FORMAS QUADRÁTICAS SOBRE CORPOS HILBERTIANOS

IRES DIAS

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E CIÊNCIA DA COMPUTAÇÃO

CAMPINAS - SÃO PAULO
BRASIL

FORMAS QUADRÁTICAS SOBRE CORPOS HILBERTIANOS

Este exemplar corresponde a redação final da tese defendida pela Srta. IRES DIAS e aprovado pela comissão julgadora.

Campinas, 21 de maio de 1984

Prof. Dr. ANTONIO PAQUES

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do título de "Mestre em Matemática.

Abril/1984

Ao meu filho Alexandre

Agradeço ao Prof.Dr. Antonio Paques pela orientação e estímulo recebido, ao Prof.Dr. Antonio José Engler pela ajuda na compreensão de alguns exemplos, aos meus pais pelo apoio e incentivo, ao CNPq e CAPES pelo custeio parcial de meus estudos de Pós-Graduação e, a todos aqueles que colaboraram para a realização deste trabalho, em especial à Candida e Junior.

ÍNDICE

INTRODUÇÃO

A noção de corpo hilbertiano foi introduzida pela primeira vez em 1967, por Fröhlich, para corpos de característica distinta de 2 , em seu artigo "Quadratic forms 'à la' local theory" [5]. Em 1981, Baeza [3], estendeu esta noção para corpos de característica 2. Estes corpos possuem uma propriedade que é comum aos corpos reais-fechados e aos corpos p-ádicos, qual seja: formas quadráticas sobre um corpo hilbertiano são classificadas segundo dimensão, invariante de Arf e invariante de Witt. Neste trabalho, nos baseamos nestes dois artigos, acima mencionados, e damos uma caracterização de corpo hilbertiano independentemente da característica. Na medida do possível, procuramos apresentar demonstrações independentes daquelas contidas nos referidos artigos.

No capítulo I, damos apenas as noções e resultados básicos da teoria de formas quadráticas, tais como o teorema da decomposição ortogonal e o Teorema do Cancelamento de Witt, necessários à compreensão dos demais capítulos.

No capítulo II, fazemos um estudo da álgebra de Clifford, de um espaço quadrático, e de seu centro, vizando determinar as condições sob as quais ela é uma álgebra central simples. Os resultados aí obtidos nos permitem definir os invariantes de Arf e de Witt.

No capítulo III, estudamos excencialmente as propriedades de uma álgebra do quatérnios de um corpo K, vista como elemento do grupo de Brauer Br(K). A noção de álgebra de quatérnios, vista desta forma, é uma generalização do conceito de símbolo de Hilbert definido para corpos locais.

No capítulo IV, estudamos os corpos hilbertianos propriamente ditos, bem como classificamos as formas quadráticas não singulares sobre tais corpos.

CAPÍTULO I

FORMAS QUADRÁTICAS

§ 1 - ESPAÇOS QUADRÁTICOS

(1.1) DEFINIÇÃO - Sejam K um corpo e E um K-espaço vetorial de dimensão finita sobre K. Uma aplicação $q : E \to K$ é uma *forma quadrática* sobre K se:

(i) $q(\lambda x) = \lambda^2 q(x)$, $\forall\, x \in E$ e $\lambda \in K$.

(ii) $b_q(x,y) = q(x+y) - q(x) - q(y)$, $x,y \in E$,

é uma forma bilinear simétrica de $E \times E$ em K.

O par (E,q) será chamado *espaço quadrático* sobre K. A dimensão do espaço vetorial E sobre K será também chamada a *dimensão da forma quadrática* q e denotada por $\dim q$.

Um espaço quadrático (E,q) sobre um corpo K (ou a forma quadrática q) é dito ser *não singular* se a aplicação $d : E \to E^* = \mathrm{Hom}(E,K)$ definida por $d(x)(y) = b_q(x,y)$, $x,y \in E$, é um isomorfismo de K-espaços vetoriais, ou, equivalentemente, se o determinante da matriz $n \times n$ $(b_q(e_i,e_j))$ é não nulo, onde $\{e_1,\ldots,e_n\}$ é uma base qualquer de E sobre K.

