = [b_q^m] = [b_q]^m$, ou seja $[b_q] \in Nil(W(R)) = I(R) \cap W(R)_t$ (cf. (2.3)(ii)). De (2.4) segue-se que existe um número inteiro $r > 0$, tal que $[2^r b_q] = 0$ e, como $[b_q] \in I(R)$

segue-se também que $[q] \in W_q(R)_o$. Assim $[q] \in W_q(R)_o$ e $[2^r q] \in$ $\in Ker\beta$. Mas $8Ker\beta = 0$, consequentemente $[q] \in W_q(R)_1$ o que mostra que $Nil(W_q(R)) \subseteq W_q(R)_o \cap W_q(R)_1$, como queríamos■

Veremos agora, alguns resultados que relacionam assinaturas e unidades de um LG-anel R.

Cada assinatura σ de R induz um homomorfismo de grupos $R^* \xrightarrow{\pi} G = R^*/(R^*)^2 \xrightarrow{\sigma|} \{\pm 1\}$, onde π é a projeção canônica. De (1.1), segue-se que σ é completamente determinada por este homomorfismo. Identificamos então σ com o homomorfismo $\sigma\pi: R^* \to \mathbb{Z}$ e, escrevemos $\sigma(a)$ no lugar de $\sigma(\langle a \rangle)$.

(3.8) Proposição - Se $\sigma: R^* \to \mathbb{Z}$ é uma assinatura, então valem as seguintes propriedades:

(i) $\sigma(a\lambda) = \sigma(a)\sigma(\lambda)$, para todo $a, \lambda \in R^*$.

(ii) $\sigma(-1) = -1$

(iii) Se $a_1, \ldots, a_r \in R^*$ e $\sigma(a_i) = 1$, $1 \leq i \leq r$, então para cada $a \in R^*$, da forma $a = \lambda_1^2 a_1 + \ldots + \lambda_r^2 a_r$ com $\lambda_i \in R$, $1 \leq i \leq r$, temos $\sigma(a) = 1$.

Dem.: (i) e (ii) seguem imediatamente do fato de σ ser um homomorfismo de grupos multiplicativos.

Para provarmos (iii), consideremos o espaço bilinear $b = \langle a_1, \ldots, a_r \rangle$. Desde que $a \in R^*$ e $a = \lambda_1^2 a_1 + \ldots + \lambda_r^2 a_r$, $\lambda_i \in R$, $1 \leq i \leq r$, temos que $\langle a \rangle$ é um subespaço não singular de b e, consequentemente $b \simeq \langle a \rangle \perp \langle a \rangle^\perp$ (cf. (II,(4.2)). Desde que o

espaço $\langle 1\rangle \perp \langle\alpha\rangle^{\perp}$ é próprio, temos que existem $\gamma_1,\ldots,\gamma_r \in R^*$, tais que $\langle 1\rangle \perp \langle\alpha\rangle^{\perp} \simeq \langle\gamma_1,\ldots,\gamma_r\rangle$ (cf.(II,(4.3)) e, por conseguinte, $\langle 1, \alpha_1,\ldots,\alpha_r\rangle \simeq \langle\alpha, \gamma_1,\ldots,\gamma_r\rangle$. Aplicando σ nas classes desses espaços obtemos $r + 1 = \sigma(\alpha) + \sigma(\gamma_1) +\ldots+ \sigma(\gamma_r)$ que, juntamente com o fato que $\gamma_i \in R^*$, $1 \leq i \leq r$, implica que $\sigma(\gamma_i) = 1$ e, em particular $\sigma(\alpha) = 1$, como queríamos■

(3.9) **Teorema** - Sejam $\alpha_1,\ldots\alpha_r \in R^*$ e, suponhamos que $2 \in R^*$. Então para cada unidade α de R são equivalentes:

(i) Para cada $\sigma \in Ass(R)$, com $\sigma(\alpha_i) = 1$, $1 \leq i \leq r$, também $\sigma(\alpha) = 1$.

(ii) A unidade α é expressa na forma $\alpha = \sum_{i_k=0 \text{ou} 1} \gamma_{i_1\ldots i_r}\alpha_1^{i_1}\ldots\alpha_r^{i_r}$, onde os coeficientes $\gamma_{i_1\ldots i_r}$ são somas de quadrados de elementos de R.

Dem.: (ii) → (i) segue-se imediatamente de (3.8).

Para provarmos (i) → (ii), consideremos o espaço bilinear de Pfister $b = \langle\langle\alpha_1,\ldots,\alpha_r\rangle\rangle = \bigotimes_{i=1}^{r}\langle 1, \alpha_i\rangle$ e $b' = \langle 1, -\alpha\rangle \otimes b$. De (i) segue-se que $\sigma(b') = 0$ para todo $\sigma \in Ass(R)$, ou seja $[b'] \in Nil(W(R))$ e, portanto $[b'] \in W(R)_t$ (cf. (2.1) e (2.2)).

Assim, existe $m \in \mathbb{N}$, $m \geq 1$, tal que $m[b'] = 0$, isto é, $m[b \perp \langle -\alpha\rangle \otimes b] = m[b] - m[\langle\alpha\rangle \otimes b] = 0$ em $W(R)$, o que implica que $m[b] = m[\langle\alpha\rangle \otimes b]$ em $W(R)$ e, como $\dim_R b = \dim_R \langle\alpha\rangle\otimes b$, temos que $m[b] = m[\langle\alpha\rangle \otimes b]$ em $\hat{W}(R)$ (cf.(1.4)). Consequentemente, existe $b_1 \in Bil(R)$ tal que $mb \perp b_1 \simeq m\langle\alpha\rangle \otimes b \perp b_1$ e, desde que

$2 \in \dot{R}^*$ temos $mb \simeq m\langle\alpha\rangle \otimes b$ (cf.(II,6.5)). Agora b representa 1, então $\langle\alpha\rangle \otimes b$ representa α, o que mostra (ii)■

(3.10) Corolário - Se $2 \in \dot{R}^*$ então as unidades de R que tem valor 1, para toda assinatura de R, são precisamente as unidades que são somas de quadrados.

Dem.: Basta tomarmos $r = 1$ e $\alpha_1 = 1$ em (3.9)■

(3.11) Corolário - Se $2 \in \dot{R}^*$ então são equivalentes:

(i) $Ass(R) = \emptyset$.

(ii) -1 é uma soma de quadrados.

Dem.: Se $-1 = \sum_{i=1}^{n} \lambda_i^2$; $\lambda_i \in R$, $1 \leq i \leq n$ e $Ass(R) \neq \emptyset$, então de (3.8) temos uma contradição, pois $\sigma(-1) = -1$ ((3.8)(ii)) e $\sigma(-1) = 1$ ((3.8)(iii)). Para a recíproca, basta tomarmos $r = 1$, $\alpha_1 = 1$ e $\alpha = -1$ em (3.9)■

CAPITULO IV

O GRUPO ORTOGONAL

Em todo este capítulo R denotará sempre um LG-anel. Seja (V,q) ∈ Quad(R). O conjunto O(V) das isometrias de (V,q) munido da operação composição tem uma estrutura de grupo, o qual é chamado o *grupo ortogonal* de V. O nosso objetivo, neste capítulo, é o estudo da estrutura de O(V) no caso em que (V,q) é um espaço quadrático de dimensão ≥ 3 e dimensão hiperbólica ≥ 1; isto é, (V,q) admite uma decomposição da forma $V \simeq (Ru \oplus Rv) \perp V_o$ onde Ru ⊕ Rv é um plano hiperbólico e $V_o = (Ru \oplus Rv)^{\perp}$ é um subespaço não nulo. No que se seguirá assumiremos sempre (V,q) com a decomposição acima descrita.

