Grupos Ortogonal e Unitário sobre Anéis Locais

VERA LÚCIA GARCIA

Orientadora: PROF^ª. DR^ª. IRES DIAS

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

USP - São Carlos
1996

“Aos meus pais e ao Mauro.”

Inicialmente agradeço À Deus, por ter me dado forças suficientes a fim de superar os obstáculos e conquistar o meu objetivo. Agradeço à profª Ires pela sua grande dedicação, paciência e amizade; aos meus pais e meus irmãos que me apoiaram e incentivaram todo o tempo; ao Mauro, que esteve sempre ao meu lado com seu amor, carinho e amizade; aos amigos que aqui conquistei e jamais esquecerei; à Ana Vitti, pela sua grande amizade; à CAPES pelo auxílio financeiro recebido; às secretárias da pós-graduação: Beth e Laura, e aos demais funcionários do ICMSC, pela simpatia, atenção e eficiência; e aos professores Ozírde (Dide) e Sandra Godoy, pelo apoio e atenção.

Abstract

The purpose of this work is to present a complete set of generators of the unitary and orthogonal groups of an isotropic space over a local ring.

Resumo

Neste trabalho apresentamos um conjunto completo de geradores dos grupos unitário e ortogonal de um espaço isotrópico sobre um anel local.

Índice

Introdução	1
1 Anéis Locais com Involução	3
1.1 Módulos Projetivos sobre um anel local	3
1.2 Anéis com involução	10
2 Espaços Hermitianos e Unitários	14
2.1 Espaços hermitianos sobre anéis locais com involução	14
2.2 Decomposição de módulos λ -hermitianos sobre anéis locais	25
2.3 Espaços Unitários sobre anéis locais	32
3 Geradores dos Grupos Unitário e Ortogonal sobre um Anel Local	44
3.1 Isometrias de $(M, [k])$	45
3.2 Geradores de $\mathcal{U}(M)$ e $\mathcal{O}(M)$	49
Bibliografia	61

Introdução

A teoria das formas quadráticas sobre corpos, teve origem em 1937 através de um artigo de Ernst Witt. Em meados de 1960, com o desenvolvimento da topologia algébrica e da K -teoria algébrica levou-se ao estudo de formas quadráticas sobre anéis comutativos e formas λ -hermitianas sobre anéis (não necessariamente comutativos) com involução. Os excelentes livros de M.-A. Knus [6] e W. Scharlau [9] contém grande parte dos artigos recentes publicados nesta direção.

Na teoria algébrica de formas quadráticas sobre anéis comutativos, uma questão fundamental é a descrição do grupo ortogonal de um espaço quadrático isotrópico. Analogamente, na teoria algébrica das formas λ -hermitianas isotrópicas sobre um anel com involução, é fundamental o estudo do grupo unitário. Tais questões levam rapidamente à fronteira do que se conhece em relação ao anel de base sobre os quais esses grupos são construídos. Nesta direção citamos os trabalhos de D. G. James [4] e [5] sobre anéis locais com 2 inversível e sobre uma classe mais geral de anéis citamos os artigos de I. Dias [2] e [3].

Neste trabalho, apresentamos uma descrição completa dos geradores do grupo ortogonal e do unitário, de um espaço isotrópico sobre um anel local, sem assumir a inversibilidade de 2 no anel de base, generalizando assim os resultados de James. Para tanto apresentamos os resultados para o caso geral, ou seja quando o anel local não é necessariamente comutativo e, em seguida apresentamos os análogos para o caso comutativo, comparando assim os resultados.

No capítulo 1, apresentamos as definições e algumas propriedades básicas de anéis

locais, módulos projetivos finitamente gerados sobre um anel local baseados em [7] e, também de anéis com involução ou mais geralmente de anéis unitários e módulos sobre tais anéis baseado em [6].

No capítulo 2, introduzimos a teoria das formas λ -hermitianas sobre anéis com involução, bem como dos espaços unitários e quadráticos utilizando o conceito de forma parâmetro sobre um anel com involução. Com isso, estudamos os Teoremas de Decomposição destes espaços, seguindo Knus [6] e Baeza [1] (no caso comutativo), os quais são essenciais para a caracterização dos geradores dos grupos unitário e ortogonal.

O capítulo 3 contém uma caracterização dos geradores dos grupos ortogonal e unitário de um espaço isotrópico sobre um anel local juntamente com uma comparação entre os resultados obtidos no caso comutativo (grupo ortogonal) e no caso não comutativo (grupo unitário).

Capítulo 1

Anéis Locais com Involução

O objetivo deste capítulo é apresentarmos propriedades básicas dos anéis locais (não necessariamente comutativo), de involução sobre tais anéis, bem como dos módulos projetivos finitamente gerados sobre anéis locais. Assim, estaremos aptos ao estudo dos espaços quadráticos e/ou hermitianos sobre tais anéis. Finalizamos este capítulo com um resultado sobre matrizes sobre um anel local, o qual nos será de grande utilidade nos capítulos seguintes.

1.1 Módulos Projetivos sobre um anel local

No que segue, sempre que escrevermos “anel A ” estaremos nos referindo a um anel (não necessariamente comutativo), com elemento identidade 1. Denotaremos também por A^* o grupo das unidades de A e $\text{rad } A$ o radical de Jacobson de A , isto é, a intersecção de todos os ideais maximais à direita de A .

Teorema 1.1 *Seja A um anel. As seguintes afirmações são equivalentes:*

- (i) *A tem um único ideal maximal à direita.*
- (ii) *A tem um único ideal maximal à esquerda.*
- (iii) *$A/\text{rad } A$ é um anel com divisão.*

(iv) $A - A^*$ é um ideal de A .

(v) $A - A^*$ é um grupo aditivo.

(v') Se $a_1 + a_2 + \dots + a_n \in A^*$ para algum natural n , então $a_i \in A^*$, para algum $i = 1, \dots, n$.

(v'') Se $a, b \in A$ são tais que $a + b \in A^*$, então $a \in A^*$ ou $b \in A^*$.

Dem.: Se mostrarmos que (i) $\Leftrightarrow$ (iii), então por simetria também teremos (ii) $\Leftrightarrow$ (iii).

(iii) $\Rightarrow$ (i). Seja $\mathcal{M}$ um ideal maximal à direita qualquer de A . Então $\text{rad } A \subseteq \mathcal{M}$. Reduzindo módulo $\text{rad } A$ temos que $\mathcal{M}/\text{rad } A$ é um ideal de $A/\text{rad } A$ e, como $A/\text{rad } A$ é um anel com divisão, obtemos $\mathcal{M}/\text{rad } A = A/\text{rad } A$ ou $\mathcal{M}/\text{rad } A = \{0\}$. Mas, $\mathcal{M} \neq A$, logo $\mathcal{M} = \text{rad } A$ e temos (i).

(i) $\Rightarrow$ (iii). De (i) segue que $\text{rad } A$ é o único ideal maximal à direita de A . Então, pela correspondência dos ideais, temos que $A/\text{rad } A$ tem somente os ideais à direita triviais, ou seja, $A/\text{rad } A$ é um anel com divisão.

(iii) $\Rightarrow$ (iv). Desde que $A/\text{rad } A$ é um anel com divisão, temos $(A/\text{rad } A)^* = (A/\text{rad } A) - \{\bar{0}\}$. Logo $A^* = A - \text{rad } A$ e assim, $A - A^* = \text{rad } A$ que é um ideal de A .

(iv) $\Rightarrow$ (v) $\Rightarrow$ (v') $\Rightarrow$ (v''). São imediatas.

(v'') $\Rightarrow$ (iii). Seja $r \notin \text{rad } A$. Então, da definição de $\text{rad } A$, temos que existe um ideal maximal à direita $\mathcal{M}$ de A tal que $r \notin \mathcal{M}$. Assim, $\mathcal{M} + rA = A$ o que implica que $1 = x + ry$, para algum $y \in A$ e $x \in \mathcal{M}$. Por (v''), temos $ry \in A^*$ e, em particular, r admite inverso à direita em $A/\text{rad } A$. Logo, (iii) segue. ■

Um anel A satisfazendo as equivalências do **Teo.(1.1)** é dito ser um *anel local*. Denotaremos por $\mathcal{M} = \text{rad } A$ o único ideal maximal à direita (e/ou à esquerda) de A . O anel quociente $A/\mathcal{M}$ será denominado o *anel das classes residuais* de A , o qual será um corpo ou um anel com divisão dependendo de A ser ou não comutativo.

Exemplos 1.1 Primeiramente veremos alguns exemplos de anéis locais comutativos.

- (1) Todo corpo K é um anel local, onde $\mathcal{M} = \{0\}$ é o único ideal maximal de K .
- (2) Se A é anel local comutativo e I é um ideal de A , então A/I é um anel local, pela correspondência de ideais.
- (3) Se A é um anel local comutativo com ideal maximal $\mathcal{M}$ então $A[[x]]$, o anel das séries de potências em uma variável x sobre A , é um anel local, com ideal maximal consistindo de todas as séries de potências com termos constantes em $\mathcal{M}$.
- (4) A localização de um anel comutativo A em um ideal primo $\mathcal{P}$ é um anel local $A_{\mathcal{P}}$ com único ideal maximal $\mathcal{P}A_{\mathcal{P}}$. Por exemplo, se $A = \mathbb{Z}$ e $\mathcal{P} = (p)$, com p um número primo, então $A_{\mathcal{P}} = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q}; p \text{ não divide } b \right\}$ é um anel local com único ideal maximal $(p)\mathbb{Z}_{(p)}$, o qual é denominado o *anel dos inteiros p -ádicos*.

Vejamos agora alguns exemplos de anéis locais não comutativos.

- (5) Todo anel com divisão é um anel local.
- (6) Se D é um anel com divisão, ou mais geralmente se D é um anel local não comutativo, então o anel das séries formais sobre D , $D[[x]]$ é um anel local não comutativo com ideal maximal como descrito no exemplo (3).
- (7) Sejam D um anel com divisão e R o anel das matrizes $n \times n$ triangulares superiores sobre D . O radical de Jacobson de R , J , que consiste das matrizes em R que possuem as diagonais nulas é tal que $J^n = 0$, ou seja é nilpotente de ordem n . Seja A o subanel de R consistindo das matrizes com diagonal constante. Temos que $J \subseteq \text{rad } A$ e, desde que $A = 1D \oplus J$, temos que $A/J \cong D$. Assim, A é um anel local com $\text{rad } A = J = \text{rad } R$.

Iniciaremos agora o estudo dos módulos sobre um anel local A . Todos os A -módulos serão considerados A -módulos à direita unitários.

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

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

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

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

Dizemos que uma seqüência exata

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

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

Para uma seqüência exata curta o seguinte resultado é imediato.

Proposição 1.1 *Se uma seqüência exata curta de A -módulos à direita*

$$0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$$

cinde, então $Y \cong X \oplus Z$ (isomorfismo de A -módulos à direita).

Definição 1.2 *Seja M um A -módulo à direita. Dizemos que M é um A -módulo livre à direita se M admite uma base. M é dito ser um A -módulo projetivo se, para todo homomorfismo sobrejetor de A -módulos à direita, $f: M' \rightarrow N'$, e todo A -homomorfismo $g: M \rightarrow N'$, existir um A -homomorfismo $h: M \rightarrow M'$ tal que $f \circ h = g$, ou seja, o seguinte diagrama é comutativo:*

$$\begin{array}{ccc} & N' & \xleftarrow{f} M' \\ g \uparrow & \searrow \exists & \nearrow h \\ M & & \end{array}$$

É fácil ver que todo A -módulo livre é projetivo. A seguinte proposição é muito conhecida em Álgebra Homológica e oferece algumas caracterizações alternativas de módulos projetivos. Sua demonstração pode ser encontrada em livros clássicos de álgebra, por exemplo em [7].

Proposição 1.2 *As seguintes afirmações são equivalentes:*

- (a) M é um A -módulo projetivo.
- (b) M é (isomorfo) a um somando direto de um A -módulo à direita livre.
- (c) Todo homomorfismo sobrejetor de A -módulos à direita sobre M cinde, ou seja a seqüência exata curta

$$0 \longrightarrow \text{Ker } f \longrightarrow N \xrightarrow{f} M \longrightarrow 0$$

de A -módulos cinde.

Observe que dado um A -módulo à direita M , o A -módulo dual $M^* = \text{Hom}(M, A)$ é um A -módulo à esquerda através da operação $(af)m = af(m)$, para todo $f \in M^*$, mas podemos ver também M^* como um A -módulo à direita, com a multiplicação por escalar dada por $f.a = af$, para todo $f \in M^*$ e $a \in A$.

Dizemos que M é um A -módulo finitamente gerado se existem elementos $x_1, \dots, x_n \in M$ tais que para todo $m \in M$, $m = x_1 a_1 + \dots + x_n a_n$, com $a_i \in A$, $i = 1, \dots, n$.

A seguir teremos um resultado que é de fundamental importância na teoria de anéis e módulos.

Proposição 1.3 (Lema de Nakayama) *Sejam A um anel, M um A -módulo à direita finitamente gerado e $\mathcal{M}$ um ideal à direita de A com $\mathcal{M} \neq A$. As seguintes afirmações são equivalentes:*

- (i) $\mathcal{M} \subseteq \text{rad } A$.
- (ii) Se $M\mathcal{M} = M$ então $M = 0$.
- (iii) Para todo A -módulo à direita $N \subseteq M$ tal que M/N é finitamente gerado, se $N + M\mathcal{M} = M$, então $N = M$.

Dem.: Primeiramente assumimos (i) e mostremos (ii). Suponhamos que $M \neq 0$. Então entre todos os submódulos de M (distintos de M) existe, pelo Lema de Zorn, um maximal, digamos M' , pois M é finitamente gerado.

Então M/M' é um A -módulo simples e, assim $\left(\frac{M}{M'}\right) \mathcal{M} = \{0\}$, isto é, $M\mathcal{M} = M'$. Em particular, $M\mathcal{M} \neq M$ o que mostra (ii).

Agora, assumindo que N é um A -módulo à direita contido em M tal que M/N é finitamente gerado e $N + M\mathcal{M} \cong M$, então $\frac{N+M\mathcal{M}}{N} = \frac{M}{N}$. Assim $\frac{M}{N} \cong \frac{M\mathcal{M}}{N \cap M\mathcal{M}} \cong \left(\frac{M}{N}\right) \mathcal{M}$. Logo pelo item (ii), $\frac{M}{N} = \{0\}$, ou seja $M = N$, o que mostra (iii).

Finalmente, suponhamos que $\mathcal{M}$ não esteja contido em $\text{rad } A$. Então existe $y \in \mathcal{M} - \text{rad } A$, ou seja, existe um ideal maximal à direita J de A tal que $y \notin J$. Como $y \in \mathcal{M}$ e J é maximal temos que $\mathcal{M} + J = A$, o que implica que $\mathcal{M} + AJ = A$. De (iii) segue que $\mathcal{M} = A$, o que é um absurdo, logo $\mathcal{M} \subseteq \text{rad } A$. Portanto (iii) $\Rightarrow$ (i). ■

Lema 1.1 *Se M é um A -módulo projetivo finitamente gerado, então existe um A -módulo projetivo finitamente gerado N , tal que $M \oplus N = A^n$, para algum $n \in \mathbb{N}$.*

Dem.: Desde que M é um A -módulo projetivo, temos que existe um A -módulo N_0 , tal que $M \oplus N_0 = L$, onde L é um A -módulo livre com base $\{e_i\}_{i \in I}$. Sendo M também finitamente gerado, existe um subconjunto finito J de I , tal que $M \subseteq L_o := \sum_{i \in J} e_i A$.

Assim, $L_o = M + (N_0 \cap L_o)$ e, tomando $N = N_0 \cap L_o$, temos $L_o = M \oplus N$, pois $M \cap N = \{0\}$. Claramente, $N \cong \frac{L_o}{M}$ que é finitamente gerado o que mostra o lema. ■

Observe que se A é um anel com divisão, M é um A -módulo projetivo finitamente gerado, então M é livre, pois podemos tomar n como sendo o número mínimo de geradores de M no lema acima e teremos $N = \{0\}$.

Lema 1.2 *Sejam A um anel local e $\tilde{A} = A/\mathcal{M}$ onde $\mathcal{M}$ é o único ideal maximal de A . Sejam P, Q A -módulos projetivos finitamente gerados à direita. Então $P \cong Q$*

como A -módulos se, e somente se, $\frac{P}{P\mathcal{M}} \cong \frac{Q}{Q\mathcal{M}}$ como $\tilde{A}$ -módulos.

Dem.: Se $P \cong Q$ como A -módulos então é imediato que $\frac{P}{P\mathcal{M}} \cong \frac{Q}{Q\mathcal{M}}$ como $\tilde{A}$ -módulos. Agora, seja $\bar{f}$ o isomorfismo de $\frac{P}{P\mathcal{M}}$ em $\frac{Q}{Q\mathcal{M}}$. Como P é projetivo, existe um A -homomorfismo $f : P \rightarrow Q$, que torna o seguinte diagrama comutativo:

$$\begin{array}{ccc} P & \xrightarrow{\pi_P} & \frac{P}{P\mathcal{M}} \\ f \downarrow & & \downarrow \bar{f} \\ Q & \xrightarrow{\pi_Q} & \frac{Q}{Q\mathcal{M}} \end{array}$$

ou seja, $\bar{f} \circ \pi_P = \pi_Q \circ f$ e, assim $Im(\pi_Q \circ f) = Im(\bar{f} \circ \pi_P)$. A sobrejetividade de $\bar{f}$ implica que $\pi_Q(Im f) = \bar{f}(P/P\mathcal{M}) = Im \bar{f}$. Logo $\frac{Im f}{(Q\mathcal{M}) \cap (Im f)} = Im \bar{f} = \frac{Q}{Q\mathcal{M}}$. Nessas condições, $\frac{Im f + Q\mathcal{M}}{Q\mathcal{M}} = \frac{Q}{Q\mathcal{M}}$ e, portanto $Im f + Q\mathcal{M} = Q$.

Como Q é finitamente gerado temos, pelo **Lema de Nakayama**, que $Im f = Q$, isto é, f é sobre. Mas, então pela projetividade de Q existe uma decomposição $P = Ker f \oplus Q$. Reduzindo módulo $\mathcal{M}$ temos

$$\frac{P}{P\mathcal{M}} \cong \frac{Ker f}{(Ker f)\mathcal{M}} \oplus \frac{Q}{Q\mathcal{M}}.$$

O fato de $\bar{f}$ ser um isomorfismo implica que $\frac{Ker f}{(Ker f)\mathcal{M}} = 0$, isto é, $Ker f = (Ker f)\mathcal{M}$. Como $Ker f$ é um somando direto de P , $Ker f$ é também um A -módulo projetivo finitamente gerado. Aplicando o **Lema de Nakayama** novamente, vemos que $Ker f = 0$. Isto significa que f é injetora. Consequentemente $f : P \rightarrow Q$ é um isomorfismo, como queríamos. ■

Teorema 1.2 *Todo módulo projetivo finitamente gerado sobre um anel local é livre.*

Dem.: Seja P um módulo projetivo finitamente gerado sobre um anel local A . Temos então que $P/P\mathcal{M}$ é um módulo projetivo finitamente gerado sobre $A/\mathcal{M}$, que é um anel com divisão. Consequentemente, como observamos anteriormente, $\frac{P}{P\mathcal{M}} \cong \left(\frac{A}{A\mathcal{M}}\right)^n$, para algum $n \in \mathbb{Z}$.

Portanto, pelo lema anterior $P \cong A^n$, ou seja, P é livre. ■

1.2 Anéis com involução

Para um estudo dos espaços unitários sobre um anel local necessitaremos da noção de involuções sobre um anel.

Definição 1.3 *Uma involução sobre um anel A é um anti-automorfismo σ de A de ordem ≤ 2 , ou seja $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(b)\sigma(a)$, $\sigma(1) = 1$ e $\sigma^2(a) = a$ para todo $a, b \in A$.*

Denotaremos nos capítulos seguintes uma involução σ sobre A , simplesmente por $-$.

Observemos que a aplicação identidade em A é uma involução sobre A se, e somente se o anel A é comutativo.

Sejam (A, σ_A) e (B, σ_B) anéis com involução. Um *morfismo de anéis com involução* é um homomorfismo de anéis $\phi : (A, \sigma_A) \rightarrow (B, \sigma_B)$ tal que $\sigma_B(\phi(a)) = \phi(\sigma_A(a))$, para todo $a \in A$.

Exemplos 1.2 (1) Se $(A, -)$ é um anel com involução e $I \subseteq A$ é um ideal de A tal que $\bar{I} \subseteq I$, então A/I é um anel com involução e a projeção canônica $A \rightarrow A/I$ é um morfismo de anéis com involução, onde $\overline{(a+I)} = \bar{a}+I$ é uma involução sobre A/I .

(2) A conjugação complexa no corpo dos números complexos $\mathbb{C}$ é uma involução. Observe que quando o anel é comutativo ou particularmente um corpo, uma involução

é simplesmente um automorfismo de ordem 2.

(3) Seja $M_n(A)$ o anel das matrizes $n \times n$ sobre um anel A . A aplicação que associa a cada matriz $x = (a_{ij})$ a sua transposta $x^t = (a_{ji})$ é uma involução sobre $M_n(A)$. Mais geralmente, se $(A, -)$ é um anel com involução, então a aplicação $x \rightarrow \bar{x}^t$, onde $\bar{x}^t = (\overline{a_{ji}})$ é uma involução sobre $M_n(A)$.

Seja $(A, -)$ um anel local com involução. Se $\mathcal{M}$ é o único ideal maximal à direita de A e $\tilde{A} = A/\mathcal{M}$, então a projeção canônica $A \rightarrow \tilde{A}$ é um morfismo de anéis com involução, onde $\tilde{a} = \bar{a} + \mathcal{M} = \overline{a + \mathcal{M}} = \bar{\bar{a}}$, para todo $a \in A$.