(1.2) EXEMPLOS

(1) Sejam $E = Ke$ e $q : E \to K$ dada por $q(e)=a$. O espaço quadrático (E,q) será também denotado, neste caso, simplesmente por $[a]$ e obviamente (E,q) é não singular se, e somente se,

$a \in \dot{K} = K - \{0\}$.

(2) Seja (E,q) um espaço quadrático sobre um corpo K, com $\dim_K E = 2$. Suponhamos que $E = Ke_1 \oplus Ke_2$ com $q(e_1)=a, q(e_2)=b$ e $b_q(e_1,e_2)=1$. Neste caso (E,q) é não singular se e somente se $\det\begin{pmatrix} 2a & 1 \\ 1 & 2b \end{pmatrix} = 1-4ab \in \dot{K}$. O espaço quadrático (E,q), neste caso, será também denotado por $[a,b]$. Se $a=b=0$, (E,q) será chamado *plano hiperbólico* e o denotaremos por $\mathbb{H}$.

Sejam (E,q) um espaço quadrático sobre um corpo K e $E^{\perp} = \{x \in E; b_q(x,y) = 0, \forall y \in E\}$ o *radical* de E. Observemos que (E,q) é não singular se e somente se $E^{\perp} = \{0\}$. Dizemos que (E,q) é um *espaço quadrático regular* (ou q é uma *forma quadrática regular*), se $\{x \in E^{\perp};\ q(x) = 0\} = \{0\}$.

(1.3) OBSERVAÇÃO - Se (E,q) é um espaço quadrático não singular sobre um corpo K, então (E,q) é regular. A recíproca não é verdadeira pois, se $E = Ke$, $q(e) \neq 0$ e característica de K é igual a 2(abreviadamente $\mathrm{car}(K)=2$) então (E,q) é regular e $E^{\perp} = E$.

(1.4) DEFINIÇÃO - Sejam (E,q) um espaço quadrático sobre um corpo K e $x \neq 0$ um elemento de E. Dizemos que x é *isotrópico* (em relação à q) se $q(x) = 0$ e *anisotrópico* caso contrário. Se (E,q) possue um vetor isotrópico dizemos que (E,q) é um *espaço quadrático isotrópico* (ou q é uma *forma quadrática isotrópica*). Caso contrário, dizemos que (E,q) é *anisotrópico* (ou q é *anisotrópica*).

(1.5) PROPOSIÇÃO - Seja (E,q) um espaço quadrático não singular isotrópico sobre um corpo K. Então (E,q) contém um plano hiperbólico.

<u>Dem.</u>- Seja $e_1 \in E$ um vetor isotrópico. Desde que (E,q) é não singular, existe $x \in E$ tal que $b_q(e_1,x) = 1$. Basta considerarmos $e_2 = -q(x)e_1 + x$ para obtermos $\mathbb{H} \subseteq E$. □

(1.6) COROLÁRIO - Se (E,q) é um K-espaço quadrático não singular isotrópico de dimensão 2, então $(E,q) = \mathbb{H}$.

<u>Dem.</u>-Imediata. □

Dizemos que uma forma quadrática q sobre um corpo K representa um elemento $d \in \dot{K}$, se existe $x \in E$ tal que $q(x)=d$. Denotaremos por $D(q)$ o conjunto dos elementos representados por q, ou seja, $D(q)= \{d \in \dot{K};\ \exists x \in E \text{ com } q(x) = d\}$.

(1.7) DEFINIÇÃO - Uma forma quadrática q sobre um corpo K será dita *universal* quando $D(q) = \dot{K}$.

(1.8) EXEMPLO - Todo espaço quadrático não singular isotrópico é universal.

(1.9) DEFINIÇÃO - Sejam (E_i,q_i), $i=1,2$, espaços quadráticos sobre um corpo K. Definimos a *soma ortogonal* dos espaços (E_1,q_1) e (E_2,q_2), a qual denotamos por $(E_1,q_1) \perp (E_2,q_2)$, como sendo o espaço quadrático $(E_1 \oplus E_2, q_1 \perp q_2)$, onde $q_1 \perp q_2(x_1+x_2) = q_1(x_1)+q_2(x_2)$ para $x_i \in E_i$, $i = 1,2$.