§ 1 - Definições e Notações

Iniciaremos este parágrafo recordando que toda transvecção de Siegel (já visto no cap. II, § 6) é um elemento de O(V). Em particular, as transvecções de Siegel com as quais trataremos neste e nos demais parágrafos, são do tipo E(u,x) e E(v,x), com $x \in V_o$; indicamos por E(V) o subgrupo de O(V) gerado por essas particulares transvecções.

Para cada $\lambda \in R^*$ denotamos por $\phi(\lambda)(u) = \lambda u$, $\phi(\lambda)(v) = \lambda v$ e $\phi(\lambda)(x) = x$, para todo $x \in V_o$. É imediato ver que $\phi(\lambda_1)\phi(\lambda_2) = \phi(\lambda_1\lambda_2)$, $\lambda_1, \lambda_2 \in R^*$; isto é; $\phi(V) = (\phi(\lambda) / \lambda \in R^*)$ é

um subgrupo de $O(V)$. Claramente $\phi(V) \cong R^*$.

Denotamos por Δ o elemento de $O(V)$ dado por $\Delta(u) = v$, $\Delta(v) = u$ e $\Delta(x) = x$, para todo $x \in V_o$.

(1.1) Observação - Estas isometrias, acima mencionadas, satisfazem as seguintes propriedades, as quais podem ser facilmente verificadas:

(1) $\Delta\phi(\lambda)\Delta^{-1} = \phi(\lambda^{-1})$, $\phi(\lambda^{-1}) = \phi(\lambda)^{-1}$

(2) $\Delta E(u,x)\Delta^{-1} = E(v,x)$

(3) $\phi(\lambda)E(u,x)\phi(\lambda^{-1}) = E(u,\lambda x)$

(4) $\phi(\lambda)E(v,x)\phi(\lambda^{-1}) = E(v,\lambda^{-1}x)$

(5) $E(u,x_1)E(u,x_2) = E(u,x_1+x_2)$, $E(u,x)^{-1} = E(u,-x)$

(6) $\theta E(u,x)\theta^{-1} = E(u,\theta(x))$, para todo $\theta \in O(V)$, tal que $\theta(u) = u$ e $\theta(v) = v$.

Seja $x \in V$ tal que $q(x) \in R^*$. Pode ser visto facilmente que a aplicação $\tau_x : V \to V$ definida por $\tau_x(y) = y - q(x)^{-1}b_q(x,y)x$, para todo $y \in V$ é um elemento de $O(V)$. Além disso $\tau_x^2 = id_V$, $\tau_x(x) = -x$ e τ_x deixa fixo todo elemento de $(Rx)^{\perp}$. Tal aplicação é chamada uma *simetria* de V. Indicamos por $S(V)$ o subgrupo de $O(V)$ gerado pelas simetrias de V.

Observemos que se $x \in V$ é um elemento tal que $q(x) \in R^*$ não necessariamente V admite uma decomposição do tipo $V = (Rx) \perp V_1$; isto só ocorre quando $2q(x) = b_q(x,x) \in R^*$. Contudo, no caso específico em que V é da forma $V = (Rx) \perp V_1$, para algum $x \in V$ (ou seja, $2q(x) \in R^*$), existe uma noção mais geral de simetria para V, a saber: a aplicação $\tau_x^a : V \to V$ dada por

$\tau_x^a(x) = ax$ e $\tau_x^a(y) = y$, $y \in V_1$, onde $a \in R$ é tal que $a^2=1$. Claramente, $\tau_x^a \in O(V)$ e se $a = -1$, $\tau_x^a = \tau_x$. Além disso, para todo $a, b \in \mu_2(R) = \{a \in R / a^2 = 1\}$ temos $\tau_x^a\tau_x^b = \tau_x^{ab}$, com $(ab)^2 = 1$, ou seja, $\mu_2(V) = \{\tau_x^a / a \in \mu_2(R)\}$ é um subgrupo de $O(V)$ naturamente isomorfo à $\mu_2(R)$.

Suponhamos agora que V admite uma decomposição do tipo $V=(Rx_1 \oplus Rx_2) \perp V'$, com $x_1, x_2 \in V$ tais $q(x_2)(1-4q(x_1)q(x_2)) \in R^*$ e $b_q(x_1,x_2) = 1$. Neste caso, para todo idempotente $e \in R$, a aplicação $\tau^e_{x_1x_2} : V \to V$ definida por $\tau^e_{x_1x_2}(x_1) = (1-2e)x_1 + eq(x_2)^{-1}x_2$, $\tau^e_{x_1x_2}(x_2) = x_2$ e $\tau^e_{x_1x_2}(y) = y$, para todo $y \in V'$, é uma isometria de V; isto é $\tau^e_{x_1x_2} \in O(V)$. Indiquemos por $I_p(R) = \{e \in R / e^2 = e\}$ o grupo dos idempotentes de R com a operação $e*e' = e+e'-2ee'$. É fácil ver que, para $e,e' \in I_p(R)$, $\tau^e_{x_1x_2}\tau^{e'}_{x_1x_2} = \tau^{e*e'}_{x_1x_2}$, ou seja $I_p(V) = \{\tau^e_{x_1x_2} / e \in I_p(R)\}$ é um subgrupo de $O(V)$, o qual é naturalmente isomorfo á $I_p(R)$.

(1.2) Observação - (1) Se $2 \in R^*$ então, $V = (Rx) \perp V_1$, com $x = -2q(x_2)x_1 + x_2$, $I_p(R) \cong \mu_2(R)$, via $e \to 1-2e$ e $I_p(V) \cong \mu_2(V)$ via $\tau^e_{x_1x_2} \to \tau_x^{(1-2e)}$.

(2) As isometrias τ_x, τ_x^a e $\tau^e_{x_1x_2}$ podem ser naturalmente definidas no caso de um espaço quadrático qualquer.

Seja $I \subseteq R$, $I \neq R$, um ideal de R. Então R/I é também um LG-anel (cf. (I,1.3)) e o homomorfismo canônico $R \to R/I$ induz naturalmente um homomorfismo de grupos de $O(V)$ em $O(V(I))$,

onde (V(I), q(I)) denota a redução módulo I de (V,q) (cf, (II,3.3)). Denotamos por O(V,I) o núcleo deste homomorfismo; isto é, O(V,I) = {$\varphi \in O(V) \;/\; \varphi \equiv id_V \bmod I$}. Indicamos por E(V,I) o subgrupo de O(V) gerado pelas isometrias $\theta E(u,x)\theta^{-1}$ e $\theta E(v,y)\theta^{-1}$, onde $\theta \in E(V)$ e $x,y \in V_o$ são tais que $b_q(x,V_o) \subseteq I$ e $b_q(y,V_o) \subseteq I$; isto é, $x,y \in IV_o$. Além disso, sejam $\phi(V,I) = \{\phi(\lambda) \;/\; \lambda \in R^* \text{ e } \lambda \equiv 1 \bmod I\}$, $\mu_2(V,I) = \{\tau_x^a \;/\; a \in \mu_2(R) \text{ e } a \equiv 1 \bmod I\}$ e $I_p(V,I) = \{\tau^{e}_{x_1x_2} \;/\; e \in I_p(I) = I_p(R) \cap I\}$. Claramente, no caso em que $I=(o)$, $O(V,I) = E(V,I) = \phi(V,I) = \mu_2(V,I) = I_p(V,I) = (id_V)$. Finalmente, no caso em que $I=R$, sejam $O(V,R) = O(V)$, $E(V,R) = E(V)$, $\phi(V,R) = \phi(V)$, $\mu_2(V,R) = \mu_2(V)$ e $I_p(V,R) = I_p(V)$.