Dado um A -módulo livre à direita M , denotamos por $\tilde{M}$ o $A/\mathcal{M}$ -módulo livre $M \otimes_A A/\mathcal{M} \cong M \otimes_A \tilde{A} \cong M/M\mathcal{M}$. Veremos agora alguns resultados sobre módulos sobre um anel local que nos serão muito úteis no decorrer do trabalho.

Observação 1.1 (Levantamento de A -módulos): Sejam M_1 e M_2 A -módulos à direita livres. Se $\tilde{M} = \tilde{M}_1 \oplus \tilde{M}_2$, então $M = M_1 \oplus M_2$, pois se $x_1, \dots, x_n \in M_1$ e $y_1, \dots, y_m \in M_2$ são tais que $\{x_i \otimes \tilde{1}\}_{1 \leq i \leq n}$ é uma base de $\tilde{M}_1$ e $\{y_j \otimes \tilde{1}\}_{1 \leq j \leq m}$ é uma base de $\tilde{M}_2$, então $\{x_i \otimes \tilde{1}\}_{1 \leq i \leq n} \cup \{y_j \otimes \tilde{1}\}_{1 \leq j \leq m}$ é uma base de $\tilde{M}$ e, agora é fácil ver que $\{x_i\} \cup \{y_j\}$ é uma base de M , onde $\{x_i\}$ é uma base de M_1 e $\{y_j\}$ é uma base de M_2 .

Com o auxílio do próximo lema, em muitos casos, reduziremos o estudo dos módulos quadráticos e/ou hermitianos sobre um anel local ao estudo destes sobre um anel com divisão. Sejam A um anel local e $\mathcal{L}(A)$ a categoria dos A -módulos livres de dimensão finita (finitamente gerados).

Lema 1.3 *Seja $\sim: \mathcal{L}(A) \rightarrow \mathcal{L}(\tilde{A})$ definida por $M \mapsto \tilde{M}$, para todo $M \in \mathcal{L}(A)$. Se $N \in \mathcal{L}(A)$ e $f \in \text{Hom}_A(M, N)$ é tal que $\tilde{f} \in \text{Hom}_{\tilde{A}}(\tilde{M}, \tilde{N})$ é um isomorfismo, então f também o é.*

Dem.: Primeiramente suponhamos que $\tilde{f} : \tilde{M} \rightarrow \tilde{N}$ é injetora e mostremos que $\text{Ker } f = \{0\}$.

Se $y \in \text{Ker } f$ então $f(y) = 0$, o que implica que $\tilde{f}(\tilde{y}) = \tilde{0}$. Mas como $\tilde{f}$ é injetora, temos que $\tilde{y} = \tilde{0}$, ou seja $y \in M\mathcal{M}$. Assim $\text{Ker } f \subset M\mathcal{M}$ e, consequentemente $\text{Ker } \tilde{f} = \frac{\text{Ker } f}{(\text{Ker } f)\mathcal{M}}$.

Por hipótese $\text{Ker } \tilde{f} = \tilde{0}$, logo $(\text{Ker } f)\mathcal{M} = \text{Ker } f$ e assim, pelo **Lema de Nakayama** $\text{Ker } f = \{0\}$.

Assumamos agora $\tilde{f}$ sobrejetora, ou seja $\tilde{f}(\tilde{M}) = \tilde{N}$. Queremos mostrar então que $\frac{N}{f(M)} = 0$, ou seja, que f é sobrejetora. Note que $\tilde{N} = \frac{N}{N\mathcal{M}}$ e, consequentemente,

$$0 = \frac{\tilde{N}}{\tilde{f}(\tilde{M})} \cong \frac{\frac{N}{N\mathcal{M}}}{\frac{f(M)}{f(M)\mathcal{M}}} \cong \frac{\frac{N}{f(M)}}{\frac{N\mathcal{M}}{f(M)\mathcal{M}}} \cong \frac{\frac{N}{f(M)}}{\left(\frac{N}{f(M)}\right)\mathcal{M}}.$$

Agora o resultado segue novamente pelo **Lema de Nakayama**. ■

Proposição 1.4 *Seja $B \in M_2(A)$, onde A é um anel local com único ideal maximal à direita $\mathcal{M}$. Então se $\tilde{B} = M_2(\tilde{A})$ é inversível sobre $\tilde{A}$, então $B \in GL_2(A)$.*

Dem.: Seja $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(A)$ tal que $\tilde{B} = \begin{pmatrix} \widetilde{b_{11}} & \widetilde{b_{12}} \\ \widetilde{b_{21}} & \widetilde{b_{22}} \end{pmatrix}$ é inversível sobre $\tilde{A}$. Então existe $\tilde{C} = \begin{pmatrix} \tilde{c}_{11} & \tilde{c}_{12} \\ \tilde{c}_{21} & \tilde{c}_{22} \end{pmatrix} \in M_2(\tilde{A})$ tal que $\tilde{B}\tilde{C} = \tilde{I}_2$. Consequentemente,

$$\tilde{B}\tilde{C} \equiv \begin{pmatrix} b_{11}c_{11} + b_{12}c_{21} & b_{11}c_{12} + b_{12}c_{22} \\ b_{21}c_{11} + b_{22}c_{21} & b_{21}c_{12} + b_{22}c_{22} \end{pmatrix} \text{mod } M_2(\mathcal{M}) = \begin{pmatrix} \widetilde{d_{11}} & \widetilde{d_{12}} \\ \widetilde{d_{21}} & \widetilde{d_{22}} \end{pmatrix},$$

onde $d_{ii} \equiv 1 \pmod{\mathcal{M}}$ e $d_{ij} \equiv 0 \pmod{\mathcal{M}}$, para $i, j = 1, 2$.

Seja $E = (e_{ij}) \in M_2(A)$ tal que $e_{ij} = -d_{ii}^{-1}d_{ij}d_{jj}^{-1}$, $i \neq j$ e $e_{ii} = d_{ii}^{-1}$, $i = 1, 2$, temos

$$BCE = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \begin{pmatrix} d_{11}^{-1} & -d_{11}^{-1}d_{12}d_{22}^{-1} \\ -d_{22}^{-1}d_{21}d_{11}^{-1} & d_{22}^{-1} \end{pmatrix} = \begin{pmatrix} 1 + d_{12}e_{21} & 0 \\ 0 & 1 + d_{21}e_{12} \end{pmatrix}$$

que é inversível pois d_{12} e $d_{21} \in \mathcal{M}$ e A é um anel local.

Pelo fato de $BCE = (d_{ij})(e_{ij})$ ser inversível segue que (d_{ij}) e (e_{ij}) são inversíveis e $B^{-1} = CE$. Logo $B \in GL_2(A)$ como queríamos. ■

Capítulo 2

Espaços Hermitianos e Unitários

Neste capítulo apresentamos uma introdução ao estudo dos espaços λ -hermitianos e unitários sobre um anel local com involução, com o objetivo de obtermos “boas” bases destes espaços, o que é essencial para o estudo dos grupos ortogonal e unitário.

No que segue, neste capítulo, A denotará um anel local, não necessariamente comutativo, com elemento identidade 1 e $\bar{\cdot}: A \rightarrow A$ uma involução sobre A . A teoria das formas quadráticas e/ou hermitianas é classicamente desenvolvida sobre os A -módulos projetivos finitamente gerados, no nosso caso, devido ao **Teo.(1.2)**, todos os módulos considerados serão A -módulos à direita livres e finitamente gerados.

2.1 Espaços hermitianos sobre anéis locais com involução

A teoria das formas hermitianas sobre anéis com involução, pode ser vista como uma extensão da teoria das formas bilineares simétricas sobre corpos, pois uma forma 1-hermitiana sobre um corpo com a involução trivial (identidade) é uma forma bilinear simétrica.

Definição 2.1 *Seja M um A -módulo. Uma forma sesquilinear sobre M , é uma aplicação $b : M \times M \rightarrow A$, tal que,*

$$b(x + y, z) = b(x, z) + b(y, z)$$

$$b(x, y + z) = b(x, y) + b(x, z)$$

$$b(xa, ya') = \bar{a} b(x, y) a'$$

para todo $x, y, z \in M$ e $a, a' \in A$.

O par (M, b) é chamado um *módulo sesquilinear* sobre A . Frequentemente escrevemos b para indicar (M, b) . A forma sesquilinear b induz um homomorfismo de A -módulos $h_b : M \rightarrow M^* = \text{Hom}_A(M, A)$, por $h_b(x)(y) = b(x, y)$, para todo $x, y \in M$. Observe que se M é um A -módulo livre à direita, então, como observado no capítulo 1, M^* também o é, com a multiplicação por escalar $f.a = \bar{a}f$, para todo $f \in M^*$ e $a \in A$.

Reciprocamente, dado um homomorfismo de A -módulos $h : M \rightarrow M^*$, definimos uma forma sesquilinear $b_h : M \times M \rightarrow A$, por $b_h(x, y) = h(x)(y)$, para todo $x, y \in M$.

A aplicação h_b associada à forma sesquilinear b é chamada a *adjunta de b* . O módulo sesquilinear (M, b) é dito ser *não-singular*, ou simplesmente um *espaço sesquilinear* sobre A , se a sua adjunta h_b é um isomorfismo de A -módulos. Como $b_{h_b} = b$ e $h_{b_h} = h$, a forma sesquilinear é determinada pela sua adjunta e vice-versa.

Definição 2.2 *Sejam (M_i, b_i) , $i = 1, 2$, módulos sesquilineares sobre A . Definimos a soma ortogonal dos módulos (M_1, b_1) e (M_2, b_2) , a qual denotamos por $(M_1, b_1) \perp (M_2, b_2)$, como sendo o módulo sesquilinear $(M_1 \oplus M_2, b_1 \perp b_2)$ onde*

$$b_1 \perp b_2(x_1 + x_2, y_1 + y_2) = b_1(x_1, y_1) + b_2(x_2, y_2),$$

para todo $x_i, y_i \in M_i, i = 1, 2$.

Consideremos o conjunto $\text{Sesq}_A(M) = \{b : M \times M \rightarrow A; b \text{ é sesquilinear}\}$. É fácil ver que $\text{Sesq}_A(M)$ é um grupo abeliano com a adição definida por: $(b, b') \mapsto (b + b')$, com

$$(b + b')(x, y) = b(x, y) + b'(x, y),$$

para todo $x, y \in M$, onde o elemento neutro é $b = 0$ e o oposto de b é $-b$, para todo $b \in \text{Sesq}_A(M)$.

Definição 2.3 *Sejam $b_1 \in \text{Sesq}_A(M_1)$ e $b_2 \in \text{Sesq}_A(M_2)$, M_1 e M_2 A -módulos. Dizemos que $\varphi \in \text{Hom}_A(M_1, M_2)$ é um morfismo de módulos sesquilineares se $b_2(\varphi(x), \varphi(y)) = b_1(x, y)$, para todo $x, y \in M_1$. Se, além disso, φ é um isomorfismo de A -módulos, dizemos que φ é uma isometria ou que os módulos sesquilineares (M_1, b_1) e (M_2, b_2) são isométricos e, neste caso, denotamos por $(M_1, b_1) \simeq (M_2, b_2)$, ou simplesmente por $b_1 \simeq b_2$.*

Dada uma forma sesquilinear b sobre M , definimos $\bar{b} : M \times M \rightarrow A$ por $\bar{b}(x, y) = \overline{b(y, x)}$, para todo $x, y \in M$. É fácil ver que $\bar{b} \in \text{Sesq}_A(M)$. Mais ainda, a aplicação $b \mapsto \bar{b}$ é um automorfismo de ordem ≤ 2 do grupo aditivo $\text{Sesq}_A(M)$ e satisfaz $\xi \bar{b} = \bar{\xi} \bar{b}$, para todo $\xi \in Z(A)$ (o centro de A). A adjunta de $\bar{b}$ é $h_{\bar{b}} = \overline{h_b}$ pois $h_{\bar{b}}(x)(y) = \bar{b}(x, y) = \overline{b(y, x)} = \overline{h_b(y)(x)} = \overline{h_b(x)(y)}$, para todo $x, y \in M$.

Considere o conjunto $G(Z) = \{\lambda \in Z(A); \lambda \bar{\lambda} = 1\}$, o qual é um subgrupo multiplicativo de A^* , o grupo das unidades de A .

Definição 2.4 *Seja $\lambda \in G(Z)$. Dizemos que uma forma $b \in \text{Sesq}_A(M)$ é λ -hermitiana se $b = \lambda \bar{b}$, ou seja, se $b(x, y) = \lambda \overline{b(y, x)}$, para todo $x, y \in M$. Neste caso dizemos que (M, b) é um módulo λ -hermitiano sobre A .*

Como a adjunta de $\bar{b}$ é $\overline{h_b}$, temos que uma forma b é λ -hermitiana se, e somente se, sua adjunta satisfaz $h_b = \lambda \overline{h_b}$. De fato, se b é λ -hermitiana, então $h_b(x)(y) = b(x, y) = \lambda \overline{b(y, x)} = \lambda \bar{b}(x, y) = \lambda h_{\bar{b}}(x)(y) = \lambda \overline{h_b(x)(y)}$, para todo $x, y \in M$, ou seja, $h_b = \lambda \overline{h_b}$. Por outro lado, se $h_b = \lambda \overline{h_b}$ então, para todo $x, y \in M$, temos que $b(x, y) = h_b(x)(y) = \lambda \overline{h_b(x)(y)} = \lambda h_{\bar{b}}(x)(y) = \lambda \bar{b}(x, y)$.

Se (M, b) é um módulo λ -hermitiano sobre A com h_b um isomorfismo de A -módulos, então diremos que (M, b) é um espaço λ -hermitiano.

Formas 1-hermitianas são classicamente chamadas *formas hermitianas* e formas (-1) -hermitianas são chamadas *formas quase-hermitianas*.

Se a involução de A é trivial (identidade), ou seja, A é comutativo, as formas hermitianas são as formas bilineares simétricas e as formas quase-hermitianas, são as formas bilineares anti-simétricas sobre anéis comutativos. No que segue, sempre que estivermos assumindo A comutativo, com a involução trivial e $\lambda = 1$, usaremos simplesmente a expressão “no caso comutativo”.

Consideremos agora, o conjunto das formas λ -hermitianas sobre M :

$$\mathcal{H}_\lambda(M) = \{k \in \text{Sesq}_A(M); k - \lambda \bar{k} = 0\} \subset \text{Sesq}_A(M).$$

É fácil ver que $\mathcal{H}_\lambda(M)$ é um subgrupo de $\text{Sesq}_A(M)$.

Definição 2.5 *Seja $b \in \mathcal{H}_\lambda(M)$. Dizemos que b é uma forma λ -hermitiana par se, e somente se, $b = k + \lambda \bar{k}$ para algum $k \in \text{Sesq}_A(M)$. Neste caso, diremos que (M, b) é um módulo λ -hermitiano par. O subconjunto das formas λ -hermitianas pares sobre M , será denotado por $\mathcal{H}_\lambda^p(M)$, ou seja*

$$\mathcal{H}_\lambda^p(M) = \{b \in \text{Sesq}_A(M); b = k + \lambda \bar{k}, \text{ para algum } k \in \text{Sesq}_A(M)\}.$$

Dado $k \in \text{Sesq}_A(M)$, temos que $k + \lambda \bar{k} \in \mathcal{H}_\lambda(M)$ pois, $(k + \lambda \bar{k}) - \lambda \overline{(k + \lambda \bar{k})} = k + \lambda \bar{k} - \lambda(\bar{k} + \lambda \bar{\bar{k}}) = k - \lambda \bar{k} = 0$. Denotaremos por $\langle, \rangle_k$ a forma λ -hermitiana par associada a forma sesquilinear k , ou seja, $\langle x, y \rangle_k = k(x, y) + \lambda \overline{k(y, x)}$, para todo $x, y \in M$. O índice k em $\langle, \rangle_k$ será suprimido quando estiver claro qual é a forma sesquilinear k em questão. Quando (M, b) é um módulo λ -hermitiano par, usaremos também a notação $(M, \langle, \rangle_k)$, onde $\langle, \rangle_k = k + \lambda \bar{k}$.

Observação 2.1 Se 2 é inversível em A , então toda forma λ -hermitiana sobre A é par, pois se $b \in \mathcal{H}_\lambda(M)$, então $b = \lambda \bar{b}$ e assim, $\frac{b + \lambda \bar{b}}{2} = \frac{b + b}{2} = b$. Logo, $b = \langle, \rangle_k$ com $k = \frac{b}{2} \in \text{Sesq}_A(M)$.

Seja $M_{n,k}(A)$ o conjunto das matrizes $(n \times k)$ com entradas em A . Para $\alpha = (a_{ij}) \in M_{n,k}(A)$ denotamos por $\bar{\alpha}^t$ a matriz $(k \times n)$, $(\overline{a_{ij}})^t$, onde t denota a transposta e $\overline{a_{ij}}$ é a involução de A aplicada no elemento $a_{ij} \in A$.

Seja $\{e_1, e_2, \dots, e_n\}$ uma base de M sobre A . É fácil ver que a aplicação $Sesq_A(M) \rightarrow M_n(A)$, tal que $b \mapsto (b_{ij})$, com $b_{ij} = b(e_i, e_j)$, $1 \leq i, j \leq n$, é um isomorfismo de $Z(A)$ -módulos. Assim, a forma b é unicamente determinada pela matriz (b_{ij}) , pois se $x = \sum_{i=1}^n x_i e_i$, $x_i \in A$ e, $y = \sum_{i=1}^n y_i e_i$, $y_i \in A$, são elementos

de M então, escrevendo as coordenadas de x e y como vetores colunas $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

e $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, temos que $b(x, y) = \sum_{i,j=1}^n \bar{x}_i b_{ij} y_j = \bar{x}^t (b_{ij}) y$. Mais ainda, a matriz

da forma $\bar{b}$ com relação a base $\{e_1, e_2, \dots, e_n\}$, é $(\bar{b}_{ij})^t$. No caso comutativo temos $b(x, y) = x^t (b_{ij}) y$ com $b_{ij} = \lambda \bar{b}_{ji} = b_{ji}$, ou seja, (b_{ij}) é simétrica.

Se $\{f_1, f_2, \dots, f_n\}$, $f_i \in M^*$, é a base dual de $\{e_1, e_2, \dots, e_n\}$, isto é,

$$f_j(e_i) = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j, \end{cases}$$

então a adjunta $h_b: M \rightarrow M^*$ de b é dada por $h_b(e_i) = \sum_j f_j \cdot \bar{b}_{ij} = \sum_j b_{ij} f_j$, onde $b_{ij} = b(e_i, e_j)$, pois $h_b(e_i)(e_k) = b(e_i, e_k) = b_{ik} = \sum_j b_{ij} f_j(e_k) = \sum_j f_j \cdot \bar{b}_{ij}(e_k)$.

Uma matriz (b_{ij}) é a matriz de uma forma λ -hermitiana par se, e somente se, $b_{ii} = a_i + \lambda \bar{a}_i$, $a_i \in A$ para $i = 1, \dots, n$, e $b_{ij} = \lambda \bar{b}_{ji}$ para $i \neq j$, onde $b_{ij} = k_{ij} + \lambda \bar{k}_{ji}$, para algum $k \in Sesq_A(M)$, onde $k_{ij} = k(e_i, e_j)$ pois $b = k + \lambda \bar{k}$. Nestas condições, $b(e_i, e_j) = \lambda \overline{b(e_j, e_i)}$, $i \neq j$ e $b(e_i, e_i) = k(e_i, e_i) + \lambda \overline{k(e_i, e_i)} = a_i + \lambda \bar{a}_i$, $a_i \in A$. Por outro lado, podemos escrever $b_{ij} = k_{ij} + \lambda \bar{k}_{ji}$, $i, j = 1, \dots, n$ com $k_{ii} = a_i$, $k_{ij} = b_{ij}$ para $i < j$ e $k_{ij} = 0$ para $i > j$, e portanto a forma b é dada pela soma das matrizes

$$\begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ 0 & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & k_{nn} \end{pmatrix} + \lambda \begin{pmatrix} \bar{k}_{11} & \bar{k}_{12} & \dots & \bar{k}_{1n} \\ 0 & \bar{k}_{22} & \dots & \bar{k}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \bar{k}_{nn} \end{pmatrix},$$

ou seja, $(b_{ij}) = (k_{ij}) + \lambda (\bar{k}_{ij})$.

Proposição 2.1 *Seja (M, b) um módulo λ -hermitiano sobre A . Então (M, b) é par se, e somente se, $b(x, x) \in S_\lambda(A) := \{S_\lambda(a) = a + \lambda\bar{a}; a \in A\}$, para todo $x \in M$.*

Dem.: Se b é par, então $b(x, x) = k(x, x) + \lambda\overline{k(x, x)} = S_\lambda(k(x, x))$, para algum $k \in \text{Sesq}_A(M)$. Portanto, $b(x, x) \in S_\lambda(A)$. Agora, se $b(x, x) \in S_\lambda(A)$, então $b(x, x) = a + \lambda\bar{a}$, para algum $a \in A$. Em particular, se $\{e_1, \dots, e_n\}$ é uma base de M sobre A , então $b(e_i, e_i) = a_i + \lambda\bar{a}_i$ e, como $b_{ij} = \lambda\bar{b}_{ji}$ para $i \neq j$, temos que (M, b) é par. ■

Seja (M, b) um módulo λ -hermitiano sobre A . Dizemos que a forma b é *não-singular*, ou simplesmente, (M, b) é um *espaço λ -hermitiano* sobre A se a adjunta $h_b : M \rightarrow M^*$ é um isomorfismo. Os módulos λ -hermitianos pares com b não-singular são denominados *espaços λ -hermitianos pares*.