(1.10) TEOREMA - Seja (E,q) um espaço quadrático não singular sobre um corpo K. Então (E,q) admite uma decomposição ortogonal do tipo:

$(E,q) = [c_1]\perp\ldots\perp[c_m]$, se $car(K) \neq 2$,

ou $(E,q) = [a_1,b_1]\perp\ldots\perp[a_n,b_n]$, se $car(K) = 2$ com $b_i \in K$, a_i, c_j, $1 - 4a_ib_i \in \dot{K}$, $(1 \leq i \leq n;\ 1 \leq j \leq m)$.

Para demonstrarmos este teorema utilizaremos o seguinte resultado auxiliar:

(1.11) LEMA - Sejam (E,q) um espaço quadrático sobre um corpo K e $F \subseteq E$ um subespaço tal que $(F,q|_F)$ é um espaço quadrático não singular sobre K. Então $E = F \oplus F^\perp$, onde $F^\perp = \{x \in E;\ b_q(x,y) = 0,\ \forall y \in F\}$.

Dem. - Cada elemento $x \in E$ define um elemento $x^* \in F^*$ tal que $x^*(y) = b_q(x,y), \forall y \in F$. Desde que $(F,q|_F)$ é não singular a aplicação $d : F \to F^*$ definida por $d(z)(y) = b_q(z,y), \forall z,y \in F$ é um isomorfismo de K-espaços vetoriais. Logo existe $x_F \in F$ tal que $x^*=d(x_F)$, ou seja, $b_q(x,y)=b_q(x_F,y), \forall y \in F$, de onde segue-se que $x - x_F \in F^\perp$. Como todo elemento $x \in E$ pode ser escrito na forma $x = x_F+(x - x_F)$, concluimos que $E=F+F^\perp$. Ainda da hipótese de $(F,q|_F)$ ser não singular obtemos $F \cap F^\perp=\{0\}$ e portanto $E = F \oplus F^\perp$. □

Dem. de (1.10) - Primeiramente suponhamos que $car(K)\neq 2$. De (E,q) ser não singular segue-se que $D(q) \neq \emptyset$ e portanto existe $c_1 \in \dot{K}$ e $e_1 \in E$ tal que $q(e_1) = c_1$. O subespaço Ke_1 de E satisfaz as condições do lema (1.11) e, assim, podemos escrever $E = Ke_1 \oplus (Ke_1)^{\perp}$ ou ainda $(E,q) = [c_1] \perp (E_1,q_1)$, onde $E_1 = (Ke_1)^{\perp}$ e $q_1 = q|_{E_1}$.

Se $\dim_K E > 1$ então (E_1,q_1) é não singular (pois (E,q) o é), e por indução sobre $m = \dim q$ obtemos $(E,q) = [c_1] \perp \ldots \perp [c_m]$; $c_i \in \dot{K}$, $(1 \leq i \leq m)$.

Suponhamos agora que car(K) = 2. Novamente porque (E,q) é não singular existe $a_1 \in \dot{K}$ e $e_1, e_2 \in E$ tais que $q(e_1) = a_1$ e $b_q(e_1,e_2) = 1$. Evidentemente os elementos e_1 e e_2 são linearmente independentes sobre K e o subespaço $Ke_1 \oplus Ke_2$ satisfaz as condições do lema (1.11). Assim, se $q(e_2) = b_1$, podemos escrever $(E,q) = [a_1,b_1] \perp (E_1,q_1)$, onde $E_1 = ([a_1,b_1])^{\perp}$ e $q_1 = q|_{E_1}$. Repetindo o mesmo método recursivamente obteremos uma decomposição do tipo $(E,q) = [a_1,b_1] \perp \ldots \perp [a_n,b_n] \perp (E_n,q_n)$, onde $\dim q_n \leq 1$. A dimensão de q_n deve ser necessariamente igual a zero, pois caso contrário (E,q) seria singular. $\square$

Em tudo o que se seguirá, a soma ortogonal $[c_1] \perp \ldots \perp [c_n]$ será denotada simplesmente por $\langle c_1, \ldots, c_n \rangle$.