§ 2- Geração de O(V,I)

De acordo com o que foi visto no § 4 do Cap.II o subespaço V_o de $V = (Ru \oplus Rv) \perp V_o$ admite sempre uma base canônica $\{x_1,\ldots,x_n\}$, isto é, V_o pode ser escrito na forma $V_o = (Rx_1 \oplus Rx_2) \perp \ldots \perp (Rx_{n-2} \oplus Rx_{n-1}) \perp Rx_n$, com $q(x_n)[\prod_{o \le k \le (n-3)/2}^{i=2k+1} (1-4q(x_i)q(x_{i+1}))q(x_{i+1})] \in R^*$ se n é impar, ou $V_o = (Rx_1 \oplus Rx_2) \perp \ldots \perp (Rx_{n-1} \oplus Rx_n)$, com $\prod_{o \le k \le (n-2)/2}^{i=2k+1} (1-4q(x_i)q(x_{i+1}))q(x_{i+1}) \in R^*$ se n é par .

Neste parágrafo e nos demais assumiremos fixas uma base canônica $\{x_1,\ldots,x_n\}$ para V_o e sua correspondente base dual $\{y_1,\ldots,y_n\}$ via o isomorfismo $d_{b_q} : V \to V^*$; isto é, $b_q(x_i,y_j) = \delta_{ij} = 1$ se $i = j$ e 0 caso contrário.

(2.1) **Proposição** - Se $|R/\mathfrak{p}| \geq 3$, para todo $\mathfrak{p} \in Spm(R)$, então o centro de $O(V)$ é $\{a\,id_V / a \in R, a^2=1\} \cong \mu_2(R)$.

Dem.: Seja φ um elemento do centro de $O(V)$. Para $x \in V_o$, temos $\varphi(x) = \alpha u + \beta v + y$, onde $y \in V_o$ e $\alpha, \beta \in R$. Desde que $|R/\mathfrak{p}| \geq 3$, para todo $\mathfrak{p} \in Spm(R)$, temos que existe $\lambda \in R^*$ tal que $\lambda-1 \in R^*$. Então $\varphi(x) = \varphi\phi(\lambda)(x) = \phi(\lambda)\varphi(x) = \lambda\alpha u + \lambda^{-1}\beta v + y$, o que implica que $\alpha = \beta = 0$ e, consequentemente, $\varphi(V_o) \subseteq V_o$. Observemos ainda que $\varphi(x_1) + b_q(y_1, \varphi(x_1))u = E(u, y_1)\varphi(x_1) = \varphi(x_1) + \varphi(u)$ e, consequentemente $\varphi(u) = b_q(y_1, \varphi(x_1))u = au$, com $a = b_q(y_1, \varphi(x_1))$. Analogamente, usando que $E(v, y_1)\varphi(x_1) = \varphi E(v, y_1)(x_1)$, obtemos também $\varphi(v) = b_q(y_1, \varphi(x_1))v = av$. De $E(v, x)\varphi(u) = \varphi E(v, x)(u)$, para todo $x \in V_o$, deduzimos que $\varphi(x) = ax$. Finalmente, usando que $1 = b_q(u, v) = b_q(\varphi(u), \varphi(v))$, temos $a^2 = 1$, como queríamos. ∎

(2.2) **Teorema** - Sejam R um LG-anel com $|R/\mathfrak{p}| \geq 3$ para todo $\mathfrak{p} \in Spm(R)$ e I um ideal de R. Se $\dim_R V_o \geq 2$, então $O(V,I)$ é gerado por $E(V,I)$, $\phi(V,I)$ e $I_p(V,I) = \{\tau^e_{x_1,x_2} / e \in I_p(I)\}$. Se $\dim_R V_o = 1$, então $O(V,I)$ é gerado por $E(V,I)$, $\phi(V,I)$ e $\mu_2(V,I) = \{\tau^a_{x_1} / a \in \mu_2(R), a \equiv 1 \bmod I\}$.

Dem.: Seja $\varphi \in O(V,I)$. Começaremos por mostrar que se $1 \leq t \leq n$ é um número inteiro tal que $\varphi(x_i) = x_i$, para $1 \leq i \leq t-1$ se $t > 1$ e $\varphi(x_1) \neq x_1$, se $t=1$, é sempre possível modificar φ por elementos de $E(V,I)$ tal que a consequente isometria ψ obtida satisfaz $\psi(x_i)$

$= x_i$ para todo $1 \leq i \leq t$.

Seja $\varphi(u + x_t) = \alpha u + \beta v + z$, onde $\alpha \equiv 1 \bmod I$, $\beta \in I$ e $z \equiv x_t \bmod I$. Mostremos que existe $w \in V_o$ tal que $E(u,w)\varphi(u + x_t) = \alpha' u + \beta v + z'$, onde $\alpha' \in R^*$, $\alpha' \equiv (1 + b_q(w,z)) \bmod I$ e $z' \equiv x_t \bmod I$. Consideremos 2 casos:

Caso 1 - Seja t impar. Neste caso se $t > 1$ temos $V_o = V_1 \perp V_1^{\perp}$, onde V_1 é um subespaço de V_o tal que $(x_1, \ldots, x_{t-1})$ é uma base canônica para V_1 (cf (II,4.4)). Para o espaço quadrático $V' = (Ru \oplus Rv) \perp V_1^{\perp}$, temos que $u + x_t$ é um vetor unimodular de V', pois $b_q(u + x_t, v) = 1$. Agora, para $1 \leq i \leq t-1$, temos $b_q(z, x_i) = b_q(\alpha u + \beta v + z, x_i) = b_q(\varphi(u + x_t), x_i) = b_q(u + x_t, x_i) = 0$, ou seja, $z \in V_1^{\perp}$. Logo existe $w \in V_1^{\perp}$ tal que $E(u,w)\varphi(u + x_t) = \alpha' u + \beta v + z'$, com $\alpha' = \alpha + b_q(w,z) - \beta q(w) \in R^*$ e $z' = z - \beta w \in V_1^{\perp}$ (cf. (II,6.1)). Observamos ainda que $\alpha' \equiv (1 + b_q(w,z)) \bmod I$ e $z' \equiv z \equiv x_t \bmod I$. Se $t = 1$ o resultado é assegurado diretamente pela Prop. (6.1) do Cap. II.

Caso 2 - Seja t par. Neste caso $(x_{t-1}, x_t, \ldots, x_n)$ é uma base canônica para um subespaço de V_o. Mostremos que existe $w = \sum_{i=t-1}^{n} \lambda_i x_i$, tal que $\alpha + b_q(w,z) - \beta q(w) \in R^*$ e $b_q(w, x_{t-1}) = 0$. O fato de $b_q(w, x_{t-1}) = 0$, implica que $w = \lambda_{t-1} x_{t-1} - 2\lambda_{t-1} q(x_{t-1}) x_t + \sum_{i=t+1}^{n} \lambda_i x_i$. Agora, se $z = \sum_{i=t-1}^{n} a_i x_i$ então $1 = b_q(x_{t-1}, x_t) = b_q(x_{t-1}, u + x_t) = b_q(x_{t-1}, \varphi(u + x_t)) = b_q(x_{t-1}, \alpha u + \beta v + z) = b_q(x_{t-1}, z) = 2a_{t-1} q(x_{t-1}) + a_t$, ou seja $a_t = 1 - 2a_{t-1} q(x_{t-1})$. Além disso, $\alpha + b_q(w,z) - \beta q(w) = \alpha + \lambda_{t-1} a_t (1 - 4q(x_{t-1}) q(x_t)) + \lambda_{t-1}^2 q(x_{t-1}) \beta (1 - 4q(x_{t-1}) q(x_t)) + b_q(\sum_{i=t+1}^{n} \lambda_i x_i, z) -$

$-\beta q(\sum_{i=t+1}^{n}\lambda_i x_i) = f(\lambda_{t-1},\ldots,\lambda_n)$. Nosso objetivo agora é mostrarmos que o polinômio f representa uma unidade em R e, desde que R é um LG-anel, basta mostrarmos isto localmente.