Seja $\phi : M_1 \oplus M_2 \rightarrow N_1 \oplus N_2$, um homomorfismo de A -módulos. Podemos escrever ϕ convenientemente na forma de blocos de matrizes, $\phi = \begin{pmatrix} \phi_{11} & \phi_{12} \\ \phi_{21} & \phi_{22} \end{pmatrix}$, onde $\phi_{ij} \in \text{Hom}_A(M_i, N_j)$, para $i, j = 1, 2$.

O próximo lema nos ajuda a determinar quando um módulo λ -hermitiano é não-singular.

Lema 2.1 *Seja $\varphi \in \text{Hom}(M_1 \oplus M_2, N_1 \oplus N_2)$, onde $M_i, N_i, i = 1, 2$ são A -módulos à direita livres de dimensão finita sobre A . A matriz de φ é $\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix}$, $\varphi_{ij} \in \text{Hom}_A(M_i, N_j)$. Então:*

- (i) *Se φ e φ_{11} são isomorfismos, então φ_{22} é um isomorfismo.*
- (ii) *Assumimos que $\varphi_{21} = 0$ ou $\varphi_{12} = 0$. Se duas das três aplicações φ , φ_{11} , φ_{22} são isomorfismos, a outra também o é.*
- (iii) *Se $\varphi_{12} = 0$ e $\varphi_{21} = 0$, então φ é um isomorfismo se, e somente se, φ_{11} e φ_{22} são isomorfismos.*

(iv) Se $\varphi_{11} = 0$ ou $\varphi_{22} = 0$. Então φ é um isomorfismo se, e somente se, φ_{12} e φ_{21} são isomorfismos.

Dem.: (i) Se (σ_{ij}) é a matriz de φ^{-1} , então $\sigma_{22} : N_2 \rightarrow M_2$ é um isomorfismo com inversa $\varphi_{22} - \varphi_{21}\varphi_{11}^{-1}\varphi_{12}$.

(ii) Assumindo que φ e φ_{11} são isomorfismos, então do item anterior temos que φ_{22} é um isomorfismo. Os outros casos são similares.

(iii) A inversa de φ é dada pela matriz $\begin{pmatrix} \varphi_{11}^{-1} & 0 \\ 0 & \varphi_{22}^{-1} \end{pmatrix}$.

(iv) Se $\varphi_{11} = 0$ a inversa de φ é dada pela matriz $\begin{pmatrix} -\varphi_{21}^{-1}\varphi_{22}\varphi_{12}^{-1} & \varphi_{21}^{-1} \\ \varphi_{12}^{-1} & 0 \end{pmatrix}$. Se $\varphi_{22} = 0$, mostra-se de maneira análoga. ■

No caso comutativo, o seguinte lema determina quando um módulo bilinear é não-singular :

Lema 2.2 *Seja (M, b) um módulo bilinear sobre um anel comutativo A com 1. São equivalentes:*

(i) b é não-singular.

(ii) $\det(b_{ij}) \in A^*$, onde (b_{ij}) é a matriz da forma b com relação a uma base $\{e_1, e_2, \dots, e_n\}$ de M sobre A .

(iii) Se $b(x, y) = 0$, para todo $y \in M$, então $x = 0$.

Dem.: Se b é não-singular, então sua adjunta h_b é um isomorfismo e, em particular, h_b é injetor, logo $\text{Ker}(h_b) = \{0\}$, ou seja, $h_b(x) = 0$ implica $x = 0$. Mas, $h_b(x)(y) = b(x, y)$ para todo $y \in M$, o que mostra (i) $\Rightarrow$ (iii).

Reciprocamente, se $b(x, y) = 0$, para todo $y \in M$ implica $x = 0$, então temos que h_b é injetor. Como h_b é uma aplicação A -linear e $\dim_A M = \dim_A M^*$, temos que h_b é um isomorfismo, isto é, vale (iii) $\Rightarrow$ (i).

Para mostrarmos (i) $\Leftrightarrow$ (ii), observamos que h_b é um isomorfismo se, e somente se (b_{ij}) é uma matriz inversível e, como A é comutativo, é suficiente mostrarmos que $(b_{ij}) \in M_n(A)$ é inversível se, e somente se $\det(b_{ij}) \in A^*$. Para tanto, se (b_{ij}) é inversível, então existe $(c_{ij}) \in M_n(A)$ tal que $(b_{ij})(c_{ij}) = I_n$ (a matriz identidade $n \times n$). Aplicando determinante temos que $\det(b_{ij}) \in A^*$. Reciprocamente, se $\det(b_{ij}) \in A^*$, então $(b_{ij})^{-1} = (\det(b_{ij}))^{-1} \cdot (\text{adj}(b_{ij}))$ (a matriz adjunta de (b_{ij})), ou seja, (b_{ij}) é inversível. ■

Se $(M_i, b_i), i = 1, 2$ são módulos λ -hermitianos sobre A , então $(M_1 \oplus M_2, b_1 \perp b_2)$ também é λ -hermitiano pois $(b_1 \perp b_2)(x_1 + x_2, y_1 + y_2) = b_1(x_1, y_1) + b_2(x_2, y_2) = \lambda \overline{b_1(y_1, x_1)} + \lambda \overline{b_2(y_2, x_2)} = \lambda \overline{(b_1 \perp b_2)(y_1 + y_2, x_1 + x_2)}$, para todo $x_i, y_i \in M_i, i = 1, 2$. Mais ainda, desde que a adjunta de $(b_1 \perp b_2)$ é $h_{b_1 \perp b_2} = h_{b_1} \perp h_{b_2}$, temos que a matriz de $h_{b_1} \perp h_{b_2}$ é $\begin{pmatrix} h_{b_1} & 0 \\ 0 & h_{b_2} \end{pmatrix}$ e, do **Lema(2.1)** obtemos que $b_1 \perp b_2$ é não-singular se, e somente se b_1 e b_2 o são. Ou seja, a soma ortogonal de espaços λ -hermitianos é um espaço λ -hermitiano.

Além disso, se b_1 e b_2 são formas λ -hermitianas pares, então $b_i = k_i + \lambda \overline{k_i}$ para algum $k_i \in \text{Sesq}_A(M_i), i = 1, 2$ e $(b_1 \perp b_2)(x_1 + x_2, y_1 + y_2) = [(k_1 + \lambda \overline{k_1}) \perp (k_2 + \lambda \overline{k_2})](x_1 + x_2, y_1 + y_2) = ((k_1 \perp k_2) + \lambda \overline{(k_1 \perp k_2)})(x_1 + x_2, y_1 + y_2)$, onde $(k_1 \perp k_2) \in \text{Sesq}_A(M_1 \oplus M_2)$, pois $\text{Sesq}_A(M_1) \oplus \text{Sesq}_A(M_2) \subseteq \text{Sesq}_A(M_1 \oplus M_2)$. Consequentemente, $b_1 \perp b_2$ também é uma forma λ -hermitiana par.

Seja (M, b) um módulo λ -hermitiano sobre A . Para um submódulo $U \subset M$ denotamos a restrição de b a U por $b|_U$ e a adjunta de $b|_U$ por $h|_U$. Claramente, se b é par, então $b|_U$ também o é. Para $x \in M$, denotaremos por $b(x, U)$ o subconjunto $\{b(x, u); u \in U\}$ de A .

Lema 2.3 *Seja (M, b) um espaço λ -hermitiano sobre A . Se U e V são submódulos de M tais que $M = U + V$ e $b(U, V) = 0$, então $(U, b|_U)$ e $(V, b|_V)$ são espaços λ -hermitianos e $(M, b) = (U, b|_U) \perp (V, b|_V)$.*

Dem.: Se $x \in U \cap V$, então $b(x, U) = b(x, V) = 0$, pois $b(U, V) = 0$. Assim, $b(x, M) = 0$ e, como b é não-singular, temos que $x = 0$. Isto mostra que $U \cap V = \{0\}$ e, consequentemente $M = U \oplus V$.

Seja $h = (h_{ij}) : U \oplus V \rightarrow (U \oplus V)^* \cong (U^* \oplus V^*)$, $i, j = 1, 2$, a adjunta de b . A aplicação $h_{21} : V \rightarrow U^*$ é dada por $v \mapsto b(v, \cdot)|_U$. Como $b(V, U) = 0$, temos que $h_{21} = 0$. Desde que b é λ -hermitiana temos $h_{12} = \lambda \overline{h_{21}}$ e, consequentemente $h_{12} = 0$.

Assim, $h = \begin{pmatrix} h_{11} & 0 \\ 0 & h_{22} \end{pmatrix}$ e, do **Lema(2.1)**, temos a decomposição ortogonal requerida. ■

Dois elementos x, y de um módulo λ -hermitiano (M, b) são ditos serem *ortogonais* se $b(x, y) = 0$. Analogamente, dizemos que dois subconjuntos $X \subset M$ e $Y \subset M$ de um módulo λ -hermitiano (M, b) são *ortogonais* se $b(x, y) = 0$, para todo $x \in X$ e $y \in Y$. Para um submódulo $U \subset M$ definimos o *complemento ortogonal* de U como sendo o submódulo $U^\perp$ de M , dado por:

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

Lema 2.4 *Sejam (M, b) um módulo λ -hermitiano sobre A e U, V submódulos de M . Então:*

- (i) *Se $U \subseteq V \subseteq M$, então $V^\perp \subseteq U^\perp$.*
- (ii) *$U \subseteq V^{\perp\perp}$.*
- (iii) *$V^\perp = V^{\perp\perp\perp}$.*

Dem.: Se $x \in V^\perp$, então $b(x, y) = 0$ para todo $y \in V$. Como $U \subseteq V$, em particular, $b(x, y) = 0$ para todo $y \in U$, ou seja, $x \in U^\perp$, o que mostra (i).

Agora, se $x \in V$ então $b(x, y) = 0$ para todo $y \in V^\perp$ e, consequentemente $x \in V^{\perp\perp}$, ou seja, (ii) é verdadeira.

O item (iii) segue de (i) e (ii). ■

Lema 2.5 *Seja (M, b) um módulo λ -hermitiano sobre A . Então:*

- (i) *Se U é um submódulo de M tal que $(U, b|_U)$ é não-singular, então $(M, b) = (U, b|_U) \perp (U^\perp, b|_{U^\perp})$.*
- (ii) *Se $(M, b) \simeq (M_1, b_1) \perp (M_2, b_2)$ para módulos λ -hermitianos (M_i, b_i) , $i = 1, 2$, então b_1 e b_2 são não-singulares se, e somente se b é não-singular.*

Dem.: (i) Como $b|_U$ é não-singular, temos que $U \cap U^\perp = \{0\}$ e, pelo **Lema(2.3)** é suficiente mostrarmos que $M = U + U^\perp$. Observe que dado $m \in M$, a aplicação $h(m) = b(m, \cdot)$ é um elemento de M^* e, consequentemente a sua restrição $h(m)|_U \in U^*$. Como $h|_U = h_b|_U$ é um isomorfismo, existe $u \in U$ tal que $b(m, \cdot)|_U = b(u, \cdot)|_U$. Isto mostra que $b(m - u, \cdot)$ é zero em U , ou seja $m - u \in U^\perp$. Portanto, $m = u + (m - u) \in U + U^\perp$, como queríamos.

(ii) É consequência imediata do **Lema(2.1)**. ■

Os lemas anteriores são claramente válidos para módulos λ -hermitianos pares.

Um elemento x de um módulo λ -hermitiano (M, b) é dito ser um *vetor isotrópico* de (M, b) se $b(x, x) = 0$. Dizemos que um módulo λ -hermitiano (M, b) é *isotrópico* se ele contém um vetor isotrópico não nulo, caso contrário, dizemos que (M, b) é *anisotrópico*. Um submódulo U de (M, b) é dito ser *totalmente isotrópico* se $b|_U = 0$, ou equivalentemente, se $U \subseteq U^\perp$. Observe que um elemento x de um módulo λ -hermitiano par $(M, \langle, \rangle_k)$ é *isotrópico* se $k(x, x) \in S^{-\lambda}(A) := \{a \in A; a = -\lambda \bar{a}\}$.

Um espaço λ -hermitiano (M, b) que contém um submódulo U totalmente isotrópico com $U^\perp = U$, é dito ser um *espaço metabólico*. Neste caso, $M = U \oplus V$ para algum submódulo V e, consequentemente, a matriz da adjunta h_b é da forma
$$\begin{pmatrix} 0 & h_{12} \\ \lambda \overline{h_{12}} & h_{22} \end{pmatrix}.$$
 Como b é não-singular, do **Lema(2.1)**, temos que $h_{12} : V \rightarrow U^*$ é um isomorfismo. Identificando V com U^* via h_{12} , temos que $(M, b) \simeq \left(M, \begin{pmatrix} 0 & 1 \\ \lambda & \overline{h_k} \end{pmatrix} \right)$ para alguma

forma λ -hermitiana $k : V \times V \rightarrow A$, pois

$$\begin{pmatrix} 1 & 0 \\ 1 & \overline{h_{12}^{-1}} \end{pmatrix} \begin{pmatrix} 0 & h_{12} \\ \lambda \overline{h_{12}} & h_{22} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & h_{12}^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \lambda & * \end{pmatrix}$$

onde $* = \lambda + 1 + \overline{h_{12}^{-1}} h_{22} h_{12}^{-1}$ é uma forma λ -hermitiana.

Se na matriz que representa um espaço λ -hermitiano metabólico $\begin{pmatrix} 0 & 1 \\ \lambda & \overline{h_k} \end{pmatrix}$, a forma λ -hermitiana k é par, então (M, b) é um espaço λ -hermitiano par metabólico.

Dado um A -módulo M , consideremos a forma λ -hermitiana

$$b : (M \oplus M^*) \times (M \oplus M^*) \rightarrow A,$$

definida por $b(x_1 + f_1, x_2 + f_2) = f_1(x_2) + \lambda \overline{f_2(x_1)}$, onde $x_i \in M$ e $f_i \in M^*$. A matriz da aplicação adjunta h_b é $\begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}$ que é claramente inversível. Logo $\text{IH}(M) = (M \oplus M^*, b)$ define um espaço λ -hermitiano, chamado de *espaço hiperbólico*.

Observe que em $\text{IH}(M)$, os submódulos M e M^* são totalmente isotrópicos, ou seja, todo espaço hiperbólico é também metabólico. Mas, em geral, um espaço λ -hermitiano metabólico não é necessariamente hiperbólico.

Por exemplo, o espaço bilinear simétrico $\left(K^2, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right)$ sobre um corpo K de característica 2 é metabólico mas não é hiperbólico, pois caso contrário teríamos $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ o que não é verdade, pois $(x \ y) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2xy = 0$ e $(x \ y) \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2xy + y^2 = y^2$, para todo $x, y \in K$.

O espaço λ -hermitiano hiperbólico $\text{IH}(M)$ descrito pela matriz $\begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}$ é também um espaço λ -hermitiano par, pois $b = k + \lambda \overline{k}$, para $k = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \text{Sesq}_A(M)$.

Se $M = xA$, então $M \oplus M^* = xA \oplus yA$, com $b(x, x) = 0$. Assim, $b(x, y) = 1$, $b(y, x) = \lambda$, $b(y, y) = 0$, ou seja, $\mathbb{H}(xA) = \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}$. A este espaço hiperbólico damos o nome de *plano hiperbólico* e denotamos apenas por $\mathbb{H}$. Mais ainda, dizemos que x e y satisfazendo as condições acima, formam um *par hiperbólico*.

A próxima proposição mostra que todo espaço λ -hermitiano par isotrópico contém um plano hiperbólico.

Proposição 2.2 *Seja (M, b) um espaço λ -hermitiano par sobre A . Seja $x \in M$ um elemento unimodular, isto é, uma base de um somando direto livre de M , que é isotrópico. Então existe $y \in M$ tal que x e y formam um par hiperbólico.*

Dem.: Como x é unimodular e isotrópico, então $b(x, M) = A$ e $b(x, x) = 0$. Desde que b é não-singular, existe um $z \in M$ tal que $b(x, z) = 1$.

Se $N = xA \oplus zA$, então a matriz de $b|_N$ é $\begin{pmatrix} 0 & 1 \\ \lambda & b(z, z) \end{pmatrix}$ que é não-singular, ou seja, $(N, b|_N)$ é um subespaço de (M, b) .

Se $b(z, z) = 0$, então z é o vetor isotrópico procurado. Caso contrário, desde que $b = k + \lambda \bar{k}$, para algum $k \in \text{Sesq}_A(M)$, temos que $k(z, z) + \lambda \overline{k(z, z)} \neq 0$ e, consequentemente $\alpha = \overline{-k(z, z)} \neq 0$. Agora o vetor $y = x\alpha + z \in N$ é tal que $b(y, y) = 0$ e $b(x, y) = 1$. Mais ainda, $\{x, y\}$ é uma base de N pois a matriz mudança da base $\{x, z\}$ para $\{x, y\}$ é $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ que é claramente inversível. Portanto x e y é o par hiperbólico procurado. ■

Essa proposição não contradiz o exemplo dado anteriormente, porque $\left(K^2, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right)$ não é par.

2.2 Decomposição de módulos λ -hermitianos sobre anéis locais

Neste parágrafo, mostraremos que todo espaço λ -hermitiano par sobre um anel local é uma soma ortogonal de subespaços de dimensão ≤ 2 . Primeiramente, mostraremos que um espaço λ -hermitiano (M, b) sobre um anel com divisão D pode ser decomposto em uma soma ortogonal de um espaço anisotrópico e um espaço metabólico, ou seja, o teorema da decomposição de Witt para espaços λ -hermitianos sobre um anel com divisão.

Proposição 2.3 *Seja (M, b) um espaço λ -hermitiano sobre um anel com divisão D . Então existe uma decomposição ortogonal*

$$(M, b) \simeq (M', b') \perp \left(D^2, \begin{pmatrix} 0 & 1 \\ \lambda & d_1 \end{pmatrix} \right) \perp \dots \perp \left(D^2, \begin{pmatrix} 0 & 1 \\ \lambda & d_r \end{pmatrix} \right),$$

com (M', b') anisotrópico e $d_i \in D$, $1 \leq i \leq r$.

Dem.: Se (M, b) é anisotrópico, ou seja, se para todo $x \in M$, $b(x, x) = 0$ implica $x = 0$, então $(M, b) = (M', b')$ que é anisotrópico. Se existe um elemento isotrópico $x_1 \neq 0$ em M , então como b é não singular, existe $y'_1 \in M$ tal que $b(x_1, y'_1) \in A^*$. Fazendo uma mudança de coordenadas temos que existe $y_1 \in M$ tal que $b(x_1, y_1) = 1$.

A restrição de b ao plano $N = x_1 D + y_1 D$ com respeito a base $\{x_1, y_1\}$ é um espaço metabólico, pois sua matriz é $\begin{pmatrix} 0 & 1 \\ \lambda & d_1 \end{pmatrix}$, onde $d_1 = b(y_1, y_1) \in D$. Do **Lema(2.3)** temos que $b|_N$ é não singular. E, assim pelo **Lema(2.5)(i)** temos uma decomposição $(M, b) \simeq (N, b|_N) \perp (N^\perp, b|_{N^\perp})$. Agora a demonstração segue por indução sobre a $\dim_A(M)$. ■

Dizemos que um módulo λ -hermitiano (M, b) sobre A é *diagonalizável* se M é livre com uma base $\{e_1, \dots, e_n\}$ tal que a matriz de b com respeito a essa base é

diagonal. Neste caso, uma tal base é dita ser uma *base ortogonal* de (M, b) .

Denotamos o módulo λ -hermitiano (A^n, b) , onde a matriz de b com respeito a base canônica de A^n é a matriz diagonal

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix},$$

por $\langle a_1, \dots, a_n \rangle$. Assim, (M, b) é um espaço λ -hermitiano diagonalizável se, e somente se, $(M, b) \simeq \langle a_1, \dots, a_n \rangle$, para alguns $a_1, \dots, a_n \in A^*$ tais que $a_i = \lambda \bar{a}_i$, $i = 1, \dots, n$.

Lema 2.6 *Todo espaço λ -hermitiano anisotrópico (M, b) sobre um anel com divisão D é diagonalizável.*

Dem.: Desde que (M, b) é anisotrópico, temos que para $x \in M$, $x \neq 0$, a forma $b|_{xD}$ é não-singular, ou seja, $b(x, x) \in D^*$. Assim, do **Lema(2.5)(i)**, temos uma decomposição ortogonal da forma $(M, b) \simeq (xD, b|_{xD}) \perp (M_1, b_1)$ onde $M_1 = (xD)^\perp$ e $b_1 = b|_{(xD)^\perp}$.

Como (M, b) é anisotrópico então (M_1, b_1) também o é, e o lema segue por indução sobre a $\dim_A(M)$. ■

Assim, combinando a **Prop.(2.3)** e o **Lema(2.6)**, temos:

Corolário 2.1 *Todo espaço λ -hermitiano (M, b) sobre um anel com divisão D é isométrico a uma decomposição ortogonal $\perp_{i=1}^n (M_i, b_i)$ com $\dim_D(M_i) \leq 2$.*

Da definição de base ortogonal, vemos claramente que espaços λ -hermitianos sobre anéis com divisão tais que todos seus elementos são isotrópicos não podem ter base ortogonal. Tais espaços ocorrem somente em casos muito especiais.

Lema 2.7 *Seja (M, b) um espaço λ -hermitiano sobre um anel com divisão D tal que todos os seus elementos são isotrópicos. Então $\lambda = \pm 1$, a involução sobre D é trivial (consequentemente D é comutativo) e b é anti-simétrica. Em particular, a dimensão de M é par e, se $\lambda = 1$, então D tem característica 2.*

Dem.: Assumimos que a involução sobre D é não trivial e, seja $d_1 \in D$ tal que $\overline{d_1} \neq d_1$. Temos que $\overline{d} = -d$ para $d = d_1 - \overline{d_1}$. Desde que b é não-singular podemos escolher $x, y \in M$ tais que $b(x, y) = d$, para cada $d \neq 0$ de D . Como todos os elementos de (M, b) são isotrópicos então $0 = b(x+y, x+y) - b(x, x) - b(y, y) = b(x, y) + b(y, x) = b(x, y) + \lambda \overline{b(x, y)} = d + \lambda \overline{d}$.