(1.12) DEFINIÇÃO - Sejam (E_i,q_i), $i = 1,2$, espaço quadráticos sobre um corpo K. Uma aplicação $\phi : E_1 \to E_2$ é dita ser uma *isometria* entre (E_1,q_1) e (E_2,q_2) se ϕ é um isomorfismo de K-espaços vetoriais tal que $q_2(\phi(x)) = q_1(x)$, para todo $x \in E_1$. Sempre que existir uma isometria entre dois espaços quadráticos (E_1,q_1) e (E_2,q_2), diremos que eles são *isométricos* e indicaremos $(E_1,q_1) \cong (E_2,q_2)$ ou simplesmente $q_1 \cong q_2$. Evidentemente espaços isométricos tem a mesma dimensão, ou seja, dimensão é *invarian-*

te por isometrias. Claramente, isometria é uma relação de equivalência definida sobre o conjunto dos espaços quadráticos não singulares sobre um corpo K, compatível com a soma ortogonal.

Dados $a \in \dot{K}$ e (E,q) um espaço quadrático sobre um corpo K, definimos sobre E a forma quadrática $\langle a \rangle q$, dada por $\langle a \rangle q(x) = aq(x)$ para todo $x \in E$. Indicaremos por $\langle a_1,\ldots,a_n\rangle q$, $a_i \in \dot{K}$, $1 \leq i \leq n$, a forma quadrática dada pela soma ortogonal $\langle a_1\rangle q \perp \ldots \perp \langle a_n\rangle q$. É fácil ver que quaisquer que sejam $a \in \dot{K}$ e $b \in K$ os espaços quadráticos $[a,b]$ e $\langle a\rangle[1,ab]$ são isométricos. Portanto toda soma ortogonal $[a_1,b_1]\perp\ldots\perp[a_n,b_n]$, com $a_i \in \dot{K}$, $1 \leq i \leq n$ pode ser escrito na forma $\langle a_1\rangle[1,c_1]\perp\ldots\perp\langle a_n\rangle[1,c_n]$ onde $c_i = a_i b_i$, $1 \leq i \leq n$.

(1.13) OBSERVAÇÕES -

(i) Sejam (E,q) um espaço quadrático não singular sobre um corpo K e $a \in D(q)$. Então (E,q) é isométrico à $(E,\langle a\rangle q)$.

(ii) Sobre um corpo de característica distinta de 2 o espaço quadrático $(E,q) = \langle 1,-1\rangle$ é hiperbólico. Evidentemente (E,q) é não singular. Logo, basta observarmos que $E = Ke_1 \oplus Ke_2$ com $q(e_1)=1, q(e_2)=-1$ $b_q(e_1,e_2)=0$, então $e_1 + e_2$ é um elemento isotrópico de (E,q) e o resultado segue-se pela proposição (1.5). Por um raciocínio análogo, dado um espaço quadrático não singular qualquer (E,q) sobre um corpo K, o espaço quadrático $\mathbb{H}(E) = (E,q)\perp(E,-q)$ é um soma ortogonal de planos hiperbólicos. Toda soma ortogonal de $n \geq 1$ planos hiperbólicos será chamada de *espaço hiperbólico* e indicada simplesmente por $n\mathbb{H}$. No caso do espaço (E,q) , $\mathbb{H}(E) = (\dim_K E)\,\mathbb{H}$.

§ 2 - TEOREMA DO CANCELAMENTO DE WITT

O teorema do cancelamento de Witt para espaços quadráticos não singulares sobre um corpo K, segue-se como um corolário do seguinte teorema:

(2.1) TEOREMA - Sejam (E,q) e (F,q') espaços quadráticos não singulares sobre um corpo K, com $F \subseteq E$ e $q'=q|_F$. Se $\phi : F \to E$ é uma aplicação K-linear tal que $q(\phi(x)) = q'(x)$ para todo $x \in F$, então existe uma isometria $\bar{\phi} : E \to E$ tal que $\bar{\phi}|_F = \phi$.