Seja $\wp \in Spm(R)$. Se $\alpha \notin \wp$, então tomando $\lambda_i = 0$ para $t-1 \leq i \leq n$, temos que f representa uma unidade em $R_\wp$. Se $\alpha \in \wp$ e $\beta \notin \wp$, temos duas alternativas: i) $q(x_{t-1}) \notin \wp$, então tomando $\lambda_i = 0$, para $t+1 \leq i \leq n$, temos que $f(\lambda_{t-1},\lambda_t,0,\ldots,0)$ representa uma unidade em $R_\wp$ (pois $|R/\wp| \geq 3$); ii) $q(x_{t-1}) \in \wp$, então, $a_t = 1 - 2a_{t-1}q(x_{t-1}) \notin \wp$ e, tomando $\lambda_i = 0$, para $t+1 \leq i \leq n$, temos que, $f(\lambda_{t-1},\lambda_t,0,\ldots,0)$ representa uma unidade em $R_\wp$. Finalmente, se $\alpha \in \wp$ e $\beta \in \wp$, tomamos w como sendo o termo de $\varphi(y_t)$ em V_o. De $b_q(\varphi(y_t),x_i) = 0$, para todo $1 \leq i \leq t-1$, segue-se que $w = \sum_{i=t-1}^{n}\lambda_i x_i$, como desejado. Agora, $1 = b_q(y_t, u + x_t) = b_q(\varphi(y_t), \alpha u + \beta v + z) = b_q(w,z)$ em $R_\wp/\wp R_\wp$, o que mostra que $f(w) \in R_\wp^*$.

Temos então que existe $w = \sum_{i=t-1}^{n}\lambda_i x_i \in V_o$, tal que $E(u,w)\varphi(u + x_t) = \alpha' u + \beta v + z$, onde $\alpha' \in R^*$, $\alpha' \equiv (1 + b_q(w,x_t)) \bmod I$, $\beta \in I$ e $z' \equiv x_t \bmod I$.

Observemos que se $t > 1$, para $1 \leq i \leq t-1$, $b_q(z' - x_t, x_i) = b_q(\alpha' u + \beta v + z', x_i) - b_q(x_t,x_i) = b_q(E(u,w)\varphi(u + x_t), x_i) - b_q(x_t,x_i) = b_q(u + x_t, x_i) - b_q(x_t,x_i) = 0$.

Tomando

$$\psi = E(u,-y_t)E(u,-w)E(u,(1 + b_q(w,x_t) - \alpha')y_t)E(v,(\alpha')^{-1}(z' - x_t))$$
$$E(u,w)\varphi E(u,y_t)$$

temos que $\psi(x_i) = x_i$ para $1 \leq i \leq t$ e $\psi \equiv id_V \bmod I$, pois $1 + b_q(w,x_t) - \alpha' \in I$ e $z' - x_t \in I$. Logo, se ψ é gerada pelas

isometrias dadas, então φ também o é. Portanto, usando indução sobre t, é suficiente mostrarmos o teorema para isometrias φ que fixam x_i, para $1 \leq i \leq n$.

Observemos que, se $\varphi(x_i) = x_i$, $1 \leq i \leq n$, então $\varphi(Ru \oplus Rv) \subseteq Ru \oplus Rv$. De fato, se $\varphi(u) = \alpha u + \beta v + z$, onde $\alpha, \beta \in R$ e $z \in V_o$, então $0 = b_q(u,x_i) = b_q(\varphi(u),x_i) = b_q(z,x_i)$, $1 \leq i \leq n$, o que implica $z = 0$. O mesmo ocorre para $\varphi(v)$.

Seja $\varphi(u) = \alpha' u + \beta v$, onde $\alpha' \equiv 1 \bmod I$ e $\beta \in I$. Para todo $\lambda \in R$, temos $E(u,\lambda y_1)\varphi(u) = \alpha u + \beta v - \beta\lambda y_1$, onde $\alpha = \alpha' - \beta\lambda^2 q(y_1)$, ou seja $\alpha \equiv \alpha' \equiv 1 \bmod I$. Desde que u é um vetor unimodular, temos que $\varphi(u)$ é unimodular e, consequentemente existe $\lambda \in R$ tal que $\alpha \in R^*$ (cf.(II,6.1)). Tomando $\psi = \phi(\alpha^{-1})E(u,-\lambda y_1)E(v,-\alpha^{-1}\beta\lambda y_1)E(u,\lambda y_1)$, temos que ψ é um produto das isometrias dadas, $\psi\varphi$ fixa $u, x_2, \ldots, x_n$ se $n > 1$ e $\psi\varphi$ fixa somente u se $n = 1$. Além disso, segue de $q(\alpha u + \beta v - \beta\lambda y_1) = q(u) = 0$ que $\psi\varphi \equiv id_V \bmod I$.

Desde que $\psi\varphi(u) = u$ e $b_q(u,v) = 1$, obtemos $\psi\varphi(v) = \eta u + v + \gamma y_1$, onde $\eta, \gamma \in I$. Agora, $E(u,\gamma y_1)\psi\varphi$ fixa $u, v, x_2, \ldots, x_n$ se $n > 1$ e fixa somente u e v se $n = 1$. De fato, $E(u,\gamma y_1)\psi\varphi(x_i) = x_i$, para $2 \leq i \leq n$, $E(u,\gamma y_1)\psi\varphi(u) = E(u,\gamma y_1)(u) = u$ e $E(u,\gamma y_1)\psi\varphi(v) = E(u,\gamma y_1)(\eta u + v + \gamma y_1) = (\eta + \gamma^2 q(y_1))u + v = v$, pois $\eta + \gamma^2 q(y_1) = q(\psi\varphi(v)) = q(v) = 0$. Supondo que $n \geq 2$ e usando que $b_q(x_1,x_i) = b_q(x_1,u) = b_q(x_1,v) = 0$ para $3 \leq i \leq n$ temos que $E(u,\gamma y_1)\psi\varphi(x_1) = ax_1 + a'x_2$. De $b_q(x_1,x_2) = 1$ segue-se que $a = 1 - 2a'q(x_2)$. De $q(x_1) = q(E(u,\gamma y_1)\psi\varphi(x_1))$ segue-se que $a'q(x_2) = e \in I_p(R)$. Portanto $E(u,\gamma y_1)\psi\varphi = \tau^e_{x_1x_2}$ para algum $e \in$

$\in I_p(R)$. De $E(u,\gamma y_1)\equiv\psi\equiv\varphi\equiv id_V \bmod I$ segue-se que $e \in I_p(I)$. Se $n=1$, então $E(u,\gamma y_1)\psi\varphi(x_1) = ax_1$ para algum $a \in R$. De $q(x_1) = q(E(u,\gamma y_1)\psi\varphi(x_1))$ segue-se que $a \in \mu_2(R)$. De $E(u,\gamma y_1)\equiv\psi\equiv\varphi\equiv id_V \bmod I$ segue que $a\equiv 1 \bmod I$, o que conclui a demonstração do teorema.■

§ 3 - Subgrupos de $O(V)$ Normalizados por $\Omega(V)$

Denotemos por $\Omega(V) = [O(V),O(V)]$, o subgrupo comutador de $O(V)$. Para todo ideal I de R, seja $\Omega(V,I) = [O(V), O(V,I)]$ o subgrupo comutador misto de $O(V)$ com respeito a I. Claramente, para $I=R$, $\Omega(V,R) = \Omega(V)$ e para $I=(0)$, $\Omega(V,I)=(id_V)$.

Denotemos por $F(V,I)$ o subconjunto de $O(V)$ definido por $F(V,I) = \{\varphi \in O(V) / [\varphi,\Omega(V)] \subseteq \Omega(V,I)\}$. Claramente $\Omega(V,I) \subseteq O(V,I) \subseteq F(V,I)$.