Assim $d + \lambda \overline{d} = 0$, para todo $d \in D^*$. Tomando $d = d_1 - \overline{d_1}$ citado acima, temos $d - \lambda d = 0$, ou seja $d(1 - \lambda) = 0$ e, consequentemente, $\lambda = 1$. Portanto, se $\lambda \neq 1$ temos que a involução sobre D é trivial.

Se a involução sobre D é trivial, temos $\lambda^2 = 1$, desde que $\lambda \overline{\lambda} = 1$. Portanto $\lambda = \pm 1$. Assim mostramos que se todo elemento de (M, b) é isotrópico, então $\lambda = \pm 1$.

Se $\lambda = -1$, então pelo que foi feito acima, a involução sobre D é trivial, ou seja, D é comutativo e b é anti-simétrica.

Se $\lambda = 1$, desde que (M, b) é não-singular, existe $x, y \in M$ tais que $b(x, y) = 1$. Assim $0 = b(x+y, x+y) - b(x, x) - b(y, y) = 1 + \lambda$. Ou seja, $2 = 0$ em D . Para todo $d \in D$, escolhemos $x, y \in M$ tais que $b(x, y) = d$ e, obtemos que $0 = d + \lambda \overline{d} = d + \overline{d}$. Logo para todo $d \in D$, temos $\overline{d} = -d = d$ pois $\text{car}(D) = 2$, ou seja, a involução sobre D é trivial. ■

Teorema 2.1 *Seja (M, b) um espaço λ -hermitiano sobre um anel com divisão D . Então (M, b) tem uma base ortogonal se, e somente se:*

- (i) *a involução sobre D é não trivial, ou*
- (ii) *a involução sobre D é trivial, a forma b é simétrica, isto é, $\lambda = 1$ e $\text{car}(D) \neq 2$.*

Dem.: Usando o **Cor.(2.1)**, podemos supor que $\dim_D(M) \leq 2$. Inicialmente, assumimos que (M, b) admite uma base ortogonal. Neste caso, $b = \langle a_1 \rangle$ ou $b = \langle a_1, a_2 \rangle$ com $a_i \in A^*$, tais que $a_i = \lambda \bar{a}_i$, para $i = 1, 2$.

Suponhamos que a involução sobre D é trivial. Então $\lambda = \pm 1$ e, como $a_i = \lambda a_i$, temos que $\lambda = 1$. Consequentemente, b é simétrica. Observe que neste caso, temos que D é comutativo, ou seja, D é um corpo e (M, b) é um espaço bilinear simétrico sobre D que admite base ortogonal, logo $\text{car}(D) \neq 2$ pois caso contrário, o espaço bilinear simétrico dado pela matriz $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ teria base ortogonal. Mas isso é equivalente a esta matriz ser semelhante a uma matriz diagonal, o que não é verdade se $\text{car}(D) = 2$. Portanto temos (ii).

Reciprocamente, assumindo (i), ou seja que a involução de D é não trivial, do **Lema(2.7)** temos que (M, b) contém um vetor x anisotrópico. Como $\dim_D(M) \leq 2$, o resultado segue do **Lema(2.5)**.

Finalmente, assumindo que a involução de D é trivial, $\lambda = 1$ e $\text{car}(D) \neq 2$, novamente dos **Lemas(2.5)** e **(2.7)** o resultado segue. ■

Seja (M, b) um espaço λ -hermitiano par sobre um anel com divisão D , isto é, $b = k + \lambda \bar{k}$, com $k \in \text{Seq}_D(M)$. Da **Prop.(2.3)** e usando indução sobre a dimensão de M , obtemos que existe um espaço λ -hermitiano par anisotrópico (M', b') tal que $(M, b) \simeq (M', b') \perp \text{IH}(D^r)$.

Dado um A -módulo λ -hermitiano (M, b) sobre um anel local A , lembremos do capítulo 1 que se $\mathcal{M}$ é o único ideal à direita maximal de A então, escrevendo $\tilde{A} = A/\mathcal{M}$, $\tilde{M} = M \otimes_A A/\mathcal{M}$, temos que $\tilde{A}$ é um anel com divisão e $\tilde{M}$ é um $\tilde{A}$ -módulo livre com $\dim_{\tilde{A}}(\tilde{M}) = \dim_A(M)$. Nestas condições, definimos uma forma sesquilinear $\tilde{b} : \tilde{M} \times \tilde{M} \rightarrow \tilde{A}$ por $\tilde{b}(x \otimes \tilde{a}, y \otimes \tilde{c}) = \tilde{a} (b(x, y) \otimes \tilde{1}) \tilde{c}$, para todo $x, y \in M$ e $\tilde{a}, \tilde{c} \in \tilde{A}$.

Desde que $\tilde{a} = \tilde{\tilde{a}}$ para $a \in A$, temos que a forma $\tilde{b}$ é $\tilde{\lambda}$ -hermitiana pois $\tilde{b}(x \otimes \tilde{a}, y \otimes \tilde{c}) = \tilde{a} (b(x, y) \otimes \tilde{1}) \tilde{c} = \tilde{a} (\lambda \overline{b(y, x)} \otimes \tilde{1}) \tilde{c} = \tilde{a} ((\lambda \otimes \tilde{1})(\overline{b(y, x)} \otimes \tilde{1})) \tilde{c} =$

$\tilde{\lambda} \tilde{a}(\overline{b(y, x) \otimes \tilde{1}}) \tilde{c} = \tilde{\lambda} \tilde{a} \overline{\tilde{b}(y, x)} \tilde{c} = \tilde{\lambda} \tilde{b}(x \otimes \tilde{a}, y \otimes \tilde{c})$, para todo $x, y \in M$ e $a, c \in A$. A adjunta de $\tilde{b}$ é $h_{\tilde{b}} = h_b \otimes 1_{A/\mathcal{M}}$ onde h_b é a adjunta de b . Consequentemente se b é não-singular, então $\tilde{b}$ também o é. Dizemos que $(\tilde{M}, \tilde{b})$ é o módulo $\tilde{\lambda}$ -hermitiano induzido (ou obtido) de (M, b) por extensão de escalares.

Assim, $\sim: \text{Sesq}_A(M) \rightarrow \text{Sesq}_{\tilde{A}}(\tilde{M})$ definida por $b \mapsto \tilde{b} = b \otimes 1_{A/\mathcal{M}} = b \otimes \tilde{1}$, é um homomorfismo (aditivo) de grupos e, desde que $\langle \cdot, \cdot \rangle_b = \langle \cdot, \cdot \rangle_{\tilde{b}}$ e se $b - \lambda \bar{b} = 0$, então $(b - \lambda \bar{b}) \otimes \tilde{1} = 0 \otimes \tilde{1} = 0$, temos que este homomorfismo leva $\mathcal{H}_\lambda(M)$ em $\mathcal{H}_{\tilde{\lambda}}(\tilde{M})$ e $\mathcal{H}_\lambda^p(M)$ em $\mathcal{H}_{\tilde{\lambda}}^p(\tilde{M})$.

Veremos agora, alguns resultados que são ferramentas importantes para a demonstração do Teorema de Decomposição dos espaços λ -hermitianos pares sobre um anel local A . Consideremos os subconjuntos $S_\lambda(A) = \{a + \lambda \bar{a}; a \in A\}$ e $S^\lambda(A) = \{a \in A; a = \lambda \bar{a}\}$.

Se $r: A \rightarrow A/\mathcal{M} = \tilde{A}$ é a projeção canônica, então $r(S^\lambda(A)) \subseteq S^{\tilde{\lambda}}(\tilde{A})$, mas em geral não vale a igualdade pois, se $\tilde{a} \in S^{\tilde{\lambda}}(\tilde{A})$, então $a + \mathcal{M} = (\lambda + \mathcal{M})(\bar{a} + \mathcal{M})$ e, consequentemente $a = \lambda \bar{a} + x$, para algum $x \in \mathcal{M}$ o que não implica que $a \in S^\lambda(A)$. Mas, apesar disso, r é sobrejetora sobre os elementos λ -hermitianos pares, isto é, $r(S_\lambda(A)) = S_{\tilde{\lambda}}(\tilde{A})$. Assim temos:

Proposição 2.4 *A aplicação $\sim: \text{Sesq}_A(M) \rightarrow \text{Sesq}_{\tilde{A}}(\tilde{M})$ definida por $b \mapsto \tilde{b}$ é sobrejetora. Mais ainda, $\sim: \mathcal{H}_\lambda^p(M) \rightarrow \mathcal{H}_{\tilde{\lambda}}^p(\tilde{M})$ é também uma sobrejeção.*

Dem.: Seja $\{e_1, \dots, e_n\}$ uma base de M . Dado $\tilde{b} \in \text{Sesq}_{\tilde{A}}(\tilde{M})$ escolhemos $a_{ij} \in A$ tal que $r(a_{ij}) = \tilde{a}_{ij} = \tilde{b}(e_i, e_j)$ e definimos $b: M \times M \rightarrow A$ por $b(e_i, e_j) = a_{ij}$. É evidente que $b \in \text{Sesq}_A(M)$ e $r(b) = \tilde{b}$. Logo $\sim: \text{Sesq}_A(M) \rightarrow \text{Sesq}_{\tilde{A}}(\tilde{M})$ é uma sobrejeção.

Seja agora, $\tilde{b} \in \mathcal{H}_{\tilde{\lambda}}^p(\tilde{M})$ então $\tilde{b}(e_i, e_j) = \tilde{k}(e_i, e_j) + \tilde{\lambda} \overline{\tilde{k}(e_j, e_i)}$, para algum $\tilde{k} \in \text{Sesq}_{\tilde{A}}(\tilde{M})$. Tomando $k \in \text{Sesq}_A(M)$ tal que $r(k) = \tilde{k}$ e $b = k + \lambda \bar{k}$, temos que $b(e_i, e_j) = k(e_i, e_j) + \lambda \overline{k(e_j, e_i)}$, ou seja $b \in \mathcal{H}_\lambda^p(M)$ e $r(b) = \tilde{b}$. ■

Agora estamos aptos a demonstrar o Teorema da Redução para espaços λ -hermitianos pares. Consideremos $\mathcal{H}_\lambda^p(A)$ a categoria dos módulos λ -hermitianos pares sobre A .

Teorema 2.2 *Seja $\tilde{r} : \mathcal{H}_\lambda^p(A) \rightarrow \mathcal{H}_\lambda^p(\tilde{A})$ o funtor definido por $\tilde{r}((M, b)) = (\tilde{M}, \tilde{b})$. Se $\tilde{r}((M, b))$ é um espaço $\tilde{\lambda}$ -hermitiano sobre $\tilde{A}$, então (M, b) é um espaço λ -hermitiano sobre A . Mais ainda, se $\tilde{r}((M, b)) = (\tilde{M}_1, \tilde{b}_1) \perp (\tilde{M}_2, \tilde{b}_2)$ com $(\tilde{M}_i, \tilde{b}_i)$ não-singulares sobre $\tilde{A}$, $i = 1, 2$, então existem $(M_i, b_i) \in \mathcal{H}_\lambda^p(A)$, não-singulares, tais que $(M, b) = (M_1, b_1) \perp (M_2, b_2)$ e $\tilde{r}((M_i, b_i)) = (\tilde{M}_i, \tilde{b}_i)$, $i = 1, 2$.*

Dem.: Pela **Prop.(2.4)** o funtor $\tilde{r}$ é sobrejetor. Mais ainda, como $(\tilde{M}, \tilde{b})$ é um espaço $\tilde{\lambda}$ -hermitiano par sobre $\tilde{A}$, pelo **Lema(1.3)** (M, b) também é um espaço λ -hermitiano par sobre A .

Além disso, como $\tilde{r}((M, b)) = (\tilde{M}, \tilde{b}) = (\tilde{M}_1, \tilde{b}_1) \perp (\tilde{M}_2, \tilde{b}_2)$, então $\tilde{M} = \tilde{M}_1 \perp \tilde{M}_2$ e pela **Obs.(1.1)** temos que $M = M_1 \oplus M_2$.

Seja agora, $\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix}$ a matriz de h_b com respeito a decomposição $M = M_1 \oplus M_2$, onde $\{e_1, \dots, e_n\}$ é uma base de M_1 e $\{f_1, \dots, f_m\}$ uma base de M_2 . Assim, $\varphi_{11} = (h_b(e_i, e_j))$, $\varphi_{12} = (h_b(e_i, f_j))$, $\varphi_{21} = (h_b(f_i, e_j))$ e $\varphi_{22} = (h_b(f_i, f_j))$.

Dado $(\tilde{M}_1, \tilde{b}_1) \in \mathcal{H}_\lambda^p(\tilde{A})$, não-singular, então existe $(M_1, b_1) \in \mathcal{H}_\lambda^p(A)$ tal que $\tilde{r}(b_1) = \tilde{b}_1$ e b_1 é não-singular pois $(h_{\tilde{b}}(\tilde{e}_i, \tilde{e}_j)) = \tilde{r}(h_b(e_i, e_j)) = \tilde{r}(a_{11}) = \tilde{a}_{11}$, então pelo **Lema(1.3)** $h_{b_1} = a_{11}$ é um isomorfismo. Consequentemente, pelo **Lema(2.5)** $(M, b) \simeq (M_1, b_1) \perp (M_1, b_1)^\perp$, ou seja, $(M, b) \simeq (M_1, b_1) \perp (M_2, b_2)$, com (M_2, b_2) não-singular. Claramente $\tilde{r}((M_2, b_2)) = (\tilde{M}_2, \tilde{b}_2)$ o que prova o teorema. ■

Deste teorema, vemos que a decomposição de espaços λ -hermitianos pares em subespaços de dimensão ≤ 2 , sobre anéis com divisão, pode ser levantada a uma decomposição ortogonal de espaços de dimensão ≤ 2 , sobre anéis locais. Mais precisamente temos:

Teorema 2.3 *Seja (M, b) um espaço λ -hermitiano par sobre um anel local A , com $\dim_A(M) = n$.*

(i) *Se $n = 2m$, então $(M, b) \simeq \perp_{i=1}^n (N_i, b_i)$ onde $\dim_A(N_i) = 2$ e N_i tem uma base $\{x_{i1}, x_{i2}\}$ com $b(x_{i1}, x_{i2}) = 1$, para cada $i = 1, \dots, m$.*

(ii) *Se $n = 2m + 1$, então $(M, b) \simeq (\perp_{i=1}^m (N_i, b_i)) \perp (N_n, b_n)$, onde os N_i , com $1 \leq i \leq m$, são como em (i) e $N_n = x_n A$ com $b(x_n, x_n) \in A^*$.*

Dem.: Usando o **Cor(2.1)** e o teorema anterior, temos a decomposição em soma ortogonal de subespaços de $\dim_A(M) \leq 2$. Logo, podemos assumir que $\dim_A(M) \leq 2$.

Se $\dim_A(M) = 1$, ou seja $M = xA$, então $b(x, x) \in A^*$, pois b é não-singular. Se $\dim_A(M) = 2$, e (M, b) é isotrópico, então da **Prop.(2.2)**, temos que $(M, b) \simeq \left(M, \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix} \right)$, ou seja, M admite uma base $\{x_1, x_2\}$ tal que $b(x_1, x_2) = 1$.

Seja (M, b) anisotrópico, com $M = x'_1 A \oplus x'_2 A$. Seja $(b_{ij}) \in GL_2(A)$ com $b_{ij} = b(x'_i, x'_j)$. Se $b_{12} \in A^*$, então $x_1 = x'_1$ e $x_2 = b_{12}^{-1} x'_2$ é uma base de M com $b(x_1, x_2) = 1$. Se $b_{12} \in \mathcal{M}$ então $b_{21} = \lambda \overline{b_{12}} \in \mathcal{M}$ e, neste caso, $\{\widetilde{x'_1}, \widetilde{x'_2}\}$ é uma base ortogonal de $(\widetilde{M}, \widetilde{b})$. Tomando $\alpha = \widetilde{b}(\widetilde{x'_1}, \widetilde{x'_1})^{-1}$, temos que $\widetilde{x'_1}$ e $\widetilde{y_1} = \alpha \widetilde{x'_1} + \widetilde{x'_2}$ formam uma base de $\widetilde{M}$ sobre $\widetilde{A}$ com $\widetilde{b}(\widetilde{x'_1}, \widetilde{y_1}) = \widetilde{1}$. Assim, a matriz de $\widetilde{b}$ em relação a esta nova base é da forma $\begin{pmatrix} \widetilde{a_{11}} & \widetilde{1} \\ \widetilde{\lambda} & \widetilde{a_{22}} \end{pmatrix}$. Levantando esta base para uma base $\{y_1, y_2\}$ de M , temos da **Prop.(1.4)**, que a matriz de b em relação a esta é da forma (b'_{ij}) com $b'_{12} \in A^*$. Consequentemente, temos que M admite uma base $\{x_1, x_2\}$ com $b(x_1, x_2) = 1$, o que mostra o teorema. ■

2.3 Espaços Unitários sobre anéis locais

Da mesma forma que espaços λ -hermitianos são uma generalização de espaços bilineares e, no caso comutativo, temos uma relação entre formas quadráticas e bilineares,

gostaríamos de obter uma extensão do conceito de formas quadráticas, para anéis não comutativos, de tal forma que tenhamos uma relação destas com formas λ -hermitianas análoga ao caso comutativo. Nesta seção apresentaremos essa extensão. Para tanto necessitamos de algumas noções preliminares.

Seja Γ um subgrupo aditivo de A tal que

- (i) $S_{-\lambda}(A) = \{a - \lambda\bar{a}; a \in A\} \subseteq \Gamma \subseteq \{a \in A; a + \lambda\bar{a} = 0\} = S^{-\lambda}(A)$.
- (ii) $ax\bar{a} \in \Gamma$, para todo $x \in \Gamma$ e $a \in A$.

Uma tripla (A, λ, Γ) , com Γ como acima é chamado um *anel unitário* e o par (λ, Γ) uma *forma parâmetro* para A . Denotaremos algumas vezes $S^{-\lambda}(A)$ por Γ_{max} e $S_{-\lambda}(A)$ por Γ_{min} .

Observe que se existe $a \in Z(A)$ tal que $a + \bar{a} = 1$, então $\Gamma_{min} = \Gamma_{max}$, pois se $x \in A$ é tal que $x + \lambda\bar{x} = 0$, então $x = ax - \lambda\bar{a}\bar{x} \in \Gamma_{min}$. Em particular, se $2 \in A^*$, então $\frac{1}{2} \in Z(A)$ é tal que $\frac{1}{2} + \bar{\frac{1}{2}} = 1$ e, assim, as únicas formas parâmetros sobre A , neste caso, são (λ, Γ_{max}) com $\lambda \in Z(A)$ tal que $\lambda\bar{\lambda} = 1$.

Definição 2.6 Um morfismo de anéis unitários $f : (A, \lambda, \Gamma) \rightarrow (A', \lambda', \Gamma')$ é um homomorfismo de anéis com involução $f : A \rightarrow A'$ tal que $f(\lambda) = \lambda'$ e $f(\Gamma) \subseteq \Gamma'$. Dizemos que f é uma sobrejeção unitária se $f(A) = A'$ e $f(\Gamma) = \Gamma'$.

Sejam (A, λ, Γ) um anel local unitário e $\mathcal{M}$ o único ideal maximal à direita de A . Então $(\tilde{A}, \tilde{\lambda}, \tilde{\Gamma})$ é um anel unitário onde $\tilde{\lambda} \equiv \lambda \text{ mod } \mathcal{M}$ e $\tilde{\Gamma} = \Gamma/\Gamma \cap \mathcal{M}$ e, mais ainda, a sobrejeção canônica $f: A \rightarrow \tilde{A}$ é uma sobrejeção unitária.

Consideremos

$$\mathcal{H}_{-\lambda}^{\Gamma}(M) = \{b \in \mathcal{H}_{-\lambda}(M); b(x, x) \in \Gamma, \forall x \in M\}$$

e

$$\Gamma(M) = \{h \in \text{Hom}_A(M, M^*); h + \lambda\bar{h} = 0, h(m)(m) \in \Gamma, \forall m \in M\}.$$

É fácil ver que $\mathcal{H}_{-\lambda}^{\Gamma}(M)$ é um subgrupo de $\mathcal{H}_{-\lambda}(M)$. Como $S_{-\lambda}(A) \subseteq \Gamma$, o subgrupo das formas $(-\lambda)$ -hermitianas pares de $Sesq_A(M)$ está contido em $\mathcal{H}_{-\lambda}^{\Gamma}(M)$. Pois, se $b \in \mathcal{H}_{-\lambda}(M)$ e b é par, então, $b = k - \lambda \bar{k}$ com $k \in Sesq_A(M)$ e assim, $b(x, x) = (k - \lambda \bar{k})(x, x) = k(x, x) - (\lambda \bar{k})(x, x) = k(x, x) - \lambda \overline{k(x, x)} \in \Gamma_{min} \subseteq \Gamma$. Portanto, $\mathcal{H}_{-\lambda}^p(M) \subseteq \mathcal{H}_{-\lambda}^{\Gamma}(M) \subseteq \mathcal{H}_{-\lambda}(M)$.

Observação 2.2 (i) Se $\Gamma = \Gamma_{max}$, então $\mathcal{H}_{-\lambda}^{\Gamma}(M) = \mathcal{H}_{-\lambda}(M)$, pois se $b \in \mathcal{H}_{-\lambda}(M)$, então $b(x, x) = -\lambda \overline{b(x, x)}$. Assim $b(x, x) + \lambda \overline{b(x, x)} = 0$, ou seja, $b(x, x) \in \Gamma_{max} = \Gamma$. Logo, $b \in \mathcal{H}_{-\lambda}^{\Gamma}(M)$.