A demonstração deste teorema é baseado no seguinte resultado:

(2.2) LEMA - Seja (E,q) um espaço quadrático sobre um corpo K com $E = (Ke_1 \oplus Ke_2) \perp E_o$, onde $E_o \neq 0$ e $Ke_1 \oplus Ke_2$ é um plano hiperbólico. Então para qualquer plano hiperbólico $Kw_1 \oplus Kw_2 \subseteq E$, (isto é, $q(w_1) = q(w_2) = 0$ e $b_q(w_1,w_2)= 1$), existe uma isometria σ de E, tal que $\sigma(e_i) = w_i$, $i = 1,2$.

<u>Dem.</u> - Sejam (E,q) um espaço quadrático sobre um corpo K e x, $y \in E$ tais que $q(x) = b_q(x,y) = 0$. Com simples cálculo pode ser verificado que a aplicação $M(x,y) : E \to E$ dada por $M(x,y)(z)=z+b_q(z,x)y - b_q(z,y)x - q(y)b_q(z,x)x$, para todo $z \in E$, é uma isometria.

Escrevemos $w_1 = \alpha e_1 + \beta e_2 + u$, com $u \in E_o$ e $\alpha, \beta \in K$. De (E,q) não singular segue-se que podemos encontrar $z \in E_o$ tal que $b_q(z,u) + \beta q(z) \neq 0$. Assim usando a isometria acima podemos supor que $\alpha \neq 0$, pois $M(e_1,z)(w_1) = \alpha' e_1 + \beta' e_2 + u'$, com $\alpha' \neq 0$. Observemos que $q(w_1) = 0$ implica $\beta = -\alpha^{-1} q(u)$. Logo a isometria $M(e_2, \alpha^{-1} u)$ leva e_1 em $\alpha^{-1} w_1$.

Seja $P(\alpha): E \to E$ a aplicação dada por $P(\alpha)(e_1) = \alpha e_1$, $P(\alpha)(e_2) = \alpha^{-1} e_2$ e $P(\alpha)(z) = z, \forall z \in E_o$. A aplicação $P(\alpha)$ é uma isometria de E e a isometria $\sigma' = M(e_2, \alpha^{-1} u) \circ P(\alpha)$ leva e_1 em w_1. Agora, sejam $w = \sigma'(e_2)$, $E = (Kw_1 \oplus Kw) \perp E_1$ e $w_2 = \gamma w_1 + \lambda w + t$; $t \in E_1, \lambda, \gamma \in K$. Desde que $b_q(w_1, w) = 1$, temos $\lambda = 1$ e $q(t) = -\gamma$. Um simples cálculo mostra que $M(w_1,t)(w_1) = w_1$ e $M(w_1,t)(w) = w_2$. Consequentemente $\sigma = M(w_1,t) \circ \sigma'$ satisfaz o requerido.□

<u>Dem. de (2.1)</u> - Consideremos o espaço quadrático $(E,q) \perp (F,-q') = (F,q') \perp (F,-q') \perp F^{\perp} = \mathbb{H}(F) \perp F^{\perp}$. Cada aplicação K-linear $\phi: F \to E$ induz uma aplicação K-linear $\phi' : \mathbb{H}(F) \to (E,q) \perp (F,-q')$, com $\phi' = \phi \perp id_F$. Agora cada isometria $\bar{\Phi}'$ de $(E,q) \perp (F,-q')$ tal que $\bar{\Phi}'|_{\mathbb{H}(F)} = \phi'$ nos dá uma isometria $\bar{\Phi}$ de E tal que $\bar{\Phi}|_F = \phi$. Assim podemos supor que F é um espaço hiperbólico, ou seja, $F = (Ke_1 \oplus Kf_1) \perp \ldots \perp (Ke_n \oplus Kf_n)$, com $Ke_i \oplus Kf_i$ planos hiperbólicos, $1 \leq i \leq n$. De (2.2) segue-se que se $n=1$ existe $\sigma: E \to E$ isometria tal que $\sigma(e_1) = \phi(e_1)$ e $\sigma(f_1) = \phi(f_1)$, isto é, $\sigma|_F = \phi$. Assumiremos $n > 1$ e demonstraremos o resultado por indução sobre n.