Seja, agora, N um subgrupo de $O(V)$ tal que $\Omega(V,I) \subseteq N \subseteq F(V,I)$. Então $[N, \Omega(V)] \subseteq [F(V,I),\Omega(V)] \subseteq \Omega(V,I) \subseteq N$, de onde segue-se que N é *normalizado por* $\Omega(V)$; isto é, para todo $\theta \in \Omega(V)$ e para todo $\varphi \in N$, $\theta^{-1}\varphi\theta \in N$.

No principal resultado deste parágrafo (veja(3.8)) mostraremos que, sob certas condições sobre R e $\dim_R V$, todo subgrupo N de $O(V)$ normalizado por $\Omega(V)$ (em particular se N é normal em $O(V)$) satisfaz $\Omega(V,I) \subseteq N \subseteq F(V,I)$ para algum ideal I de R. Este resultado foi demonstrado por D. G. James [J] no caso de um anel local.

(3.1) Lema - Sejam α , $\beta \in R$ e $x \in V_o$ tais que $\lambda = 1 - \alpha\beta q(x)$ é

uma unidade. Então $E(v,\alpha x)E(u,\beta x) = E(u,\beta\lambda^{-1}x)E(v,\alpha\lambda x)\phi(\lambda^{-2})$.

Dem.: Basta verificar as imagens de u, v e y $\in V_o$.■

O teorema seguinte, no caso de um anel local, é devido à D. G. James [J].

(3.2) Teorema - Seja $I \leq R$ um ideal. Se, $|R/\mathfrak{p}| \geq 4$, para todo $\mathfrak{p} \in$ $\in Spm(R)$, então $E(V,I) = \Omega(V,I) = [E(V),E(V,I)]$.

Dem.: Desde que R é um LG-anel com $|R/\mathfrak{p}| \geq 4$, para todo $\mathfrak{p} \in$ $\in Spm(R)$, temos que existem unidades λ, ε em R, tais que $\lambda(\varepsilon - 1) = 1$, ou mais precisamente existem λ, $\varepsilon \in R^*$, tais que $\varepsilon - \lambda^{-1} = 1$.

Seja $x \in V_o$, com $b_q(x,V) \leq I$. Então $E(u,x) = \phi(\varepsilon)E(u,\lambda x)\phi(\varepsilon^{-1})E(u,-\lambda x) = [\phi(\varepsilon),E(u,\lambda x)]$, e $E(v,x) = \phi(\varepsilon^{-1})E(v,\lambda x)\phi(\varepsilon)E(v,-\lambda x) = [\phi(\varepsilon^{-1}),E(v,\lambda x)]$, o que mostra que $E(V,I) \leq [O(V),O(V,I)] = \Omega(V,I)$.

De (1.1) e (2.2) segue-se que todo elemento φ de $O(V,I)$, pode ser expresso na forma $\varphi = \tau^{e}_{x_1x_2}\phi(\varepsilon)\psi$, se $\dim_R V_o \geq 2$ ou $\varphi = \tau^{a}_{x_1}\phi(\varepsilon)\psi$ se $\dim_R V_o = 1$, onde $\varepsilon \in R^*$, $\varepsilon \equiv 1 \bmod I$, $a \in \mu_2(R)$, $a \equiv 1 \bmod I$, $e \in I_p(I)$ e $\psi \in E(V,I)$.

De maneira análoga, um elemento $\theta \in O(V)$, pode ser expresso na forma $\theta = \tau^{e'}_{x_1x_2}\phi(\lambda)\chi$, onde $\lambda \in R^*$, $e' \in I_p(R)$ e $\chi \in$ $\in E(V)$.

Suponhamos que $\dim_R V_o \geq 2$. Observemos que

$$[\theta,\varphi] = \tau^{\theta'}_{x_1x_2}\phi(\lambda)\chi\tau^{\theta}_{x_1x_2}\phi(\varepsilon)\psi\chi^{-1}\phi(\lambda^{-1})\tau^{\theta'}_{x_1x_2}\psi^{-1}\phi(\varepsilon^{-1})\tau^{\theta}_{x_1x_2} =$$

$$= \tau^{\theta'}_{x_1x_2}\chi_1\ \tau^{\theta}_{x_1x_2}\psi_2\ \chi_2^{-1}\ \tau^{\theta'}_{x_1x_2}\ \psi_1^{-1}\tau^{\theta}_{x_1x_2} =$$

$$= (\tau^{\theta'}_{x_1x_2}\chi_1\tau^{\theta'}_{x_1x_2})(\tau^{\theta*\theta'}_{x_1x_2}\chi_2^{-1}\tau^{\theta*\theta'}_{x_1x_2})(\tau^{\theta*\theta'}_{x_1x_2}\psi_2\tau^{\theta*\theta'}_{x_1x_2})(\tau^{\theta}_{x_1x_2}\psi^{-1}\ \tau^{\theta}_{x_1x_2})$$

onde $\psi_1 = \phi(\varepsilon)\psi\phi(\varepsilon^{-1}) \in E(V,I)$, $\psi_2 = \phi(\lambda)\psi_1\phi(\lambda^{-1}) \in E(V,I)$, $\chi_1 = \phi(\lambda)\chi\phi(\lambda^{-1}) \in E(V)$ e $\chi_2 = \phi(\varepsilon)\chi_1\phi(\varepsilon^{-1}) \in E(V)$.

Agora usando que $\varepsilon \equiv 1 \bmod I$, e $\in I$, mostra-se facilmente que $(\tau^{\theta'}_{x_1x_2}\chi_1\tau^{\theta'}_{x_1x_2})(\tau^{\theta*\theta'}_{x_1x_2}\chi_2^{-1}\tau^{\theta*\theta'}_{x_1x_2}) \in E(V,I)$ e, consequentemente $[\theta,\varphi] \in E(V,I)$, o que mostra que $\Omega(V,I) \subseteq E(V,I)$. Por um raciocínio idêntico e trocando $\tau^{\theta}_{x_1x_2}$ e $\tau^{\theta'}_{x_1x_2}$ por $\tau^{\alpha}_{x_1}$ e $\tau^{\alpha'}_{x_1}$ nas expressões acima, obtemos também o mesmo resultado no caso $\dim_R V_o = 1$. Temos então $E(V,I) = \Omega(V,I)$ e, em particular $E(V) = \Omega(V)$.

Claramente $E(V,I) \subseteq O(V,I)$ e, portanto $[E(V), E(V,I)] \subseteq \Omega(V,I) = E(V,I)$.

Resta portanto mostrarmos que $E(V,I) \subseteq [E(V),E(V,I)]$. Novamente, desde que $|R/p| \geq 4$, para todo $p \in \mathrm{Spm}(R)$, vê-se facilmente que existem λ, $\varepsilon \in R^*$ tais que $\lambda(\varepsilon^2-1) = 1$. Assim, dado $x \in V_o$, com $b_q(x,V) \subseteq I$, temos: $E(u,x) = \phi(\varepsilon^2)E(u,\lambda x)\phi(\varepsilon^{-2})E(u,-\lambda x) = [\phi(\varepsilon^2),E(u,\lambda x)]$ e $E(v,x) = [\phi(\varepsilon^{-2}),E(v,\lambda x)]$. Logo, para mostrarmos que $E(V,I) \subseteq [E(V),E(V,I)]$, é suficiente mostrarmos que $\phi(\varepsilon^2) \in E(V)$, para todo $\varepsilon \in R^*$. Basta considerarmos $x \in V_o$ com $q(x) \in R^*$, $\varepsilon \in R^*$, $\alpha = (1-\varepsilon)q(x)^{-1} \in R$ e $\beta = 1$ em (3.1) para termos $\phi(\varepsilon^2) \in E(V)$. ∎

(3.3) Lema - Suponhamos que $|R/\mathfrak{p}| \geq 3$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, e $\varphi \in \Omega(V)$. Então existe $\psi \in \Omega(V)$ tal que $\psi\varphi\psi^{-1} = E(u,x)E(v,y)\phi(\varepsilon)\theta$ onde $x, y \in V_o$, $\varepsilon \in R^*$ e θ fixa u e v.