(ii) Se $\Gamma = \Gamma_{min}$, então $\mathcal{H}_{-\lambda}^p(M) = \mathcal{H}_{-\lambda}^{\Gamma}(M)$, pois se $b \in \mathcal{H}_{-\lambda}^{\Gamma}(M)$, então $b \in \mathcal{H}_{-\lambda}(M)$ e $b(x, x) \in \Gamma = \Gamma_{min}$. Assim $b(x, x) = a - \lambda \bar{a}$, para algum $a \in A$. Portanto, $b \in \mathcal{H}_{-\lambda}^p(M)$.

Seja $M = A^n$ com a base canônica $\{e_1, \dots, e_n\}$. Se identificarmos o grupo $Sesq_A(A^n)$ com $M_n(A)$ via $b \mapsto (b_{ij})$ onde $b_{ij} = b(e_i, e_j)$, então, $\mathcal{H}_{-\lambda}^{\Gamma}(A^n)$ é o conjunto das matrizes $(n \times n)$, (b_{ij}) tais que $b_{ij} = -\lambda \overline{b_{ji}}$ e $b_{ii} \in \Gamma$, para todo $i, j = 1, \dots, n$.

Definimos um *módulo* (λ, Γ) -unitário sobre A como sendo um par $(M, [k])$ onde $[k]$ é a classe de $k \in Sesq_A(M)$ (módulo $\mathcal{H}_{-\lambda}^{\Gamma}(M)$).

A forma parâmetro (λ, Γ) será omitida na notação quando estiver claro sobre qual anel unitário estamos trabalhando.

Como $\mathcal{H}_{-\lambda}^{\Gamma}(M) \subseteq \mathcal{H}_{-\lambda}(M)$, a forma λ -hermitiana par associada à forma sesquilinear $k, \langle, \rangle_k$ é unicamente determinada pelo módulo unitário $(M, [k])$. De fato, se $[k] = [k']$, com $k, k' \in Sesq_A(M) \pmod{\mathcal{H}_{-\lambda}^{\Gamma}(M)}$, então $k = k' + h$, onde $h \in \mathcal{H}_{-\lambda}^{\Gamma}(M)$, ou seja, $k + \lambda \bar{k} = (k' + h) + \lambda \overline{(k' + h)} = (k' + \lambda \bar{k}') + (h + \lambda \bar{h}) = k' + \lambda \bar{k}'$, pois $h = -\lambda \bar{h}$. Nessas condições, $\langle, \rangle_k = \langle, \rangle_{k'}$. Neste caso, dizemos que $(M, \langle, \rangle_k)$ é o *módulo* λ -hermitiano par associado ao módulo unitário $(M, [k])$.

O par $(M, [k])$ é dito ser um *espaço unitário* se o módulo λ -hermitiano par $(M, \langle, \rangle_k)$ é não-singular.

Observação 2.3 Se $\Gamma = \Gamma_{max}$, então $(M, [k])$ é unicamente determinado pelo módulo

par associado $(M, <, >_k)$, pois se $k + \lambda \bar{k} = k' + \lambda \bar{k}'$ para $k, k' \in \text{Sesq}_A(M)$, então $k - k' = \lambda(\bar{k}' - \bar{k}) = -\lambda(\overline{k - k'})$, ou seja, $k - k' \in \mathcal{H}_{-\lambda}^\Gamma(M)$ e $(k - k')(x, x) \in \Gamma$.

Em geral, o mesmo espaço λ -hermitiano par pode corresponder a diferentes espaços unitários. Por exemplo, no caso comutativo, se K é um corpo com $\text{car}(K) = 2$, então todo espaço quadrático (M, q) sobre K , tem a mesma forma bilinear simétrica associada.

Se M tem como base $\{e_1, \dots, e_n\}$ sobre A , podemos identificar uma forma sesquilinear k com a matriz $(k_{ij}) \in M_n(A)$, com $k_{ij} = k(e_i, e_j)$. Como a matriz (s_{ij}) com

$$s_{ij} = \begin{cases} k_{ij}, & \text{se } i > j \\ 0, & \text{se } i = j \\ -\lambda \bar{k}_{ji}, & \text{se } i < j \end{cases}$$

define uma forma sesquilinear $s \in \mathcal{H}_{-\lambda}^\Gamma(M)$, temos $[k] = [k - s]$. Assim, toda classe $[k]$ pode ser representada por uma matriz triangular, ou seja,

$$[k] = [k - s] = \begin{pmatrix} k_{11} & k_{12} + \lambda \bar{k}_{21} & \dots & k_{1n} + \lambda \bar{k}_{n1} \\ 0 & k_{22} & \dots & k_{2n} + \lambda \bar{k}_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & k_{nn} \end{pmatrix}.$$

Um módulo quadrático sobre um anel comutativo A é um par (M, q) onde M é um A -módulo e $q : M \rightarrow A$ é tal que :

- (i) $q(ax) = a^2 q(x)$, para todo $x \in M, a \in A$
- (ii) $b_q(x, y) = q(x + y) - q(x) - q(y)$ define sobre M uma forma bilinear simétrica $b_q : M \times M \rightarrow A$.

Gostaríamos de ter essa relação no caso não comutativo. Para tanto, definimos :

Definição 2.7 Uma “função quadrática” associada a um módulo unitário $(M, [k])$ sobre A é uma aplicação $[q] : M \rightarrow A/\Gamma$ definida por $[q](x) = k(x, x) + \Gamma \in A/\Gamma$, para todo $x \in M$.

Como $\bar{a}xa \in \Gamma$, para todo $x \in \Gamma$ e $a \in A$, temos que $\bar{a}(x + \Gamma)a = \bar{a}xa + \Gamma$ e, consequentemente, $[q](xa) = \bar{a}([q](x))a$, para todo $x \in M$ e $a \in A$.

A função quadrática $[q]$ e a forma par $\langle, \rangle_k$ estão relacionadas pela fórmula

$$[q](x + y) - [q](x) - [q](y) \equiv \langle x, y \rangle_k \text{ mod } \Gamma,$$

pois $k(x + y, x + y) - k(x, x) - k(y, y) + \Gamma = k(x, y) + k(y, x) + \Gamma = \langle x, y \rangle_k + k(y, x) - \lambda \overline{k(y, x)} = \langle x, y \rangle_k + \Gamma$, para todo $x, y \in M$.

Observemos que um módulo quadrático (M, q) pode ser visto como um módulo $(1, \Gamma)$ -unitário $(M, [k])$, onde $\Gamma = \{0\}$, a aplicação quadrática correspondente $[q]: M \rightarrow A/\Gamma$ é apenas a forma quadrática q e, $\langle, \rangle_k$ a forma bilinear simétrica b_q associada à forma quadrática q . Assim, vemos que o conceito de módulo (λ, Γ) -unitário é realmente uma generalização de módulo quadrático.

Sejam $(M_1, [k_1])$ e $(M_2, [k_2])$ módulos unitários sobre A . Se $\varphi: M_1 \rightarrow M_2$ é um homomorfismo de A -módulos, então φ induz uma aplicação $Z(A)$ -linear $Sesq(\varphi): Sesq_A(M_2) \rightarrow Sesq_A(M_1)$, onde $Sesq(\varphi)(b)(x, y) = b(\varphi(x), \varphi(y))$ para todo $b \in Sesq_A(M_2)$ e $x, y \in M_1$. Dizemos que $\varphi: (M_1, [k_1]) \rightarrow (M_2, [k_2])$ é uma *isometria de módulos unitários* se φ é um isomorfismo de A -módulos e $[k_1] = [Sesq(\varphi)(k_2)]$.

Lema 2.8 *Sejam $(M_i, [k_i])$, $i = 1, 2$, módulos unitários sobre A . Um isomorfismo de A -módulos $\varphi: M_1 \rightarrow M_2$ é uma isometria de módulos unitários se, e somente se $\langle \varphi(x), \varphi(y) \rangle_{k_2} = \langle x, y \rangle_{k_1}$ e $[q_{k_2}](\varphi(x)) = [q_{k_1}](x)$, para todo $x, y \in M_1$.*

Dem.: O isomorfismo φ é uma isometria se, e somente se $[k_1] = [Sesq(\varphi)(k_2)]$, ou seja, $k_1 - Sesq(\varphi)(k_2) \in \mathcal{H}_{-\lambda}^\Gamma(M_1)$, ou equivalentemente, $k_1 - Sesq(\varphi)(k_2) = -\lambda(k_1 - Sesq(\varphi)(k_2))$ e $(k_1 - Sesq(\varphi)(k_2))(x, x) \in \Gamma$, para todo $x \in M_1$. Isto ocorre se, e somente se $k_1 + \lambda \overline{k_1} = Sesq(\varphi)(k_2 + \lambda \overline{k_2})$ e $k_1(x, x) \equiv Sesq(\varphi)(k_2)(x, x) \text{ mod } \Gamma$ e, o lema segue. ■

Sejam $(M_i, [k_i])$, $i = 1, 2$, módulos unitários sobre A . Como $\mathcal{H}_{-\lambda}^\Gamma(M_1) \oplus \mathcal{H}_{-\lambda}^\Gamma(M_2) \subseteq \mathcal{H}_{-\lambda}^\Gamma(M_1 \oplus M_2)$, a classe $[k_1 \perp k_2]$ depende somente das classes $[k_1]$ e $[k_2]$. Assim a

soma ortogonal de módulos unitários é um módulo unitário, $(M_1, [k_1]) \perp (M_2, [k_2]) = (M_1 \oplus M_2, [k_1 \perp k_2])$.

Observação 2.4 Seja $(M, [k])$ um módulo unitário tal que $M = M_1 \oplus M_2$, para submódulos M_1 e M_2 de M . Suponhamos que M_1 e M_2 são ortogonais com respeito a forma λ -hermitiana par associada $\langle, \rangle_k$. Afirmamos que $(M, [k]) = (M_1, [k_1]) \perp (M_2, [k_2])$, como módulos unitários, onde $k_i = k|_{M_i}$, $i = 1, 2$. De fato, se $k' = k_1 \perp k_2$ e $t = k - k'$, então, para todo $x = x_1 + x_2$, $y = y_1 + y_2 \in M = M_1 \oplus M_2$, temos

$$\begin{aligned} \langle x, y \rangle_t &= (k - k')(x, y) + \lambda(\overline{k - k'})(x, y) = \\ &= k(x_1, y_2) + k(x_2, y_1) + \lambda\overline{k}(x_1, y_2) + \lambda\overline{k}(x_2, y_1) = \\ &= (k + \lambda\overline{k})(x_1, y_2) + (k + \lambda\overline{k})(x_2, y_1) = \\ &= \langle x_1, y_2 \rangle_k + \langle x_2, y_1 \rangle_k = 0. \end{aligned}$$

Mais ainda, $[q_t](x) \equiv t(x, x) \mod \Gamma$, para todo $x \in M$. Mas

$$t(x, x) = (k - k')(x, x) = k(x_1, x_2) + k(x_2, x_1) = k(x_1, x_2) + \lambda\overline{k}(x_2, x_1) = \langle x_1, x_2 \rangle_t$$

em A/Γ . Logo $[q_t](x) \equiv 0 \mod \Gamma$. Portanto $[t] = [0]$, ou seja $[k] = [k']$.

Assim, decomposição ortogonal de módulos unitários é equivalente a decomposição ortogonal dos módulos λ -hermitianos pares associados. Uma importante consequência desta observação é que o **Lema(2.5)** vale para módulos unitários, desde que vale para formas λ -hermitianas pares.

Lema 2.9 *Seja $(M, [k])$ um módulo unitário. Se U é um submódulo de M tal que $(U, [k|_U])$ é não-singular, então $(U, [k|_U])$ é um somando ortogonal de $(M, [k])$.*

Dado um A -módulo M , consideremos o módulo unitário

$$\mathbb{H}_\Gamma(M) = \left(M \oplus M^*, \left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right] \right).$$

O módulo λ -hermitiano par associado é $\left(M \oplus M^*, \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix} \right)$, ou seja $\mathbb{H}(M)$. Assim $\mathbb{H}_\Gamma(M)$ é um espaço unitário chamado um *espaço unitário hiperbólico*. Em particular, se $M = xA$, então $\mathbb{H}_\Gamma(M) = \left(xA \oplus yA, \left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right] \right)$, ou seja, $[q](x) = [q](y) = 0$ e $\langle x, y \rangle_k = 1$. Neste caso, diremos que $\mathbb{H}_\Gamma(M)$ é um *plano hiperbólico unitário* e denotaremos simplesmente por $\mathbb{H}_\Gamma$. Diremos também que x e y como acima, formam um *par hiperbólico unitário*.

Definição 2.8 Um espaço (λ, Γ) -unitário $(M, [k])$ é dito ser metabólico se existe uma decomposição $M = N \oplus P$ com $N = N^\perp$, isto é,

$$[k] = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

com $\alpha \in \Gamma(N)$.

Afirmamos que espaços unitários metabólicos são também hiperbólicos, pois se adicionarmos à $[k]$ a matriz $[s] = \begin{pmatrix} -\alpha & -\gamma\lambda \\ -\gamma & 0 \end{pmatrix} \in \Gamma(M)$, obtemos $[k] = [k + s] = \begin{pmatrix} 0 & \beta_1 \\ 0 & \delta \end{pmatrix}$ onde $\beta_1 = \beta - \gamma\lambda$ e pelas equações :

$$\begin{pmatrix} 1 & 0 \\ 0 & \overline{\beta_1}^{-1} \end{pmatrix} \begin{pmatrix} 0 & \beta_1 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \beta_1^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & \delta_1 \end{pmatrix}$$

e

$$\begin{pmatrix} 1 & 0 \\ -\delta_1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & \delta_1 \end{pmatrix} \begin{pmatrix} 1 & -\overline{\delta_1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

ou seja, a afirmação segue.

Como no caso λ -hermitiano, temos também a noção de vetor isotrópico, espaços isotrópicos e anisotrópicos para módulos unitários. Um elemento $x \in (M, [k])$ é dito

ser *isotrópico* se $[q](x) = 0$, ou seja se $k(x, x) \in \Gamma$ e, $(M, [k])$ é dito ser *anisotrópico* se 0 é o único vetor isotrópico de M . Um submódulo U de $(M, [k])$ é *totalmente isotrópico* se $[q](U) = 0$ e $\langle, \rangle_{k|_{U \times U}} = 0$.

Observe que o espaço λ -hermitiano par $(M, \langle, \rangle_k)$ não é necessariamente anisotrópico se $(M, [k])$ é anisotrópico. Por exemplo, no caso comutativo, se K é um corpo com $\text{car}(K) = 2$, a forma bilinear b_q é isotrópica, mesmo quando a forma q é anisotrópica.

A **Prop.(2.2)** para espaços λ -hermitianos pares, tem seu correspondente para espaços unitários.

Proposição 2.5 *Sejam $(M, [k])$ um espaço unitário e $x \in M$ um vetor unimodular e isotrópico. Então existe $y \in M$ tal que $[q](y) = 0$ e $\langle x, y \rangle_k = 1$. Em particular, $\{x, y\}$ é a base de um plano hiperbólico $\mathbb{H}_\Gamma$ em $(M, [k])$.*

Dem.: Desde que $(M, [k])$ é um espaço (λ, Γ) -unitário e x é unimodular, então existe $z \in M$ tal que $\langle x, z \rangle_k = 1$. Observe que a matriz de $\langle, \rangle_k$ restrita ao subespaço gerado por x e z é $\begin{pmatrix} 0 & 1 \\ \lambda & \langle z, z \rangle_k \end{pmatrix}$, que é claramente inversível. Logo $(M_1 = xA \oplus zA, [k|_{M_1}])$ é não-singular. Se $\langle z, z \rangle_k = 0$, então x e z é o par procurado. Caso contrário, se $\langle z, z \rangle_k = \delta \neq 0$ como $\langle z, z \rangle_k = k(z, z) + \lambda \overline{k(z, z)}$, consideremos $h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ a matriz de k restrita a M_1 , onde $\alpha = k(x, x) \in \Gamma$ (pois x é isotrópico) e $\langle x, z \rangle_k = k(x, z) + \lambda \overline{k(z, x)} = \beta + \lambda \overline{\gamma} = 1$.

Se $g = \begin{pmatrix} -\alpha & \lambda \overline{\gamma} \\ \gamma & 0 \end{pmatrix}$, então $g \in \Gamma(M_1)$ pois $g = -\lambda \overline{g}$ e, além disso se $m = xa_1 + za_2 \in M_1$, então $[q_g](m) \equiv g(xa_1 + za_2, xa_1 + za_2) \text{ mod } \Gamma \equiv -\overline{a_2} \gamma a_1 + \lambda \overline{a_1} \gamma a_2 \text{ mod } \Gamma \equiv 0 \text{ mod } \Gamma$.

Assim, $[h] = [h + g] = \begin{pmatrix} 0 & 1 \\ 0 & \delta \end{pmatrix}$. Tomando $y = -x\overline{\delta} + z$ temos $\langle x, z \rangle_k = k(x, -x\overline{\delta} + z) + \lambda \overline{k(-x\overline{\delta} + z, x)} = -k(x, x)\overline{\delta} + k(x, z) + \lambda \overline{(-\delta k(x, x) + k(z, x))} = 1$.

Além disso,

$$[q](y) \equiv k(y, y) \bmod \Gamma \equiv k(-x\bar{\delta} + z, -x\bar{\delta} + z) \bmod \Gamma \equiv -\delta + \delta \bmod \Gamma \equiv 0 \bmod \Gamma.$$

Logo x e y formam o par hiperbólico unitário procurado. ■

Os próximos três resultados, já provados para espaços λ -hermitianos pares, seguem diretamente da **Obs.(2.4)**, com demonstrações análogas, para espaços unitários.

Proposição 2.6 *Seja $(M, [k])$ um espaço (λ, Γ) -unitário sobre um anel com divisão D . Então existe uma decomposição ortogonal finita*

$$(M, [k]) \simeq (\perp (M_i, [k_i]) \perp (\perp \mathbb{H}_j),$$

com $(M_i, [k_i])$ anisotrópicos de dimensão ≤ 2 e os $\mathbb{H}_j$ planos hiperbólicos unitários.

Seja $\sim : \text{Sesq}_A(M) \rightarrow \text{Sesq}_{\tilde{A}}(\tilde{M})$ o homomorfismo (aditivo) como definido na seção 2. Como já vimos, $\sim$ leva $\mathcal{H}_{-\lambda}(M)$ em $\mathcal{H}_{-\tilde{\lambda}}(\tilde{M})$, mais ainda $\sim$ leva $\mathcal{H}_{\lambda}^{\Gamma}(M)$ em $\mathcal{H}_{\tilde{\lambda}}^{\tilde{\Gamma}}(\tilde{M})$, pois basta verificar que $\tilde{b}(\tilde{x}, \tilde{x}) \in \tilde{\Gamma}$ para todo $\tilde{x} \in \tilde{M}$, e todo $b \in \mathcal{H}_{-\lambda}^{\Gamma}(M)$. Sabemos que se $b(x, x) \in \Gamma$, então $b(x, x) \otimes \tilde{1} \in \tilde{\Gamma}$. Logo $\tilde{b}(\tilde{x}, \tilde{x}) = \tilde{b}(x \otimes \tilde{1}, x \otimes \tilde{1}) = b(x, x) \otimes \tilde{1} \in \tilde{\Gamma}$.

Portanto existe um homomorfismo canônico

$$\frac{\text{Sesq}_A(M)}{\mathcal{H}_{-\lambda}^{\Gamma}(M)} \rightarrow \frac{\text{Sesq}_{\tilde{A}}(\tilde{M})}{\mathcal{H}_{-\tilde{\lambda}}^{\tilde{\Gamma}}(\tilde{M})}$$

que associa a um módulo unitário $(M, [k])$ sobre A um bem definido módulo unitário $(\tilde{M}, [\tilde{k}])$ sobre $\tilde{A}$. Denotaremos por $EU(A)$ o conjunto dos espaços (λ, Γ) -unitários sobre A .

Teorema 2.4 (Redução) *Sejam $(M, [k])$ um espaço (λ, Γ) -unitário sobre A , $\tilde{F}: EU(A) \rightarrow EU(\tilde{A})$ o funtor definido por $\tilde{F}((M, [k])) = (\tilde{M}, [\tilde{k}])$ e $\tilde{F}((M, [k])) = (\tilde{M}_1, [k_1]) \perp (\tilde{M}_2, [k_2])$ sobre $\tilde{A}$. Então existem $(M_1, [g_1]), (M_2, [g_2])$ espaços unitários sobre A tais que $(M, [k]) = (M_1, [g_1]) \perp (M_2, [g_2])$ e $\tilde{F}((M_i, [g_i])) = (\tilde{M}_i, [k_i])$, para $i = 1, 2$.*

Como consequência do teorema de redução, temos o Teorema de decomposição para espaços unitários sobre anéis unitários locais.

Teorema 2.5 *Seja $(M, [k])$ um espaço unitário sobre o anel unitário local (A, λ, Γ) , com $\dim_A(M) = n$.*

- (i) *Se $n = 2m$, então $(M, [k]) \simeq \perp_{i=1}^m (N_i, [k_i])$ onde $\dim_A(N_i) = 2$ e N_i tem uma base $\{x_{i1}, x_{i2}\}$ com $\langle x_{i1}, x_{i2} \rangle = 1$, para cada $i = 1, \dots, m$.*
- (ii) *Se $n = 2m + 1$, então $(M, [k]) \simeq \perp_{i=1}^m (N_i, [k_i]) \perp (N_n, [k_n])$, onde os N_i , $1 \leq i \leq m$, são como em (i) e $N_n = x_n A$ com $\langle x_n, x_n \rangle \in A^*$.*

Seja $(N, [k])$ um espaço unitário sobre A com $\dim_A(N) = 2$. Dizemos que uma base $\{x_1, x_2\}$ de N é uma *base especial* de $(N, [k])$ se

$$\langle x_1, x_2 \rangle = 1, (\lambda - \langle x_1, x_1 \rangle \langle x_2, x_2 \rangle) \in A^* \text{ e } [q](x_1) \cap A^* \neq \emptyset.$$

Se $\dim_A(N) = 1$, $\{x\}$ é uma *base especial* de $(N, [k])$ se $\langle x, x \rangle \in A^*$ e $[q](x) \cap A^* \neq \emptyset$. Seja agora $(M, [k])$ um espaço unitário sobre (A, λ, Γ) com $\dim_A(M) = n$. Se cada N_i , na decomposição de M dada no **Teo.(2.5)**, tem uma base especial, a correspondente base de M é dita ser uma *base especial* de $(M, [k])$.