Consideremos a restrição ϕ' de ϕ ao subespaço

$(Ke_1 \oplus Kf_1)\perp\ldots\perp(Ke_{n-1}\oplus Kf_{n-1})$. Por hipótese de indução existe uma isometria $\sigma: E \to E$ que estende ϕ'. Observemos que $\sigma^{-1} \circ \phi$: $: F \to E$ é uma aplicação linear que é a identidade em $(Ke_1 \oplus Kf_1)\perp\ldots\perp(Ke_{n-1}\oplus Kf_{n-1})$ e que $q(\sigma^{-1}\circ\phi(x)) = q'(x), \forall x \in$ $\in Ke_n \oplus Kf_n$. Assim $\sigma^{-1}\circ\phi$ induz uma aplicação linear de $Ke_n \oplus Kf_n$ em $((Ke_1 \oplus Kf_1)\perp\ldots\perp(Ke_{n-1}\oplus Kf_{n-1}))^{\perp}$, que, por hipótese de indução, pode ser estendida a uma isometria $\tau: E \to E$. Assim $\sigma \circ \tau : E \to E$ é uma isometria e $(\sigma\circ\tau)|_F = \phi$. □

(2.3) COROLÁRIO - (Teorema do Cancelamento de Witt) - Sejam $(E_i, q_i), i = 1,2,3$, espaços quadráticos não singulares sobre um corpo K. Se $(E_1,q_1)\perp(E_2,q_2)$ e $(E_1,q_1)\perp(E_3,q_3)$ são isométricos, então (E_2,q_2) e (E_3,q_3) também o são.

<u>Dem.</u> - Sejam $\lambda : E_1 \oplus E_2 \to E_1 \oplus E_3$ uma isometria dada e $i : E_1 \to E_1 \oplus E_2$ a inclusão natural. Tomaremos $\alpha = \lambda \circ i :$ $: E_1 \to E_1 \oplus E_3$ e estenderemos para uma isometria β de $E_1 \oplus E_3$ (cf.(2.1)). Entretanto $\gamma = \lambda^{-1} \circ \beta : E_1 \oplus E_3 \to E_1 \oplus E_2$ satisfaz $\gamma|_{E_1} = id_{E_1}$. Consequentemente $\gamma|_{E_3} : E_3 \to E_2$ é uma isometria.□

CAPÍTULO II

GRUPO DE BRAUER E ÁLGEBRAS DE CLIFFORD

§ 1 - ÁLGEBRAS CENTRAIS SIMPLES

Seja K um corpo. Por uma K-álgebra entenderemos sempre uma álgebra de dimensão finita sobre K, associativa, (não necessariamente comutativa), com elemento identidade. Todo homomorfismo de K-álgebras será suposto unitário (isto é, leva elemento identidade em elemento identidade). Um isomorfismo entre duas K-álgebras A e B será denotado simplesmente por $A \cong B$. O produto tensorial de duas K-álgebras será sempre considerado sobre K e indicado simplesmente por $\otimes$.

(1.1) DEFINIÇÃO - Dados uma K-álgebra A e um subconjunto não vazio S de A, o conjunto $C_A(S) = \{x \in A; xs=sx, \forall s \in S\}$ será chamado o *centralizador de* S *em* A. É imediato que $C_A(S)$ é uma subálgebra de A, qualquer que seja o subconjunto S. No caso específico em que $S = A$ a subálgebra $C_A(A)$ será chamada *centro* de A e a denotaremos por $Z(A)$. Quando $Z(A)=K$ diremos que A é uma *K-álgebra central*. Uma K-álgebra A que não possui ideais bilaterais próprios será chamada *simples*.

(1.2) EXEMPLOS

(1) A álgebra $M_n(K)$ das matrizes de ordem n a coeficientes

em um corpo K é uma K-álgebra central simples. Mais geralmente, se D é uma K-álgebra central com divisão então $M_n(D)$ é uma K-álgebra central simples.