Dem.: Desde que v é um vetor unimodular de V e $\varphi \in \Omega(V)$, temos que $\varphi(v)$ é unimodular. Consequentemente, existe $w \in V_o$ tal que $E(u,w)\varphi(v) = \alpha u + \beta v + z$, com $\alpha \in R$, $\beta \in R^*$ e $z \in V_o$ (cf. (II,6.1)).

Sejam $\varphi_1 = E(v,w)\varphi$ e $\varphi_2 = \phi(\beta)E(u,\beta^{-1}z)\varphi_1$. Temos então $0 = q(v) = q(\varphi_1(v)) = \alpha\beta + q(z)$, o que implica que $\varphi_2(v) = v$.

Seja $\varphi_2(u) = \lambda u + \gamma v + z'$, com $\lambda, \gamma \in R$ e $z' \in V_o$. Observemos que $\lambda = b_q(\varphi_2(u),\varphi_2(v)) = 1$ e $0 = q(u) = q(\varphi_2(u)) = \gamma + q(z')$. Assim $\theta = E(v,z')\varphi_2$ é uma isometria que fixa u e v. Ainda, $\varphi_1 = E(u,-\beta^{-1}z)\phi(\beta^{-1})E(v,z')\theta$, o que mostra que $E(v,w)\varphi = E(u,x)E(v,y')\phi(\varepsilon')\theta$, com $x, y' \in V_o$, $\varepsilon' \in R^*$ e $\theta \in \Omega(V)$ que fixa u e v. Portanto $E(v,w)\varphi E(v,-w) = E(u,x)E(v,y' + \theta(-w))\phi(\varepsilon'^{-1})\theta = E(u,x)E(v,y)\phi(\varepsilon)\theta$, o que mostra o lema, pois $\psi = E(v,w) \in E(V) = \Omega(V)$ (cf. (3.2)). ∎

(3.4) Lema - Suponhamos que $|R/\mathfrak{p}| > 5$ e $\neq 9$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$ e, $\varphi = E(u,x)E(v,y)\phi(\varepsilon)\theta \in N$, onde $x, y \in V_o$, $\varepsilon \in R^*$ e $\theta \in \Omega(V)$ fixa u e v. Então, existem $\varepsilon_1, \varepsilon_2 \in R^*$ (que independem de φ) tais que $E(u,\varepsilon_1 x)$ e $E(v,\varepsilon_2 y)$ estão em N.

Dem.: Escolhendo $\lambda \in R^*$ tal que $1 - \lambda^2 \in R^*$, temos $\phi(\lambda^2) = [\phi(\lambda),\Delta] \in \Omega(V)$. Então $[\varphi,\phi(\lambda^2)] \in N$ e $[\varphi,\phi(\lambda^2)] = E(u,x)E(v,(1 - \lambda^{-2})y)E(u,-\lambda^2 x)$. Usando o fato que N é

normalizado por $\Omega(V)$ e que $\Omega(V) = E(V)$ (cf. (3.2)). Obtemos $E(u,-x)[\varphi,\phi(\lambda^2)]E(u,x) = E(v,(1-\lambda^{-2})y)E(u,(1-\lambda^2)x) \in N$. Agora, $1-\lambda^2 \in R^*$ e $1-\lambda^{-2} = \lambda^{-2}(\lambda^2-1) \in R^*$. Consequentemente é suficiente mostrarmos que se $E(u,x)E(v,y) \in N$, então existem ε_1, $\varepsilon_2 \in R^*$ tais que $E(u,\varepsilon_1 x)$ e $E(v,\varepsilon_2 y)$ estão em N.

Dados λ_1 e $\lambda_2 \in R^*$, consideremos $\alpha = \lambda_1^2 + \lambda_2^2$ e $\beta = \lambda_1^{-2} + \lambda_2^{-2}$.

Afirmação - Podemos escolher λ_1, $\lambda_2 \in R^*$, de modo que $\beta \in R^*$ e $1 - \alpha^2\beta^2 \in R^*$.

Desde que $E(u,x)E(v,y) \in N$, e $\phi(\lambda_i^2) \in \Omega(V)$, $i = 1, 2$, temos $\phi(\lambda_i^2)E(u,x)E(v,y)\phi(\lambda_i^{-2}) = E(u,\lambda_i^2 x)E(v,\lambda_i^{-2}y) \in N$, $i = 1, 2$. Tomando $E(u,\lambda_1^2 x) \in E(V) = \Omega(V)$ (cf. (3.2)), obtemos $E(u,\lambda_1^2 x)E(u,\lambda_2^2 x)E(v,\lambda_2^{-2}y)E(u,-\lambda_1^2 x) = E(u,\alpha x)E(v,\lambda_2^{-2}y)E(u,-\lambda_1^2 x) \in N$ e, como $E(u,\lambda_1^2 x)E(v,\lambda_1^{-2}y) \in N$, temos que $E(u,\alpha x)E(v,\beta y) \in N$.

Repetindo o mesmo argumento obtemos $E(u,\alpha^2 x)E(v,\beta^2 y) \in N$ e, como $\beta \in R^*$ e $\phi(\beta^2) \in \Omega(V)$, segue-se que $E(u,\alpha^2\beta^2 x)E(v,y) \in N$, o que implica que $E(v,-y)E(u,-\alpha^2\beta^2 x) = (E(u,\alpha^2\beta^2 x)E(v,y))^{-1} \in N$.

Agora, juntando o fato que $E(u,x)E(v,y) \in N$, obtemos que $E(u,\varepsilon_1 x) \in N$, onde $\varepsilon_1 = 1 - \alpha^2\beta^2 \in R^*$. Analogamente, mostra-se que existe $\varepsilon_2 \in R^*$ tal que $E(v, \varepsilon_2 y) \in N$.

Finalmente, provaremos a afirmação, ou seja, que existem λ_1, $\lambda_2 \in R^*$ tais que $(\lambda_1^2 + \lambda_2^2) / (\lambda_1\lambda_2)^2 \in R^*$ e $1 - (\lambda_1^2 + \lambda_2^2)^2 / (\lambda_1\lambda_2)^4 \in R^*$. Para tanto, basta provarmos que o polinômio $f(X_1,X_2) = (X_1^2 + X_2^2)(X_1^4 X_2^4 - (X_1^2 + X_2^2)^4)X_1X_2$, representa uma unidade em R. Mas R é um LG-anel com $|R/\mathfrak{n}| > 5$ e $\neq 9$, para todo $\mathfrak{n} \in Spm(R)$. Logo é suficiente mostrar que f representa um

elemento não nulo em $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong R/\mathfrak{p}$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$ tal que $|R/\mathfrak{p}| > 5$ e $\neq 9$.

Se $|R/\mathfrak{p}| = 7$, então $f(1,1) \neq 0$. Se $|R/\mathfrak{p}| = 8$, então $R/\mathfrak{p} \cong \mathbb{F}_2(\alpha)$, com $\alpha^3 + \alpha + 1 = 0$ e $f(1,\alpha) \neq 0$. Se $|R/\mathfrak{p}| = 11$, então $f(1,1) \neq 0$. Se $|R/\mathfrak{p}| > 11$, então f representa um elemento não nulo em $R/\mathfrak{p}$, pois o grau de f é 12. Portanto f representa uma unidade em R, como queríamos.■

(3.5) Observação - Se trocarmos as hipóteses $|R/\mathfrak{p}| > 5$ e $\neq 9$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, por 2, 3 e 5 $\in R^*$ em (3.4) temos $E(u,x)$ e $E(v,y)$ estão em N. Neste caso a demonstração é análoga a demonstração do Lemma 5.2 de [I].