Proposição 2.7 *Seja $(M, [k])$ um espaço unitário sobre um anel unitário local (A, λ, Γ) . Então $(M, [k])$ admite uma base especial.*

Dem.: É suficiente mostrar a existência de uma base especial quando $\dim_A M \leq 2$. Primeiramente consideremos $\dim_A M = 2$. Do **Teo.(2.5)**, o espaço $(M, [k])$ tem uma base $\{x_1, x_2\}$ com $\langle x_1, x_2 \rangle = 1$. Assim o espaço λ -hermitiano par associado é representado pela matriz $\begin{pmatrix} a_{11} & 1 \\ \lambda & a_{22} \end{pmatrix}$, onde $a_{ii} = \langle x_i, x_i \rangle$, $i = 1, 2$.

Desde que $\begin{pmatrix} 1 & -\overline{a_{11}} \\ 0 & 1 \end{pmatrix}$ e $\begin{pmatrix} a_{11} & 1 \\ \lambda & a_{22} \end{pmatrix}$ são inversíveis e

$$\begin{pmatrix} 1 & -\overline{a_{11}} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & 1 \\ \lambda & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} - \lambda \overline{a_{11}} & 1 - \overline{a_{11}} a_{22} \\ \lambda & a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 1 - \lambda \overline{a_{11}} a_{22} \\ \lambda & a_{22} \end{pmatrix}$$

temos que $1 - \overline{a_{11}} a_{22} \in A^*$ e, conseqüentemente, $\lambda - a_{11} a_{22} = \lambda(1 - \overline{a_{11}} a_{22}) \in A^*$.

Resta mostrarmos que $[q](x_1) \cap A^* \neq \emptyset$, mas isto é equivalente a existência de $B = (b_{ij}) \in GL_2(A)$ tal que

$$\alpha_1 = \overline{b_{11}} k_{11} b_{11} + \overline{b_{11}} b_{12} + \overline{b_{12}} k_{22} b_{12} \in A^*$$

e

$$\alpha_2 \overline{b_{11}} a_{11} b_{12} + \overline{b_{11}} b_{12} + \lambda \overline{b_{12}} b_{12} + \overline{b_{12}} a_{22} b_{22} \in A^*,$$

onde $k_{ii} = k(x_i, x_i)$, $i = 1, 2$, pois $x'_1 = x_1 b_{11} + x_2 b_{12}$ e $x'_2 = x_1 b_{21} + x_2 b_{22}$ será uma nova base de M , com $\alpha_1 \in [q](x_1) \cap A^*$ e $\langle x'_1, x'_2 \rangle \in A^*$.

Seja $\mathcal{M}$ o único ideal maximal à direita de A . Mostremos então que existe $B = (b_{ij}) \in M_2(A)$, com $\overline{B}$ inversível em $M_2(A/\mathcal{M})$ e $\alpha_1, \alpha_2 \notin \mathcal{M}$.

Se $k_{11} \notin \mathcal{M}$ (ou $k_{22} \notin \mathcal{M}$), tomamos $b_{ii} = 1$ e $b_{ij} = 0$, $i \neq j$ (ou $b_{ii} = 0$ e $b_{ij} = 1$, $i \neq j$). Se k_{11} e $k_{22} \in \mathcal{M}$, então $\alpha_2 = 1 + a_{22} = 1 + k_{22} + \lambda \overline{k_{22}} \in A^*$ e $\alpha_1 \in 1 - \mathcal{M} = A^*$. Assim, segue da **Prop.(1.4)** que $B \in GL_2(A)$, como queríamos.

Se $\dim_A(M) = 1$, ou seja, se $M = xA$, então $\langle x, x \rangle = 1$. Assim, $k(x, x) + \lambda \overline{k(x, x)} = 1$ e, claramente, $k(x, x) \notin \mathcal{M}$, o que implica que $[q](x) \cap A^* \neq \emptyset$. ■

Consideremos agora A comutativo, $\lambda = 1$ e a involução trivial sobre A . Do **Teo.(2.5)** um espaço quadrático (M, q) sobre A é da forma

$$(M, q) \simeq \perp_{i=1}^n (x_i A \oplus y_i A)$$

ou

$$(M, q) \simeq \perp_{i=1}^n (x_i A \oplus y_i A) \perp zA$$

com $b_q(x_i, y_i) = 1$ e, $(1 - 4q(x_i)q(y_i))q(z) \in A^*$, $1 \leq i \leq n$ e, $q(x_i) \in A^*$ para cada $i = 1, \dots, n$.

Além disso, se $|A/\mathcal{M}| \geq 4$ então podemos também considerar $q(y_i) \in A^*$, para $i = 1, \dots, n$. Para vermos isto, basta considerarmos $\dim_A(M) = 2$, ou seja $M = xA \oplus yA$ com $q(x) = \alpha \in A^*$, $q(y) = \beta$, $b_q(x, y) = 1$ e $(1 - 4q(x)q(y)) \in A^*$.

Se $\beta \notin A^*$, mudamos o vetor y da base de M , de modo que $q(y)$ esteja em A^* . Para tanto é suficiente verificarmos que o polinômio $f(X) = X(\alpha + X + \beta X^2)(2\alpha + X)$ representa uma unidade de A . De fato, queremos fazer uma mudança da base $\{x, y\}$ para uma base $\{x, y'\}$ tal que $b_q(x, y')q(y') \in A^*$. Tomamos $y' = x + Xy$ e impomos as condições que queremos. Primeiro, a matriz mudança de base será $\begin{pmatrix} 1 & 1 \\ 0 & X \end{pmatrix}$, assim X tem que ser uma unidade de A . Agora $b_q(x, y')q(y') \in A^*$ é equivalente à $(2\alpha + X)(\alpha + X + \beta X^2) \in A^*$. Portanto, queremos que $f(X)$ represente uma unidade de A .

Como $|A/\mathcal{M}| \geq 4$ e o grau do polinômio $f(X)$ é ≤ 4 , então é suficiente mostrarmos que f representa um elemento não nulo de $A/\mathcal{M}$ quando $|A/\mathcal{M}| = 4$.

Se $|A/\mathcal{M}| = 4$, então $A/\mathcal{M} = \mathbb{F}_2(\gamma)$ com $\gamma^2 + \gamma + 1 = 0$ é um corpo de característica 2. Logo $f(X) = X^2(\alpha + X + \beta X^2)$. Assim f representa um elemento não nulo de $A/\mathcal{M}$ se, e somente se $g(X) = X(\alpha + X + \beta X^2)$ representa e, como grau de g é ≤ 3 o resultado segue.

Portanto se $\dim_A(M) = 2$, então M admite uma base $\{x_1, x_2\}$ tal que $q(x_1)q(x_2) \in A^*$ e $(1 - 4q(x_1)q(x_2)) \in A^*$. Uma tal base, é dita ser uma *base estritamente canônica* de (M, q) e, se (M, q) é um espaço quadrático sobre A com uma decomposição como no **Teo.(2.5)** e $\{x_{i1}, x_{i2}\}$ são bases estritamente canônicas de N_i , para $i = 1, \dots, m$, então a correspondente base de (M, q) é dita ser uma *base estritamente canônica* de (M, q) .

Capítulo 3

Geradores dos Grupos Unitário e Ortogonal sobre um Anel Local

Este capítulo contém os resultados principais do que nos propomos a apresentar neste trabalho, ou seja, a caracterização dos geradores do grupo unitário e do grupo ortogonal de um espaço unitário sobre um anel local, da forma descrita no próximo parágrafo.

Em todo este capítulo assumiremos que A é um anel local (não necessariamente comutativo), com elemento identidade 1 , $\mathcal{M}$ seu único ideal maximal à direita, $(M, [k])$ é um espaço unitário sobre o anel unitário (A, λ, Γ) , com uma decomposição do tipo $M = \mathbb{H}_\Gamma \perp N$ onde $\mathbb{H}_\Gamma$ é um plano hiperbólico unitário e $(N, [k])$ é um subespaço unitário de $(M, [k])$ com $\dim_A(N) \geq 1$. Fixemos também uma base $\{u, v\}$, de $\mathbb{H}_\Gamma$, ou seja, $\langle u, v \rangle_k = 1$ e $[q_k](u) = [q_k](v) = 0$ em A/Γ . Desde que fixamos um espaço unitário $(M, [k])$, no que segue, omitiremos o índice k nas formas λ -hermitiana par e quadrática associada à $[k]$ e, também o índice Γ de $\mathbb{H}_\Gamma$.

3.1 Isometrias de $(M, [k])$

O conjunto de todas as isometrias do espaço unitário $(M, [k])$, com a operação de composição, forma um grupo, chamado o *grupo unitário* de $(M, [k])$ e denotado por $\mathcal{U}(M, [k])$, ou simplesmente por $\mathcal{U}(M)$.

Nesta seção, apresentaremos alguns elementos de $\mathcal{U}(M)$, ou seja, algumas isometrias de $(M, [k])$ que, como veremos na próxima seção, compõem o conjunto dos geradores de $\mathcal{U}(M)$. Apresentaremos também algumas relações entre elas.

Lembremos que, usando o **Lema(2.8)**, para mostrarmos que um automorfismo φ de M é um elemento de $\mathcal{U}(M)$, é suficiente mostrarmos que $[q](\varphi(x)) = [q](x)$ e $\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$, para todo $x, y \in M$.

Sejam $\Delta: M \rightarrow M$ e, para cada $\varepsilon \in A^*$, $\phi(\varepsilon): M \rightarrow M$, definidas por:

$$\begin{aligned}\Delta(u) &= v & \phi(\varepsilon)(u) &= u\varepsilon \\ \Delta(v) &= u\bar{\lambda} & \phi(\varepsilon)(v) &= v\varepsilon^{-1} \\ \Delta(z) &= z & \phi(\varepsilon)(z) &= z\end{aligned}$$

para todo $z \in N$. Estendendo por linearidade e, usando que $\langle u, v \rangle = 1$, $\langle v, u \rangle = \lambda$, $\langle u, z \rangle = \langle v, z \rangle = 0$, $[q](u) = [q](v) = 0$, é fácil verificar que Δ e $\phi(\varepsilon) \in \mathcal{U}(M)$, para todo $\varepsilon \in A^*$.

Para $c \in \Gamma$ definimos $T_c(u): M \rightarrow M$ por:

$$T_c(u)(w) = w + uc\bar{\lambda} \langle u, w \rangle,$$

para todo $w \in M$. Analogamente definimos $T_c(v)$. Observando que $T_c(u)(v) = v + uc\bar{\lambda}$ e $T_c(u)$ restrita à $(uA \oplus N)$ é a identidade, com simples cálculos mostra-se que $T_c(u) \in \mathcal{U}(M)$. Analogamente obtemos $T_c(v) \in \mathcal{U}(M)$. Mais ainda, $T_c(v) = \Delta T_c(u) \Delta^{-1}$.

Para $x \in N$ e $a \in [q](x)$, ou seja, $a \equiv k(x, x) \pmod{\Gamma}$, definimos $E_{u,a,x}: M \rightarrow M$ por

$$E_{u,a,x}(w) = w + u \langle x, w \rangle - x\bar{\lambda} \langle u, w \rangle - u\bar{\lambda}a \langle u, w \rangle,$$

para todo $w \in M$. De maneira similar, definimos $E_{v,a,x}$. Aplicando nos elementos u, v e $z \in N$ separadamente, vemos facilmente que $E_{v,a,x} = \Delta E_{u,a,x} \Delta^{-1}$. Mostremos agora que $E_{u,a,x} \in \mathcal{U}(M)$. Para tanto, basta observarmos que

$$\begin{aligned}
\langle E_{u,a,x}(u), E_{u,a,x}(v) \rangle &= \langle u, -u\bar{\lambda}a + v - x\bar{\lambda} \rangle = \langle u, v \rangle; \\
\langle E_{u,a,x}(u), E_{u,a,x}(z) \rangle &= \langle u, z + u \langle x, z \rangle \rangle = \langle u, z \rangle; \\
[q](E_{u,a,x}(u)) &= [q](u), \text{ pois } E_{u,a,x}(u) = u, \\
[q](E_{u,a,x}(v)) &= [q](-u\bar{\lambda}a + v - x\bar{\lambda}) \equiv \\
&\equiv \langle -u\bar{\lambda}a + v, -x\bar{\lambda} \rangle + [q](-u\bar{\lambda}a) + [q](v) \pmod{\Gamma} \equiv \\
&\equiv \langle -u\bar{\lambda}a, -x\bar{\lambda} \rangle + \langle v, -x\bar{\lambda} \rangle \pmod{\Gamma} = \\
&= [q](v); \\
[q](E_{u,a,x}(z)) &= [q](u \langle x, z \rangle + z) \equiv \\
&\equiv \langle u \langle x, z \rangle, z \rangle + [q](u \langle x, z \rangle) + [q](z) \pmod{\Gamma} = \\
&= [q](z).
\end{aligned}$$

As isometrias do tipo $E_{u,a,x}$ e $E_{v,a,x}$ são chamadas de *Transvecções de Eichler-Siegel*.

Para as isometrias definidas acima, temos as seguintes identidades relacionando-as:

- (1) $[\phi(\varepsilon), \Delta] = \phi(\varepsilon)\Delta(\phi(\varepsilon))^{-1}(\Delta)^{-1} = \phi(\varepsilon\bar{\varepsilon}), \phi(\varepsilon)^{-1} = \phi(\varepsilon^{-1}).$
- (2) $T_c(u)T_d(u) = T_{c+d}(u), T_c(u)^{-1} = T_{\lambda\bar{c}}(u).$
- (3) $T_c(ua) = T_{ac\bar{a}}(u), \forall a \in A.$
- (4) $\phi(\varepsilon)T_c(u)\phi(\varepsilon^{-1}) = T_{\varepsilon c\bar{\varepsilon}}(u).$
- (5) $\phi(\varepsilon)T_c(v)\phi(\varepsilon^{-1}) = T_{\bar{\varepsilon}^{-1}c\varepsilon^{-1}}(v).$
- (6) $\varphi E_{u,a,x}\varphi^{-1} = E_{\varphi(u),a,\varphi(x)}, \forall \varphi \in \mathcal{U}(M).$
- (7) $T_c(u)E_{u,a,x}T_c(u)^{-1} = E_{u,a,x}.$
- (8) $E_{u,a,x}E_{u,a',y} = E_{u,a+a'+\langle x,y \rangle, x+y} = E_{u,k(x+y,x+y),x+y}T_c(u), \text{ com } c = k(y,x) - \lambda\overline{k(y,x)}.$
- (9) $(E_{u,a,x})^{-1} = E_{u,\langle x,x \rangle - a, -x} = E_{u,a,-x}T_c(u), \text{ com } c = a - \lambda\bar{a}.$
- (10) $[E_{u,a,x}, E_{u,a',y}] = T_c(u), \text{ com } c = \langle y, x \rangle - \langle x, y \rangle.$
- (11) $E_{ur,a,x} = E_{u,ra\bar{r},x\bar{r}}, \forall r \in A.$

$$(12) \phi(\varepsilon)E_{u,a,x}\phi(\varepsilon^{-1}) = E_{u,\varepsilon a\bar{\varepsilon},x\bar{\varepsilon}}.$$

$$(13) \phi(\varepsilon)E_{v,a,x}\phi(\varepsilon^{-1}) = E_{v,\bar{\varepsilon}^{-1}a\varepsilon^{-1},x\varepsilon^{-1}}.$$

Façamos algumas observações sobre cada uma das identidades citadas acima, ou seja, diremos porque tem sentido as isometrias que figuram nas igualdades e um esboço de como se verifica cada igualdade.

Nas identidades de (1) a (5), observamos que podemos definir as isometrias $\phi(\varepsilon\bar{\varepsilon})$, $\phi(\varepsilon^{-1})$, $T_{c+d}(u)$, $T_{\lambda\bar{\varepsilon}}(u)$, $T_{a\bar{c}\bar{a}}(u)$, $T_{\varepsilon c\bar{\varepsilon}}$ e $T_{\bar{\varepsilon}^{-1}c\varepsilon^{-1}}$, somente usando os fatos que se $\varepsilon \in A^*$, então $\bar{\varepsilon}$ também é uma unidade e a definição do subgrupo Γ de A . Para a verificação destas identidades, basta aplicar cada lado da igualdade nos elementos u , v , e $z \in N$ separadamente.

(6) Nesta igualdade observamos que para todo $\varphi \in \mathcal{U}(M)$, temos que $\varphi(u)$ e $\varphi(v)$ formam um par hiperbólico de M e, conseqüentemente, M tem uma decomposição da forma $\varphi(\mathbb{H}) \perp \varphi(N)$. Mais ainda, desde que $[q](\varphi(x)) = [q](x)$, temos que $a \in [q](\varphi(x))$ para todo $a \in [q](x)$. Logo tem sentido a definição de $E_{\varphi(u),a,\varphi(x)}$ para toda $\varphi \in \mathcal{U}(M)$. A igualdade é verificada de maneira análoga às anteriores.

(7) Esta igualdade verifica-se utilizando a identidade (2) e aplicando separadamente em u , v , e $z \in N$.

(8) Aqui observamos que $x + y \in N$, para todo $x, y \in N$, $c = k(y, x) - \lambda\overline{k(y, x)} \in \Gamma_{min} \subseteq \Gamma$ e se $a \in [q](x)$ e $a' \in [q](y)$, então $a \equiv k(x, x) \pmod{\Gamma}$ e $a' \equiv k(y, y) \pmod{\Gamma}$. Logo $a + a' + \langle x, y \rangle \equiv k(x + y, x + y) \pmod{\Gamma}$, ou seja, $a + a' + \langle x, y \rangle \in [q](x + y)$. Conseqüentemente, tem sentido definir $E_{u,a+a'+\langle x,y \rangle,x+y}$ e $T_c(u)$. Agora, é fácil ver que

$$E_{u,a,x}E_{u,a',y}(u) = E_{u,a+a'+\langle x,y \rangle,x+y}(u) = E_{u,k(x+y,x+y),x+y}T_c(u)(u) = u.$$

Aplicando estas 3 isometrias em v , obteremos todos os resultados iguais a $v - (x + y)\bar{\lambda} - u\bar{\lambda}(a + a' + \langle x, y \rangle)$. Finalmente, aplicando estas isometrias em um elemento $z \in N$, obteremos $z + u\langle x + y, z \rangle$ em todos os casos, o que mostra as igualdades de (8).

(9) Nesta observamos que $[q](x) = [q](-x)$, $\langle x, x \rangle - a \in [q](x)$ e $c = a - \lambda\bar{a} \in$

$\Gamma_{min} \subseteq \Gamma$. Para verificar as igualdades, basta aplicarmos (8).

(10) Desde que $\langle x, y \rangle = \lambda \overline{\langle y, x \rangle} \equiv \langle y, x \rangle \pmod{\Gamma}$, temos que $c = \langle y, x \rangle - \langle x, y \rangle \in \Gamma$. A igualdade é verificada usando (8) e (9).

(11) Se $a \in [q](x)$, ou seja, $a \equiv k(x, x) \pmod{\Gamma}$, então $ra\bar{r} \equiv k(x\bar{r}, x\bar{r}) \pmod{\Gamma}$, para todo $r \in A$. Novamente a igualdade se verifica aplicando-se separadamente os dois lados nos elementos u, v e $z \in N$.

(12) Segue de (6) e (11) para $\varphi = \phi(\varepsilon) \in \mathcal{U}(M)$.

(13) Usando que $E_{v,a,x} = \Delta E_{u,a,x} \Delta^{-1}$, (6) e (11) esta igualdade segue.

Se A é comutativo, $\lambda = 1$, a involução é trivial sobre A , ou seja, no caso comutativo, e $\Gamma = \{0\}$, então $(M, [k])$ é o espaço quadrático (M, q) , $M = \mathbb{H} \perp N$, $\{u, v\}$ é uma base de $\mathbb{H}$ com $q(u) = q(v) = 0$, $b_q(u, v) = 1$ e $\dim_A N \geq 1$.

Neste caso, o grupo unitário das isometrias de (M, q) é denominado o *grupo ortogonal* de (M, q) e denotado por $\mathcal{O}(M, q)$, ou simplesmente por $\mathcal{O}(M)$.

Veamos agora, como se comportam as isometrias definidas anteriormente como elementos de $\mathcal{O}(M)$. Primeiramente observamos que, desde que $\Gamma = \{0\}$, então $T_c(u)$ e $T_c(v)$ são a isometria identidade de M . Nas isometrias $E_{u,a,x}$ e $E_{v,a,x}$, temos que $a \in [q](x) = q(x)$, assim omitiremos o índice a , ou seja, escreveremos somente $E_{u,x}$ e $E_{v,x}$.

As identidades citadas, com as observações acima, tornam-se:

$$(1)' \Delta \phi(\varepsilon) \Delta^{-1} = \phi(\varepsilon^{-1}) = \phi(\varepsilon)^{-1}.$$

$$(6)' \varphi E_{u,x} \varphi^{-1} = E_{\varphi(x), \varphi(x)}, \forall \varphi \in \mathcal{O}(M).$$

$$(8)' E_{u,x} E_{u,y} = E_{u,x+y}.$$

$$(9)' (E_{u,x})^{-1} = E_{u,-x}.$$

$$(10)' E_{u,x} E_{u,y} = E_{u,y} E_{u,x}.$$

$$(11)' E_{ur,x} = E_{u,xr}, \forall r \in A.$$

$$(12)' \phi(\varepsilon) E_{u,x} \phi(\varepsilon^{-1}) = E_{u,x\varepsilon}.$$

$$(13)' \phi(\varepsilon) E_{v,x} \phi(\varepsilon^{-1}) = E_{v,x\varepsilon^{-1}}.$$

3.2 Geradores de $\mathcal{U}(M)$ e $\mathcal{O}(M)$

Usando as isometrias apresentadas na seção anterior, nesta apresentaremos os geradores dos grupos $\mathcal{U}(M)$ e $\mathcal{O}(M)$.

Seja x um elemento unimodular de $(M, [k])$, isto é, $\langle M, x \rangle = A$. Escrevendo $x = u\alpha' + v\beta' + z'$, com $\alpha', \beta' \in A$, $z' \in N$, temos que

$$\langle M, u\alpha' + v\beta' + z' \rangle = \langle M, u \rangle \alpha' + \langle M, v \rangle \beta' + \langle M, z' \rangle = A,$$

ou seja, $A\alpha' + A\beta' + \langle N, z' \rangle = A$.

Dado $w \in N$ e $a \in [q](w)$ temos que

$$E_{u,a,w}(x) = E_{u,a,w}(u\alpha' + v\beta' + z') = u(\alpha' + \langle w, z' \rangle - \bar{\lambda}a\beta') + v\beta' + z' = u\alpha + v\beta' + z,$$

com $\alpha = \alpha' + \langle w, z' \rangle - \bar{\lambda}a\beta' \in A$.

Fixaremos uma base especial $\{x_1, \dots, x_n\}$ para N que existe pela **Prop.(2.7)**. Escrevendo $a_{ij} = \langle x_i, x_j \rangle$ e $k_{ij} = k(x_i, x_j)$, $1 \leq i, j \leq n$, temos $a_{ij} = k_{ij} + \lambda \bar{k}_{ji}$ e $a_{ij} = \lambda \bar{a}_{ji}$, $1 \leq i, j \leq n$. Para $w = \sum_{i=1}^n x_i w_i \in N$ temos

$$\begin{aligned} k(w, w) &= k\left(\sum_{i=1}^n x_i w_i, \sum_{i=1}^n x_i w_i\right) = \\ &= \sum_{i=1}^n \bar{w}_i k_{ii} w_i + \sum_{i < j} (\bar{w}_i k_{ij} w_j + \bar{w}_j k_{ji} w_i) \equiv \\ &\equiv \sum_{i=1}^n \bar{w}_i k_{ii} w_i + \sum_{i < j} \bar{w}_i (k_{ij} + \lambda \bar{k}_{ji}) w_j \pmod{\Gamma} \equiv \\ &\equiv \sum_{i=1}^n \bar{w}_i k_{ii} w_i + \sum_{i < j} \bar{w}_i a_{ij} w_j \pmod{\Gamma}. \end{aligned}$$

Assim,

$$k(w, w) \equiv \sum_{i=1}^n \bar{w}_i k_{ii} w_i + \sum_{i < j} \bar{w}_i a_{ij} w_j \pmod{\Gamma}.$$

Seja $a = \sum_{i=1}^n \bar{w}_i k_{ii} w_i + \sum_{i < j} \bar{w}_i a_{ij} w_j \in [q](w)$, onde $k_{ii} \in [q](x_i) \cap A^*$ se i é ímpar, que é possível desde que $\{x_1, x_2, \dots, x_n\}$ é uma base especial de N . Temos então:

$$(14) \quad \alpha = \alpha' + \sum_{i=1}^n \bar{w}_i \langle x_i, z' \rangle - \bar{\lambda} \sum_{i=1}^n \bar{w}_i k_{ii} w_i \beta' - \bar{\lambda} \sum_{i \leq j} \bar{w}_i a_{ij} w_j \beta',$$

com $A\alpha' + A \langle x_1, z' \rangle + \dots + A \langle x_n, z' \rangle + A\beta' = A$, pois x é unimodular.

Proposição 3.1 *Sejam $|A/\mathcal{M}| \geq 3$ e $x = u\alpha' + v\beta' + z'$, $\alpha', \beta' \in A$ e $z' \in N$ um elemento unimodular de M . Então existe $w \in N$ e $a \in [q](w)$ tal que o coeficiente de u em $E_{u,a,w}(x)$ é uma unidade de A .*

Dem.: É suficiente mostrar que existem $w_1, \dots, w_n \in A$ tais que $\alpha \in A^*$, onde α é como em (14), ou seja, desde que A é um anel local, existem $w_1, \dots, w_n \in A$ tais que $\alpha \notin \mathcal{M}$.

Se $\alpha' \notin \mathcal{M}$ tomando $w_i = 0$, para $i = 1, \dots, n$, temos $\alpha \in A^*$. Podemos então assumir que $\alpha' \in \mathcal{M}$. Se $\beta' \in \mathcal{M}$ então, da expressão $A\alpha' + A\beta' + \langle N, z' \rangle = A$ obtemos que x é um elemento unimodular de N , ou seja, $\langle x, N \rangle = A$, logo existe $i \in \{1, \dots, n\}$ tal que $\langle x_i, z' \rangle \notin \mathcal{M}$ e assim, tomando $w_i = 1$ e $w_j = 0$ para $j \neq i$, temos que $\alpha \in A^*$.

Agora, se $\beta' \notin \mathcal{M}$, desde que $k_{11} \in A^*$, tomando $w_i = 0$ para $1 < i \leq n$ em (14), obtemos

$$\alpha \equiv \overline{w_1} \langle x_1, z' \rangle - \overline{\lambda} \overline{w_1} k_{11} w_1 \beta' \pmod{\mathcal{M}}$$

Se $c_1 = \langle x_1, z' \rangle \in \mathcal{M}$, tomando $w_1 = 1$, temos $\alpha = \overline{\lambda} k_{11} \beta' \in A^*$ e se $c_1 \notin \mathcal{M}$, como $\alpha = \overline{w_1} (c_1 - \overline{\lambda} k_{11} w_1 \beta')$ e $|A/\mathcal{M}| \geq 3$ então existe $w_1 \in A$ tal que $w_1 \notin \mathcal{M}$ e $c_1 - \overline{\lambda} k_{11} w_1 \beta' \notin \mathcal{M}$. Assim, $\alpha \in A^*$. ■

O análogo a esta proposição para o caso comutativo é:

Proposição (3.1)' *Seja $x = u\alpha' + v\beta' + z'$, com $\alpha', \beta' \in A$ e $z' \in N$ um vetor unimodular de (M, q) , isto é, $b_q(x, M) = A$. Se $|A/\mathcal{M}| \geq 3$ ou x é isotrópico, então existe $w \in N$ tal que $E_{u,w}(x) = u\alpha + v\beta' + z$, com $\alpha \in A^*$ e $z \in N$.*

Dem.: Se $|A/\mathcal{M}| \geq 3$, então o resultado segue da **Prop.(3.1)**. Podemos então assumir que x é isotrópico. Assim, $0 = q(x) = \alpha'\beta' + q(z')$, ou seja, $q(z') = -\alpha'\beta'$. O coeficiente de u em $E_{u,w}(x)$ é

$$\alpha = \alpha' + b_q(w, z') - \beta' q(w).$$

Queremos encontrar $w \in N$ tal que $\alpha \in A^*$, isto é, $\alpha \notin \mathcal{M}$.

Se $\alpha' \in \mathcal{M}$, então $q(z') = -\alpha'\beta' \in \mathcal{M}$ e, consequentemente, $\tilde{z}' = z' \otimes \tilde{1}$ é um vetor isotrópico do espaço quadrático $(\tilde{N}, \tilde{q})$ sobre $\tilde{A} = A/\mathcal{M}$. Se $\tilde{z}' = \tilde{0}$, como $\alpha' \in \mathcal{M}$ e x é unimodular, temos que $\beta' \notin \mathcal{M}$. Mas $(\tilde{N}, \tilde{q})$ é não-singular sobre $\tilde{A}$, logo existe $w \in N$ tal que $\tilde{q}(\tilde{w}) \neq \tilde{0}$, ou seja, $q(w) \notin \mathcal{M}$. Consequentemente $\alpha \in A^*$ neste caso.

Finalmente, se $\tilde{z}' \neq \tilde{0}$, então $(\tilde{N}, \tilde{q})$ é um espaço isotrópico sobre $\tilde{A}$ e, da **Prop.(2.2)** existe $\tilde{w} \in \tilde{N}$ tal que $\tilde{z}'$ e $\tilde{w}$ formam um par hiperbólico de $\tilde{N}$, ou seja, $\tilde{q}(\tilde{w}) = 0$ e $b_{\tilde{q}}(\tilde{z}', \tilde{w}) = \tilde{1}$. Assim, existe $w \in N$ tal que $q(w) \in \mathcal{M}$ e $b_q(z', w) \notin \mathcal{M}$ e, consequentemente $\alpha \notin \mathcal{M}$ com queríamos. ■

Seja $\mathcal{E}(M)$ o subgrupo de $\mathcal{U}(M)$ gerado por todas as transvecções $E_{u,a,x}$ com $x \in N$ e $a \in [q](x)$. Da identidade (6) temos que $\mathcal{E}(M)$ é um subgrupo normal de $\mathcal{U}(M)$.

Seja I um ideal de A tal que $\bar{I} = I$, ou seja, I é invariante pela involução (em particular $\bar{I} = I$ implica que I é bilateral). Para tal ideal I , denotamos por $\mathcal{E}(M, I)$ o subgrupo normal de $\mathcal{U}(M)$ gerado pelas transvecções $E_{u,a,x}$ com $a \in [q](x)$ e $x \in N.I = \{\sum y_i a_i, y_i \in N, a_i \in I\}$. Observe que se $x \in N.I$ e $a \in [q](x)$, então $a \in I$. Mais ainda da equação (6), tomando $\varphi = \Delta \in \mathcal{U}(M)$, temos que $E_{u,a,x} \in \mathcal{E}(M, I)$, para todo $x \in N.I$ e $a \in q(x)$.

Para $\varphi \in \mathcal{U}(M)$, dizemos que $\varphi \equiv id_M(mod I)$ se $\varphi(x) \equiv x(mod I)$, ou seja $\varphi(x) - x \in M.I$ para todo $x \in M$. Consideremos

$$\mathcal{U}(M, I) = \{\varphi \in \mathcal{U}(M); \varphi \equiv id_M(mod I)\}.$$

Claramente $\mathcal{U}(M, I)$ é um subgrupo normal de $\mathcal{U}(M)$ e, mais ainda, $\mathcal{E}(M, I) \subseteq \mathcal{U}(M, I)$, pois $E_{u,a,x}(w) \equiv w(mod I)$, para todo $x \in N.I$, $a \in [q](x)$ e $w \in M$.

Seja $\mathcal{U}(\Gamma, I) = \{\varphi \in \mathcal{U}(M, I); \varphi \text{ fixa } N\}$.

Desde que $T_c(u) = E_{u,-c,0}$ para todo $c \in \Gamma$, temos $T_c(u) \in \mathcal{E}(M, I)$ para todo $c \in \Gamma \cap I$. Observe também que se $I = A$, então $\mathcal{U}(M, I) = \mathcal{U}(M)$ e $\mathcal{E}(M, I) = \mathcal{E}(M)$ e se $I = \{0\}$ temos que $\mathcal{U}(M, I) = \mathcal{E}(M, I) = \{id_M\}$.

Agora, se $M = M' \perp xA$ para algum elemento unimodular $x \in M$, então para cada unidade central $a \in A$ com $a\bar{a} = 1$, a aplicação linear $\tau_x^a(x) = xa$ e $\tau_x^a(z) = z$ para todo $x \in M'$, é uma isometria de M com $(\tau_x^a)^{-1} = \tau_x^{\bar{a}}$. Se $a = -1$, escrevemos τ_x ao invés de τ_x^a . Esta isometria é chamada uma *simetria* com respeito ao vetor x .

Se existe $a' \in [q](x) \cap A^*$ com $a' = \lambda\bar{a}'$, então τ_x é também dado pela fórmula

$$\tau_x(z) = z - xa'^{-1} \langle x, z \rangle, \forall z \in M.$$

Contudo, observemos que para a definição de τ_x não é necessário que xA seja um subespaço de M , ou seja, que $\langle x, x \rangle \in A^*$, mas somente que $[q](x) \cap A^* \neq \emptyset$.

Vejamos agora um lema que será necessário na demonstração do teorema de caracterização dos geradores de $\mathcal{U}(M, I)$.

No que segue, neste capítulo, assumiremos que $|A/\mathcal{M}| \geq 3$.

Lema 3.1 *Se $(M, [k])$ é um espaço unitário sobre (A, λ, Γ) com $\text{rank}_A(M) = 2$ e $\{x_1, x_2\}$ é uma base especial de M , então $[q](x_1 - x_2a_{11}) \cap A^* \neq \emptyset$, onde $a_{11} = \langle x_1, x_1 \rangle$.*

Dem.: Temos para $k_{ij} = k(x_i, x_j)$, $i = 1, 2$, que

$$\begin{aligned} [q](x_1 - x_2a_{11}) &\equiv k(x_1 - x_2a_{11}, x_1 - x_2a_{11})(\text{mod } \Gamma) \equiv \\ &\equiv k_{11} - k_{12}(k_{11} + \lambda\bar{k}_{11}) - (\overline{k_{11} + \lambda\bar{k}_{11}})k_{21} + \bar{a}_{11}k_{22}a_{11}(\text{mod } \Gamma) \equiv \\ &\equiv k_{11} - k_{12}k_{11} - \lambda k_{12}\bar{k}_{11} - \bar{k}_{11}(k_{21} + \lambda\bar{k}_{12}) + \bar{a}_{11}k_{22}a_{11}(\text{mod } \Gamma) \equiv \\ &\equiv -k_{12}k_{11} - \lambda k_{12}\bar{k}_{11} + k_{11} - \lambda\bar{k}_{11} + \bar{a}_{11}k_{22}a_{11}(\text{mod } \Gamma) \equiv \\ &\equiv -k_{12}k_{11} - \lambda k_{12}\bar{k}_{11} + \bar{a}_{11}k_{22}a_{11}(\text{mod } \Gamma) \equiv \\ &\equiv (k_{12} + \lambda\bar{k}_{21})(-k_{11}) + \bar{a}_{11}k_{22}a_{11}(\text{mod } \Gamma) \equiv \\ &\equiv -k_{11} + \bar{a}_{11}k_{22}a_{11}(\text{mod } \Gamma). \end{aligned}$$

Seja $k = \bar{a}_{11}k_{22}a_{11} - k_{11} \in [q](x_1 - x_2a_{11})$. Queremos mostrar que $k \equiv \gamma(\text{mod } \Gamma)$ para algum $\gamma \in A^*$. Para tanto é suficiente mostrarmos que $k \notin \mathcal{M}$.

Suponhamos que $k \in \mathcal{M}$ então $\bar{k} \in \mathcal{M}$ e $k + \lambda\bar{k} \in \mathcal{M}$. Assim, $(\bar{a}_{11}k_{22}a_{11} - k_{11}) + \lambda(\bar{a}_{11}k_{22}a_{11} - \bar{k}_{11}) = (\bar{a}_{11}k_{22}a_{11} - k_{11}) + \lambda(\bar{a}_{11}k_{22}a_{11} - \bar{k}_{11}) = \bar{a}_{11}(k_{22} + \lambda\bar{k}_{22})a_{11} - a_{11} = (\bar{a}_{11}a_{22} - 1)a_{11} \in \mathcal{M}$. Logo $a_{11} \in \mathcal{M}$, pois $\bar{a}_{11}a_{22} - 1 \in A^*$.

Como $k \in \mathcal{M}$ e $a_{11} \in \mathcal{M}$ então do fato de $k = \overline{a_{11}}k_{22}a_{11} - k_{11}$ temos que $k_{11} \in \mathcal{M}$ o que é uma contradição, pois $\{x_1, x_2\}$ é uma base especial de M . Portanto $k \equiv \gamma(\text{mod } \Gamma)$ para algum $\gamma \in A^*$ como queríamos. ■

Teorema 3.1 *Seja $(M, [k])$ um espaço unitário sobre (A, λ, Γ) como assumido no início do capítulo. Então $\mathcal{U}(M, I)$ é gerado por $\mathcal{U}(\mathbb{H}, I)$ e $\mathcal{E}(M, I)$.*

Dem.: Fixemos $\{x_1, \dots, x_n\}$ uma base especial de N e $\{y_1, \dots, y_n\}$ sua base dual. Dado $\varphi \in \mathcal{U}(M, I)$, existe $m \geq 1$ tal que $\varphi(x_i) = x_i$ para $1 \leq i \leq m-1$ (se $\varphi(x_1) \neq x_1$ tomamos $m = 1$).

Desde que $\varphi \equiv \text{id}(\text{mod } I)$, podemos escrever

$$\varphi(x_m) = u\alpha' + v\beta' + z',$$

onde $\alpha', \beta' \in I$ e $z' \equiv x_m(\text{mod } I)$.

Afirmamos que existe $w \in N$, $a \in [q](w)$ tal que

- (i) $E_{u,a,w}\varphi(x_m) = u\alpha + v\beta' + z$, com $\alpha \in A^*$, $\alpha \equiv \langle w, z' \rangle (\text{mod } I)$ e $z \equiv x_m(\text{mod } I)$
- (ii) se $m > 1$ então $E_{u,a,w}(x_i) = x_i$ para $1 \leq i \leq m-1$.

Para provarmos esta afirmação consideraremos os casos m par e m ímpar separadamente.

Caso 1: m ímpar. Se $m > 1$, então $N = N_0 \perp N_0^\perp$ onde N_0 é o subespaço unitário de N gerado por $\{x_1, \dots, x_{m-1}\}$.

Desde que $\langle x_i, \varphi(x_m) \rangle = 0$ para $1 \leq i \leq m-1$, temos que $z' \in N_0^\perp$. Assim, como $\varphi(x_m)$ é um elemento unimodular de $M_0 = \mathbb{H} \perp N_0^\perp$ (pois x_m é um elemento unimodular de M_0), pela **Prop(3.1)** existe $w \in N_0^\perp \subseteq N$ e $a \in [q](w)$ satisfazendo (i) e, como $m > 1$, então $E_{u,a,w}(x_i) = x_i$ para $1 \leq i \leq m-1$, pois $w \in N_0^\perp$. Se $m = 1$ a afirmação segue diretamente da **Prop.(3.1)**.

Caso 2: m par. Neste caso, podemos escrever $N = N_1 \perp N_1^\perp$, onde N_1 é o subespaço unitário de N gerado por $\{x_{m-1}, x_m, \dots, x_n\}$ e $z' \in N_1$, pois $\langle x_i, z' \rangle = \langle x_i, u\alpha' + v\beta' + z' \rangle = \langle x_i, \varphi(x_m) \rangle = \langle x_i, x_m \rangle = 0$, $1 \leq i \leq m-2$.

Agora, é suficiente encontrar $w \in N_1$, $a \in [q](w)$, tal que $\alpha = \alpha' + \langle w, z' \rangle - \bar{\lambda}a\beta' \in A^*$ e $\langle x_{m-1}, w \rangle = 0$.

Escrevendo $w = \sum_{i=m-1}^n x_i w_i$ e tomando $w_{m+1} = \dots = w_n = 0$, podemos assumir que $m = 2$, isto é, $N_1 = x_1 A \oplus x_2 A$ com $\langle x_1, x_2 \rangle = 1$, $k_{11} \in [q](x_1) \cap A^*$ e $(\lambda - a_{11}a_{22}) \in A^*$ onde $a_{ii} = \langle x_i, x_i \rangle$, $i = 1, 2$, pois $\{x_1, x_2\}$ é uma base especial de N_1 .

Desde que queremos $\langle x_1, w \rangle = 0$, temos que $w = (x_1 - x_2 a_{11})w_1$ e assim $[q](w) = \bar{w}_1[q](x_1 - x_2 a_{11})w_1$.

Seja $a' \in [q](x_1 - x_2 a_{11}) \cap A^*$, que existe pelo **Lema(3.1)**. Agora, segue do fato de $\langle x_1, z' \rangle = \langle x_1, \varphi(x_2) \rangle = 1$ que $z' = x_1 z_1 + x_2(1 - a_{11}z_1)$ para algum $z_1 \in A$ e, consequentemente, $\langle w, z' \rangle = \bar{w}_1(1 - \bar{a}_{11}a_{22})(1 - a_{11}z_1)$. Nestas condições temos

$$\alpha = \alpha' + \bar{w}_1 c - \bar{\lambda} \bar{w}_1 a' w_1 \beta',$$

onde $c = (1 - \bar{a}_{11}a_{22})(1 - a_{11}z_1) \in A$ e $a' \in [q](x_1 - x_2 a_{11}) \cap A^*$.