(3.6) Lema - Se $|R/\mathfrak{p}| \geq 3$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, e $x, y, \in V_o$ são tais que $q(x)q(y) \in R^*$, então as isometrias $\phi(q(x)q(y))\tau_x\tau_y$ e $\phi(-q(x))\Delta\tau_x$ estão em $\Omega(V)$.

Dem.: Comparando as imagens de u, v e $z \in V_o$, vemos que $\Delta\tau_x =$ $= \phi(-q(x))E(v,-x)E(u,q(x)^{-1}x)E(v,-x)$. Consequentemente $\phi(-q(x))\Delta\tau_x \in E(V) = \Omega(V)$ (cf.(2.2)).

Agora de (1.1), (3.2) e $\phi(-q(x))\Delta\tau_x \in \Omega(V)$ segue-se facilmente que $\phi(q(x)q(y))\tau_x\tau_y \in \Omega(V)$.■

Antes de vermos o próximo resultado observemos que se (V,q) é um espaço quadrático sobre R, tal que $\{x_1,\ldots,x_n\}$ é uma base estritamente canônica de V, a qual sempre existe se $|R/\mathfrak{p}| \geq 4$ para todo $\mathfrak{p} \in \mathrm{Spm}(R)$ (cf.(II, 4.5)), e $\{y_1,\ldots,y_n\}$ é a

correspondente base dual, então $q(y_i) \in R^*$, $1 \leq i \leq n$. De fato, basta observar que: a) se n é par e $V = (Rx_1 \oplus Rx_2) \perp \ldots \perp (Rx_{n-1} \oplus Rx_n)$, então $y_i = \alpha_i^{-1}(-2q(x_{i+1})x_i + x_{i+1})$, $y_{i+1} = \alpha_i^{-1}(x_i - 2q(x_i)x_{i+1})$ onde $\alpha_i = 1 - 4q(x_i)q(x_{i+1})$ para $i = 2k + 1$, com $0 \leq k \leq (n-2)/2$; b) se n é impar e $V = (Rx_1 \oplus Rx_2) \perp \ldots \perp (Rx_{n-2} \oplus Rx_{n-1}) \perp \ldots \perp Rx_n$, os y_i e y_{i+1} para $i = 2k + 1$, com $0 \leq k \leq (n-3)/2$, são dados pelas mesmas fórmulas e $y_n = b_q(x_n, x_n)^{-1}x_n$.

Assumiremos, a partir de agora, que $|R/\mathfrak{p}| \geq 4$ para todo $\mathfrak{p} \in \mathrm{Spm}(R)$ e que a base canônica $(x_1, \ldots, x_n)$ de V_o, considerada no início do § 2, seja também estritamente canônica.

(3.7) Lema - Suponhamos que $|R/\mathfrak{p}| \geq 4$, para todo $\mathfrak{p} \in \mathrm{Spm}(R)$, e $\dim_R V \geq 7$. se $E(u,z) \in N$, então $\Omega(V, z.V) \subseteq N$, onde $z.V$ é o ideal de R gerado por $b_q(z,x)$; $x \in V$.

Dem.: Desde que $\Omega(V, z.V) = E(z.V)$ (cf. (2.2)), temos que $\Omega(V, z.V)$ é gerado por $\theta E(u,z)\theta^{-1}$ e $\theta E(v,z)\theta^{-1}$, com $\theta \in E(V)$. Mas $E(V) = \Omega(V)$ (cf. (3.2)), e N é normalizado por $\Omega(V)$, então $\theta E(u,z)\theta^{-1} \in N$, para todo $\theta \in E(V) = \Omega(V)$. Logo é suficiente mostrarmos que se $E(u,z) \in N$, então $E(v,z) \in N$.

Seja $z = \sum_{i=1}^{n} \alpha_i x_i = \sum_{i=1}^{n} \beta_i y_i$, $\alpha_i, \beta_i \in R$. Considerando $x, y \in V_o$, com $\varepsilon = q(x)q(y) \in R^*$ e $b_q(x,y) = 1$, temos $\varepsilon\tau_x\tau_y(z) - \varepsilon\tau_y\tau_x(z) = b_q(y,z)x - b_q(x,z)y$. Mas $E(u, \varepsilon\tau_x\tau_y(z) - \varepsilon\tau_x\tau_y(z)) = E(u, \varepsilon\tau_x\tau_y(z))E(u, \varepsilon\tau_y\tau_x(z))^{-1} =$

$= (\phi(\varepsilon)\tau_x\tau_y)E(u,z)(\phi(\varepsilon)\tau_x\tau_y)^{-1}(\phi(\varepsilon)\tau_y\tau_x)^{-1}E(u,z)^{-1}(\phi(\varepsilon)\tau_y\tau_x) \in N$,

pois $\phi(\varepsilon)\tau_x\tau_y$ e $\phi(\varepsilon)\tau_y\tau_x$ estão em $\Omega(V)$ (cf.(3.6)).

Obtemos então que $E(u, b_q(y,z)x - b_q(x,z)y) \in N$, para todo $x, y \in V_o$ com $b_q(x,y) = 1$, $q(x)q(y) \in R^*$ e $z \in V$, com $E(u,z) \in N$.

Tomando $x = x_i$ e $y = y_i$, temos $E(u, \alpha_i x_i - \beta_i y_i) \in N$, para $1 \leq i \leq n$. Para $x = x_i + \lambda x_j$, $y = y_i$, tais que $b_q(x_i, x_j) = 0$, $\lambda \in R$; $q(x) \in R^*$ (que existem pois $\dim_R V_o \geq 5$ e R é um LG-anel com $|R/\mathfrak{p}| \geq 4$, para todo $\mathfrak{p} \in Spm(R)$) obtemos $E(u, \lambda(\alpha_i x_j + \beta_j y_i)) \in N$.

Considerando $z = \lambda(\alpha_i x_j + \beta_j y_i)$, $y = cy_j + \eta y_k$ e $x = \eta^{-1}x_k$, com $b_q(x_i, x_j) = b_q(x_i, x_k) = b_q(x_j, x_k) = 0$ (que existem pois $\dim_R V_o \geq 5$), $c \in R$ e $\eta \in R^*$ é tal que $q(y) \in R^*$ (que existe pois R é um LG-anel com $|R/\mathfrak{p}| \geq 4$, para todo $\mathfrak{p} \in Spm(R)$), temos $E(u, b_q(y,z)x - b_q(x,z)y) = E(u, c\lambda\eta^{-1}\alpha_i x_k) \in N$. Disto concluimos que $E(u, c'\alpha_i x_k) \in N$, para todo $c' \in R$ e para todo $i, k \in \{1, \ldots, n\}$, tais que $b_q(x_i, x_k) = 0$.

Agora, tomando $z = c'\alpha_i x_k$, $y = \gamma y_i + y_k$, $x = \gamma^{-1}x_i$, com $b_q(x_i, x_k) = 0$ e $\gamma \in R^*$, tal que $q(y) \in R^*$, temos $E(u, c'\gamma^{-1}\alpha_i x_i) \in N$. Portanto, $E(u, c\alpha_i x_i) \in N$, para todo $c \in R$ e $1 \leq i \leq n$.

Tomando $\psi = \phi(-q(x_i))\Delta\tau_{x_i} \in \Omega(V)$ (cf (3.6)) obtemos $\psi E(u, c\alpha_i x_i)\psi^{-1} = E(v, cq(x_i)^{-1}\alpha_i x_i) \in N$ para todo $1 \leq i \leq n$ e $c \in R$. Tomando $c' = cq(x_i)^{-1}$, obtemos $E(v, c'\alpha_i x_i) \in N$ para todo $c' \in R$ e $1 \leq i \leq n$.