Observe que a condição $\varphi(x_2)$ unimodular, implica que α', c e β' não pertencem a $\mathcal{M}$ simultaneamente. Pois caso contrário, se $c \in \mathcal{M}$, então desde que $1 - \bar{a}_{11}a_{22} \in A^*$, temos que $1 - a_{11}z_1 \in \mathcal{M}$, ou seja $a_{11}z_1 \equiv 1 \pmod{\mathcal{M}}$. Mais ainda $a_{22} = \langle x_2, x_2 \rangle = \langle \varphi(x_2), \varphi(x_2) \rangle \equiv \langle z', z' \rangle \pmod{\mathcal{M}}$ pois $\alpha', \beta' \in \mathcal{M}$. Mas $\langle z', z' \rangle = \bar{z}_1 a_{11} z_1 + \bar{z}_1(1 - a_{11}z_1) + (\bar{1} - \bar{a}_{11}z_1)a_{21}z_1 + (\bar{1} - \bar{a}_{11}z_1)a_{22}(1 - a_{11}z_1) \equiv \bar{z}_1 a_{11} z_1 \pmod{\mathcal{M}}$, ou seja, $\langle z', z' \rangle \equiv \bar{z}_1 \pmod{\mathcal{M}}$ e, como $\langle z', z' \rangle = \lambda \overline{\langle z', z' \rangle}$, temos $a_{22} \equiv \lambda z_1 \pmod{\mathcal{M}}$. Assim $a_{11}a_{22} \equiv \lambda a_{11}z_1 \pmod{\mathcal{M}}$, ou seja $\lambda - a_{11}a_{22} \in \mathcal{M}$ o que é uma contradição pois $\lambda - a_{11}a_{22} \in A^*$. Logo α', c e β' não estão em $\mathcal{M}$ simultaneamente e, podemos mostrar que $\alpha \in A^*$ como na demonstração da **Prop.(3.1)**. Isto completa a demonstração da afirmação.

Temos então $w \in N$ e $a \in [q](w)$ tal que $E_{u,a,w}\varphi(x_m) = u\alpha + v\beta' + z$, com $\alpha \in A^*$, $z = z' - \bar{\lambda}w\beta'$ (ou seja $z \equiv x_m \pmod{I}$) e $E_{u,a,w}\varphi$ fixa $x_1, \dots, x_{m-1}$ se $m > 1$.

Agora $\langle w, x_m \rangle - \alpha \equiv \langle w, x_m \rangle - \alpha' - \langle w, z' \rangle + \bar{\lambda}a\beta' \equiv \langle w, x_m - z' \rangle \equiv 0 \pmod{I}$. Tomando $a_1 \in [q]((z - x_m)\alpha^{-1})$, temos que $E_{v,a_1,(z-x_m)\alpha^{-1}} \in \mathcal{E}(M, I)$ e

$$E_{v,a_1,(z-x_m)\alpha^{-1}} E_{u,a,w}\varphi(x_m) = u\alpha + v\beta + x_m,$$

com $\beta = \beta' + \langle (z - x_m)\alpha', z \rangle - a_1\alpha \in I$. Observe que $\beta\alpha^{-1} \in I$. Para $\sigma = E_{v,a_1,(z-x_m)\alpha^{-1}}E_{u,a,w}\varphi \in \mathcal{U}(M, I)$, temos $\sigma(x_m) = u\alpha + v\beta + x_m$, logo $[q](\sigma(x_m)) = [q](x_m)$, o que implica que $\bar{\alpha}\beta + k(x_m, x_m) \equiv k(x_m, x_m)(\text{mod } \Gamma)$, isto é, $\bar{\alpha}\beta \in \Gamma$. Para $\bar{\alpha}^{-1} \in A^*$, temos $\beta\alpha^{-1} = \bar{\alpha}^{-1}(\bar{\alpha}\beta)\alpha^{-1} \in \Gamma$. Assim $\beta\alpha^{-1} \in I \cap \Gamma$.

Tomando $c = \beta\alpha^{-1} \in I \cap \Gamma$, temos $E_{v,c,0} \in \mathcal{E}(M, I)$ e $E_{v,c,0}\sigma(x_m) = u\alpha + x_m$.

Seja $a_2 \in [q](y_m(\overline{\langle w, x_m \rangle - \alpha}))$. Desde que $\langle w, x_m \rangle \equiv \alpha(\text{mod } I)$, temos que $a_2 \in I$ e $E_{u,a_2,y_m(\overline{\langle w, x_m \rangle - \alpha})} \in \mathcal{E}(M, I)$. Temos então que

$$\psi_m = (E_{u,a,w})^{-1}E_{u,a_2,y_m(\overline{\langle w, x_m \rangle - \alpha})}E_{v,c,0}E_{v,a_1,(z-x_m)\alpha^{-1}}E_{u,a,w}$$

é uma isometria de $(M, [k])$ tal que, em sua expressão, todos os fatores a menos de $E_{u,a,w}$ e $(E_{u,a,w})^{-1}$ estão em $\mathcal{E}(M, I)$ que é um subgrupo normal de $\mathcal{U}(M, I)$. Portanto $\psi_m \in \mathcal{E}(M, I)$ e, além disso, $\psi_m\varphi(x_m) = x_m$. Mais ainda, com alguns cálculos mostra-se que $\psi_m\varphi$ fixa $x_1, \dots, x_{m-1}$.

Finalmente, usando indução sobre m , concluímos que existe $\psi \in \mathcal{E}(M, I)$ tal que $\psi\varphi$ fixa $x_1, \dots, x_n$. Consequentemente $\psi\varphi \in \mathcal{U}(\mathbb{H}, I)$, o que mostra o teorema. ■

No próximo teorema tentamos dar uma caracterização melhor dos geradores de $\mathcal{U}(M, I)$. Para tanto consideremos

$$\Phi(M, I) = \{\phi(\varepsilon); \varepsilon \in A^* \text{ com } \varepsilon \equiv 1(\text{mod } I)\}.$$

Teorema 3.2 *Sejam (A, λ, Γ) e $(M, [k])$ como no Teo.(3.1). Então $\mathcal{U}(M, I)$ é gerado por $\mathcal{E}(M, I)$, $\Phi(M, I)$ e as isometrias $\theta \in \mathcal{U}(M, I)$, tais que θ é a identidade em $\mathbb{H} \perp (x_1A + \dots + x_{n-1}A)$.*

Dem.: Seja $\varphi \in \mathcal{U}(M, I)$. Do Teo.(3.1) existe $\psi \in \mathcal{E}(M, I)$ tal que $\psi\varphi$ é a identidade em N . Consequentemente, $\psi\varphi(\mathbb{H}) \subseteq \mathbb{H}$ pois

$$\langle \psi\varphi(ua + vb), x_i \rangle = \langle \psi\varphi(ua + vb), \psi\varphi(x_i) \rangle = \langle ua + vb, x_i \rangle = 0.$$

Podemos então escrever $\psi\varphi(u) = u\alpha' + v\beta'$, com $\alpha' \equiv 1(\text{mod } I)$ e $\beta' \in I$.

Se n é ímpar, $\psi\varphi(u)$ é um elemento unimodular de $\mathbb{H} \perp x_n A$, onde $a_{nn} = \langle x_n, x_n \rangle \in A^*$. Pela **Prop.(3.1)** existe $w \in x_n A$ e $a \in [q](w)$ tal que $E_{u,a,w}\psi\varphi(u) = u\alpha + v\beta' - \bar{\lambda}w\beta'$ com $\alpha \in A^*$, onde $\alpha = \alpha' - \bar{\lambda}a\beta' \equiv 1(\text{mod } I)$.

Se n é par, $\psi\varphi(u)$ é um elemento unimodular de $\mathbb{H} \perp (x_{n-1}A \perp x_n A)$ onde $\{x_{n-1}, x_n\}$ é uma base especial de $(x_{n-1}A \oplus x_n A)$. Para simplificar a notação, assumimos $n = 2$. Tomando $w = x_1 w_1 + x_2 w_2$ com $\langle x_1, w \rangle = 0$, temos $w_2 = -a_{11}w_1$, e assim, $w = (x_1 - x_2 a_{11})w_1$.

Portanto $w = (x_1 - x_2 a_{11})w'$ para algum $w' \in A$. Para $a' \in [q](x_1 - x_2 a_{11}) \cap A^*$, que existe pelo **Lema(3.1)**, temos que

$$E_{u,a,x}\psi\varphi(u) = u\alpha + v\beta' - \bar{\lambda}w\beta',$$

onde $a = \bar{w}'a'w' \in [q](w)$ e $\alpha = \alpha' - \bar{\lambda}a\beta'$.

Desde que $a' \in A^*$ e como $\psi\varphi(x_2)$ é um elemento unimodular, temos que α' e β' não pertencem a $\mathcal{M}$ simultaneamente. Agora podemos encontrar $w' \in A$ tal que $\alpha \in A^*$, como na demonstração de **Prop.(3.1)**.

Assim, existe $w \in N$ e $a \in [q](w)$ tal que

$$E_{u,a,x}\psi\varphi(u) = u\alpha + v\beta' - \bar{\lambda}w\beta',$$

com $\alpha \in A^*$, $\alpha \equiv 1(\text{mod } I)$, $\beta' \in I$ e $\langle x_i, w \rangle = 0$ para $1 \leq i \leq n-1$.

Para $a_1 \in [q](-\bar{\lambda}w\beta')$, temos que $a_1 \in I$, $E_{v,a_1,-\bar{\lambda}w\beta'} \in \mathcal{E}(M, I)$ e

$$E_{v,a_1,-\bar{\lambda}w\beta'}E_{u,a,w}\psi\varphi(u) = u\alpha + v\beta,$$

para $\beta = \beta' + \bar{\beta}' \langle w, w \rangle \beta' - a_1 \alpha \in I$. Tomando $\sigma = E_{v,a_1,-\bar{\lambda}w\beta'}E_{u,a,w}\psi\varphi \in \mathcal{U}(M, I)$ e usando que $c = \beta\alpha^{-1} \in I \cap \Gamma$ temos que $E_{v,c,0} \in \mathcal{E}(M, I)$ e

$$\rho = (E_{u,aw})^{-1}E_{v,c,0}E_{v,a_1,-\bar{\lambda}w\beta'}E_{u,a,w}\psi \in \mathcal{E}(M, I).$$

Agora é fácil ver que $\phi(\alpha^{-1})\rho\phi$ fixa $u, x_1, \dots, x_{n-1}$.

Usando que $\phi(\alpha^{-1})\rho\phi(u) = u$ e $\langle u, v \rangle = 1$, podemos escrever

$$\phi(\alpha^{-1})\rho\phi(v) = u\gamma' + v + z,$$

com $\gamma' \in I$, $z \in N.I$ e $\langle x_i, z \rangle = 0$ para $i \leq i \leq n-1$.

Para $a_2 \in [q](\lambda z)$, temos que $a_2 \in I$, $E_{u,a_2,\lambda z} \in \mathcal{E}(M, I)$ e

$$E_{u,a_2,\lambda z}\phi(\alpha^{-1})\rho\phi(v) = u\gamma + v,$$

com $\gamma = \gamma' + \bar{\lambda} \langle z, z \rangle - \bar{\lambda}a_2 \in I$.

Novamente, usando que $E_{u,a_2,\lambda z}\phi(\alpha^{-1})\rho\phi \in \mathcal{U}(M, I)$ e, portanto preserva a forma quadrática $[q]$, obtemos que $\bar{\gamma} \in I \cap \Gamma$. Consequentemente $\lambda\gamma \equiv \bar{\gamma}(\text{mod } \Gamma)$ pertence à $I \cap \Gamma$. Assim $E_{u,\lambda\gamma,0} \in \mathcal{E}(M, I)$ e

$$E_{u,\lambda\gamma,0}E_{u,a_2,\lambda z}\phi(\alpha^{-1})\rho\phi(v) = v.$$

Desde que $\langle x_i, z \rangle = 0$ para $1 \leq i \leq n-1$, temos que

$$\theta = E_{u,\lambda\gamma,0}E_{u,a_2,\lambda z}\phi(\alpha^{-1})\rho\phi$$

é um elemento de $\mathcal{U}(M, I)$ que fixa $u, v, x_1, \dots, x_{n-1}$, o que prova o teorema. ■

No caso comutativo temos uma descrição mais detalhada dos geradores de $\mathcal{U}(M, I)$. Consideremos agora A um anel comutativo local, $\lambda = 1$, a involução trivial sobre A e $\Gamma = \{0\}$. Se I é um ideal de A , então temos o grupo correspondente à $\mathcal{U}(M, I)$,

$$\mathcal{O}(M, I) = \{\varphi \in \mathcal{O}(M); \varphi \equiv id_M(\text{mod } I)\}.$$

Analogamente temos o subgrupo normal de $\mathcal{O}(M)$ gerado pelas transvecções $E_{u,x}$ com $x \in N.I$ e o subgrupo $\mathcal{O}(\mathbb{H}, I) = \{\varphi \in \mathcal{O}(M, I); \varphi \text{ fixa } N\}$.

Se $M = M' \perp Ax$, para algum elemento unimodular x de M , então para todo $a \in A^*$ tal que $a^2 = 1$, temos a simetria $\tau_x^a(x) = xa$ e $\tau_x^a(z) = z$ para todo $z \in M'$. Se $a = -1$, então τ_x^a coincide com a simetria dada pela fórmula

$$\tau_x(z) = z - b_q(x, z)q(x)^{-1}x;$$

para todo $z \in M$. Observemos novamente que na definição de τ_x , necessitamos somente de $q(x) \in A^*$ e não $b_q(x, x) \in A^*$.

Denotamos por $\mu_2(M_x)$ o conjunto de todas as simetrias de M com respeito a um vetor x fixado. É imediato que $\mu_2(M_x)$ é um subgrupo de $\mathcal{O}(M)$ naturalmente isomorfo ao grupo das raízes quadráticas de 1, $\mu_2(A) = \{x \in A; x^2 = 1\}$, pois $\tau_x^a \tau_x^c = \tau_x^{ac}$ para todo $a, c \in \mu_2(A)$. Mais ainda,

$$\mu_2(M_x, I) = \{\tau_x^a \in \mu_2(M_x); a \equiv 1(\text{mod } I)\}$$

é um subgrupo de $\mathcal{O}(M, I)$.

Para uma melhor descrição dos geradores de $\mathcal{O}(M, I)$, introduziremos outra classe de isometrias de (M, q) .

Se $M = \mathbb{H} \perp N$ com $\dim_A N \geq 2$, então $N = (x_1 A \oplus x_2 A) \perp N'$ onde $\{x_1, x_2\}$ é uma base especial de $(x_1 A \oplus x_2 A, q)$. Para todo $e \in A$ com $e^2 = e$, definimos $\tau_{x_1 x_2}^e : M \rightarrow M$ por:

$$\begin{aligned}\tau_{x_1 x_2}^e(x_1) &= x_1 \\ \tau_{x_1 x_2}^e(x_2) &= eq(x_1)^{-1}x_1 + (1 - 2e)x_2 \\ \tau_{x_1 x_2}^e(z) &= z\end{aligned}$$

para todo $z \in \mathbb{H} \perp N'$. Usando que $e^2 = e$, com alguns cálculos mostra-se que $\tau_{x_1 x_2}^e \in \mathcal{O}(M)$.

Consideremos agora $\mathcal{I}_p(A) = \{e \in A; e^2 = e\}$. Com a operação $e * e' = e + e' - 2ee'$, para todo $e, e' \in \mathcal{I}_p(A)$, temos que $\mathcal{I}_p(A)$ é um grupo abeliano onde o elemento neutro é o 0(zero) e, $e^{-1} = e$, para todo $e \in \mathcal{I}_p(A)$.

Agora é fácil ver que $\mathcal{I}_p(M_{x_1 x_2}) = \{\tau_{x_1 x_2}^e; e \in \mathcal{I}_p(A)\}$ é um subgrupo de $\mathcal{O}(M)$ naturalmente isomorfo a $\mathcal{I}_p(A)$, pois $\tau_{x_1 x_2}^e \tau_{x_1 x_2}^{e'} = \tau_{x_1 x_2}^{e * e'}$, para todo $e, e' \in \mathcal{I}_p(A)$. Mais ainda, se $2 \in A^*$, então os subgrupos $\mathcal{I}_p(M_{x_1 x_2})$ e $\mu_2(M_x)$, com $x = x_1 - 2q(x_1)x_2$ são isomorfos, com o isomorfismo dado por $\tau_{x_1 x_2}^e \mapsto \tau_x^{(1-2e)}$. Claramente

$$\mathcal{I}_p(M_{x_1 x_2}, I) = \{\tau_{x_1 x_2}^e \in \mathcal{I}_p(M_{x_1 x_2}); e \in I\}$$

é um subgrupo de $\mathcal{O}(M, I)$.

É fácil ver que se $I = \{0\}$ então $\mathcal{O}(M, I) = \mathcal{E}(M, I) = \Phi(M, I) = \mu_2(M_x, I) = \mathcal{I}_p(M_{x_1x_2}, I) = \{id_M\}$ e, se $I = A$ temos $\mathcal{O}(M, I) = \mathcal{O}(M)$, $\mathcal{E}(M, I) = \mathcal{E}(M)$, $\Phi(M, I) = \Phi(M)$, $\mu_2(M_x, I) = \mu_2(M_x)$ e $\mathcal{I}_p(M_{x_1x_2}, I) = \mathcal{I}_p(M_{x_1x_2})$.

Com estas novas isometrias e notações, temos o teorema correspondente ao **Teo. (3.2)** para o caso comutativo.

Teorema (3.2)' *Seja I um ideal do anel local A e assumamos que $|A/I| \geq 3$. Se (M, q) é um espaço quadrático sobre A com $M = \mathbb{H} \perp N$, onde $n = \dim_A N \geq 1$, então temos que $\mathcal{O}(M, I)$ é gerado por $\mathcal{E}(M, I)$, $\Phi(M, I)$ e $\mathcal{I}_p(M_{x_{n-1}x_n}, I)$ se n é par e $\mathcal{E}(M, I)$, $\Phi(M, I)$ e $\mu_2(M_{x_n}, I)$ se n é ímpar.*

Dem.: Seja $\varphi \in \mathcal{O}(M, I)$. Do **Teo. (3.2)** existe ψ que pertence ao subgrupo gerado por $\mathcal{E}(M, I)$ e $\Phi(M, I)$ tal que $\psi\varphi$ fixa u, v se $n = 1$ e fixa $u, v, x_1, \dots, x_{n-1}$ se $n > 1$. Separamos em 2 casos:

Caso 1: n ímpar. Neste caso $N = N' \perp x_n A$ com $q(x_n)b_q(x_n, x_n) \in A^*$ e $\psi\varphi$ é a identidade em $\mathbb{H} \perp N'$. Desde que $b_q(z, x_n) = 0$ e $\psi\varphi(z) = z$ para todo $z \in \mathbb{H} \perp N'$, temos que $\psi\varphi(x_n) = x_n a$ para algum $a \in A$, com $a \equiv 1 \pmod{I}$. Mais ainda, $q(x_n) = q(\psi\varphi(x_n)) = q(x_n a) = q(x_n)a^2$ com $q(x_n) \in A^*$. Então $a^2 = 1$, ou seja $\psi\varphi = \tau_{x_n}^a \in \mu_2(M_{x_n}, I)$.

Caso 2: n par. Agora $N = N_1 \perp (x_{n-1}A \oplus x_n A)$ com $q(x_{n-1})(1 - 4q(x_{n-1})q(x_n)) \in A^*$, $\psi\varphi$ é a identidade em $\mathbb{H} \perp N_1$ e $\psi\varphi(x_{n-1}) = x_{n-1}$. Como $b_q(z, x_n) = 0$ e $\psi\varphi(z) = z$ para todo $z \in \mathbb{H} \perp N_1$, temos que $\psi\varphi(x_n) = ax_{n-1} + a'x_n$, para $a, a' \in A$ com $a' \equiv 1 \pmod{I}$ e $a \in I$.

Mas $b_q(x_{n-1}, x_n) = 1$, o que implica que $1 = b_q(x_{n-1}, \psi\varphi(x_n)) = 2aq(x_{n-1}) + a'$, ou seja $a' = 1 - 2aq(x_{n-1})$.

Da igualdade $q(x_n) = q(\psi\varphi(x_n))$, obtemos $(1 - aq(x_{n-1}))a(1 - 4q(x_{n-1})q(x_n)) = 0$. Como $(1 - 4q(x_{n-1})q(x_n)) \in A^*$, temos que $a = a^2q(x_{n-1})$. Assim $(aq(x_{n-1}))^2 = a^2q(x_{n-1})^2 = aq(x_{n-1})$, ou seja, $aq(x_{n-1}) \in I_p(A)$. Tomando $e = aq(x_{n-1})$, temos que

$eq(x_{n-1})^{-1} = a$ e $\psi\varphi(x_n) = eq(x_{n-1})^{-1}x_{n-1} + (1 - 2e)x_n = \tau_{x_{n-1}x_n}^e(x_n)$. Finalmente $e = aq(x_{n-1}) \in I$, pois $a \in I$, o que mostra que $\tau_{x_{n-1}x_n}^e \in \mathcal{I}_p(M_{x_{n-1}x_n}, I)$ como queríamos. ■

Bibliografia

- [1] BAEZA, R., *Quadratic Forms Over Semilocal Rings*, Lecture Notes in Mathematics, 1978.
- [2] DIAS, I., *On the Orthogonal Group over an LG-ring*, Communications in Algebra 19(2),(1991), 443-454.
- [3] DIAS, I., *Unitary Groups over Strongly Semilocal Rings*, Communications in Algebra 23(5),(1995), 1797-1814.
- [4] JAMES, D. G., *On the Structure of Orthogonal Groups over Local Rings*, Am. J. Math. (1973), 255-265.
- [5] JAMES, D. G., *Unitary Groups over Local Rings*, J. Algebra 52, (1978), 354-363.
- [6] KNUS, M. A., *Quadratic and Hermitian Forms over Rings*, A Series of Comp. Studies in Math.294, Springer-Verlag, Berlin-Heidelberg-New York, 1991.
- [7] LAM, T.Y., *A First Course in Noncommutative Rings*, Graduate Texts in Math. 131, Springer-Verlag, Heidelberg, New York, 1991.
- [8] MICALI, A. and VILLAMAYOR, O.E., *Sur les Algèbres de Clifford*, Ann. Scient.

Éc. Norm. Sup., t. 1, (1968), 271 - 304.

[9] SCHARLAU, W., *Quadratic and Hermitian Forms*, A Series of Comp. Studies in Math. 270, Springer-Verlag, Berlin-Heidelberg-New York, 1985.