Portanto, tomando $c' = 1$, temos $E(v,z) = E(v, \sum_{i=1}^{n} \alpha_i x_i) = \prod_{i=1}^{n} (E(v, \alpha_i x_i)) \in N$ como queríamos.

(3.8) Teorema - Suponhamos que $|R/\wp| \geq 5$ e $\neq 9$, para todo $\wp \in$ $\in Spm(R)$ e $dim_R V \geq 7$. Se $N \leq O(V)$ é um subgrupo normalizado por $\Omega(V)$ e I é o maior ideal de R tal que $\Omega(V,I) \leq N$, então $\Omega(V,I) \leq$ $\leq N \leq F(V,I)$.

Dem.: Seja $\varphi \in N$. De (3.3), existe $\psi \in \Omega(V)$ tal que $\psi\varphi\psi^{-1} =$ $= E(u,x)E(v,y)\phi(\varepsilon)\theta \in N$, onde $x, y \in V_o$, $\varepsilon \in R^*$ e $\theta \in O(V)$ fixa u e v. De (3.4), existem ε_1, $\varepsilon_2 \in R^*$ tais que $E(u,\varepsilon_1 x)$ e $E(v,\varepsilon_2 y)$ estão em N.

Observemos que $\varepsilon_1 x.V = x.V$, $\varepsilon_2 y.V = y.V$ e, $\Omega(V,x.V) \leq N$ e $\Omega(V,y.V) \leq N$ (cf.(3.7)). Consequentemente, da maximalidade de I, temos $x.V \leq I$ e $y.V \leq I$, o que implica que $E(u,x)$, $E(v,y) \in E(V,I) = \Omega(V,I) = [E(V),E(V,I)]$ (cf.(3.2)). Isto mostra que $E(u,x)E(v,y) \in F(V,I)$.

Desde que $\psi\varphi\psi^{-1} \in N$ e $E(u,x)E(v,y) \in \Omega(V,I) \leq N$, segue-se que $\phi(\varepsilon)\theta \in N$. Para $z \in V$, arbitrário, temos $[E(u,-z),\phi(\varepsilon)\theta] = E(u,\varepsilon\theta(z) - z) \in N$, pois $E(V) = \Omega(V)$ (cf.(3.2)), de onde segue-se que $\Omega(V,\varepsilon\theta(z) - z) \leq N$ (cf.(3.7)). Novamente, pela maximalidade de I, temos que $(\varepsilon\theta(z) - z).V \leq I$. De maneira análoga $[E(v,-z),\phi(\varepsilon)\theta] = E(v,\varepsilon^{-1}\theta(z) - z) \in N$ e, consequentemente $(\varepsilon^{-1}\theta(z) - z).V \leq I$, o que implica que $E(u,\varepsilon^{-1}\theta(z) - z)$ e $E(v,\varepsilon^{-1}\theta(z) - z)$ estão em $E(V,I)$. Assim, $\phi(\varepsilon)\theta \in F(V,I)$ e, como $E(u,x)E(v,y) \in F(V,I)$, temos $\psi\varphi\psi^{-1} \in F(V,I)$ com $\psi \in \Omega(V)$.

Portanto, para todo $\tau \in E(V)$, temos $[\psi\varphi\psi^{-1},\tau] \in$ $\in E(V,I)$ e, como $\psi \in \Omega(V)$ (cf.(3.2)), então $\psi^{-1}[\psi\varphi\psi^{-1},\tau]\psi =$ $= \varphi(\psi^{-1}\tau\psi)\varphi^{-1}(\psi^{-1}\tau\psi)^{-1} \in E(V,I)$, o que mostra que $\varphi \in F(V,I)$,

como queríamos■

REFERÊNCIAS BIBLIOGRÁFICAS

[A] Arf, C.; *Untersuchungen über Quadratische Formen in Körpern der Charakteristik 2*, J. reine und angew Math. 183, 148 - 167 (1941).

[B] Baeza, R.; *Quadratic forms over semi-local rings*, Lecture Notes in Mathematics 655, Springer Verlag, (1978).

[Ba] Bass, H.; *Lectures on Topics in algebraic K-Theory*, Tata Inst. Fund. Res., Bombay, (1961).

[Bo] Bourbaki, *Algèbre Commutative*, Chap. 2, Hermann, (1961).

[E-G] Estes, D.; Guralnick, R.; *Module equivalences: Local to Global when primitive polynomials represent units*, J. of Algebra 77, 138 - 157 (1982).

[G-W] Goodearl, K. R.; Warfield, R. B. Jr; *Algebras over Zero-Dimensional Rings*, Math. Ann. 223, 157 - 168 (1976).

[I] Ishibashi, H.; *Structure of O(V) over Full Rings*, J. of Algebra 75, 1 - 9 (1982).

[J] James, D. G.; *On the Structure of Orthogonal Groups over Local Rings*, Am. J. Math. 95, 255 - 265 (1973).

[K] Kirkwood, B. H.; *Orthogonal geometry over rings with stability conditions*, PhD. Thesis, Oklahoma University, (1977).

[K-McD]$_1$ Kirkwood, B. H.; McDonald, B. R.; *The orthogonal group of a full ring*, J. of Algebra 51, 536 - 549 (1978).

[K-McD]$_2$ Kirkwood, B. H.; McDonald, B. R,; *The Witt ring of a full ring*, J. of Algebra 64, 148 - 166 (1980).

[Kn]$_1$ Knebusch, M.; *Bemerkungen zur Theorie der quadratischen Formen über semi-lokalen Ringen*, Scrhften des Math. Inst. der Univ. des Saarlandes, Saarbrüchen (1971).

[Kn]$_2$ Knebusch, M.; *Isometrien über semi-lokalen Ringer*, Math. Z. 108, 255 - 268 (1969).

[Kn]$_3$ Knebusch, M.; *Symmetric bilinear forms over algebraic varietes*, Conference on Quadratic Forms, 1976, Ed. G. Orzech, Queen's Papers in Pure and App. Math. 46 (1977).

[K-R-W]$_1$ Knebusch, M.; Rosenberg, A.; Ware, R.; *Signatures on*

semi-local rings, J. of Algebra 26, 208 - 250 (1973).

[K-R-W]$_2$ Knebusch, M.; Rosenberg, A.; Ware, R.; *Strcture of Witt rings and quotients of abelian groups rings*, Am. J. of Math. 94, 119 - 155 (1972).

[L] Lam, T. Y.; *The algebraic theory of quadratic forms*, Benjamin (1973).

[Mc-W] McDonald, B. R.; Waterhouse, W. C.; *Projective Modules over rings with many units*, Proc. Am. Math. Soc. 83, 455 - 458 (1981).

[M-V] Micali, A.; Villamayor, O. E.; *Sur les algèbres de Clifford*, Ann. Sc. Ec. Norm. Sup. 1, 271 - 304 (1968).

[M] Milnor, J.; *Symmetric inner produts in Characteristic 2*, Prospects in Math., Annals Study 70, Princeton Univ. Press(1971).

[Pf] Pfister, A.; *Quadratische Formen in biliebigen Körpern*, Inv. Math. 1, 116 - 132 (1966).

[P] Pierce, R.; *Associative Algebras*, G. T. M. 88, Springer Verlag (1982).

[Sa] Sah, C-H.; *Symmetric bilinear forms and quadratic forms*, J. of Algebra 20, 144 - 169 (1972).

[S] Serre, J. P.; *Cours d'Arithmetique*, Collection Sup., Press Univ. de France (1970).

[W] Witt, E.; *Theorie der quadratischen Formen in beliebigen Körpern*, J. reine und ang. Math. 176, 31 - 44 (1937).