(2) (Teorema de Wedderburn) (Ver [4] Teo.24.1)

(a) Se A é uma K-álgebra central simples, então existe uma K-álgebra central com divisão D tal que A é isomorfa à K-álgebra de matrizes $M_n(D)$.

(b) Dadas D e D', K-álgebras centrais com divisão, as K-álgebras de matrizes $M_n(D)$ e $M_m(D')$ são isomorfas se e somente se $n = m$ e as K-álgebras D e D' são isomorfas.

(1.3) TEOREMA - Sejam A e B álgebras sobre um corpo K.

(1) Se $A' \subseteq A$ e $B' \subseteq B$ são subálgebras, então $C_{A \otimes B}(A' \otimes B') = C_A(A') \otimes C_B(B')$. Em particular se A e B são centrais, então $A \otimes B$ também o é.

(2) Se A é central simples e B é simples, então $A \otimes B$ é simples. Em particular, se A e B são centrais simples, então $A \otimes B$ também o é.

Dem. - Em (1) a inclusão $C_A(A') \otimes C_B(B') \subseteq C_{A \otimes B}(A' \otimes B')$ é imediata. Mostraremos então que $C_{A \otimes B}(A' \otimes B') \subseteq C_A(A') \otimes C_B(B')$.

Consideremos $\{b_1, \ldots, b_n\}$ uma base de B sobre K e $c = \sum_{i=1}^{n} a_i \otimes b_i \in C_{A \otimes B}(A' \otimes B')$. Observemos que $(a' \otimes 1)\, c = c(a' \otimes 1)$, para todo $a' \in A'$, isto é $\sum_{i=1}^{n} a'a_i \otimes b_i = \sum_{i=1}^{n} a_i a' \otimes b_i$, o que implica que $\sum_{i=1}^{n} (a'a_i - a_i a')(1 \otimes b_i) = 0$. Da independência linear de $\{1 \otimes b_1, \ldots, 1 \otimes b_n\}$ sobre K, segue-se que $a'a_i = a_i a'$, ou seja $a_i \in C_A(A')$, $1 \leq i \leq n$, e consequentemente temos $c \in C_A(A') \otimes B$.

Considerando agora $\{a_1 \ldots, a_m\}$ uma base de A sobre K e escrevendo $c = \sum_{i=1}^{m} a_i \otimes b_i$; $b_i \in B$, da equação $(1 \otimes b')c =$ $= c(1 \otimes b')$; $b' \in B'$, obteremos, por um raciocínio análogo, $c \in A \otimes C_B(B')$. Portanto $c \in C_A(A') \otimes C_B(B')$ o que demonstra a igualdade pretendida.

Em particular, $Z(A \otimes B) = Z(A) \otimes Z(B)$ e, consequentemente, se A e B são centrais então $A \otimes B$ também o é e com isso demonstramos (1).

Sejam, agora, A uma K-álgebra central simples e B uma K-álgebra simples. Queremos mostrar que $A \otimes B$ é simples. Para tanto, dado um ideal bilateral não nulo I de $A \otimes B$ basta mostrarmos que $1 \otimes 1 \in I$. Observemos que um elemento z de I é da forma $z = \sum_{i=1}^{r} a_i \otimes b_i$; $a_i \in A$ e $b_i \in B$. Entre os elementos não nulos de I consideremos $z = \sum_{i=1}^{r} a_i \otimes b_i$ de tal forma que r seja o menor inteiro positivo possível.

Nossa primeira observação é que os a_i (e similarmente os b_i) são linearmente independentes sobre K pois, caso contrário, teríamos, com uma nova reenumeração, $a_1 = \sum_{i=2}^{s} \lambda_i a_i$; $\lambda_i \in K$. Assim a soma dos s primeiros termos de z seria $a_1 \otimes b_1 + \sum_{i=2}^{s} a_i \otimes b_i =$ $= \sum_{i=2}^{s} a_i \otimes (\lambda_i b_1 + b_i)$ e consequentemente $z = \sum_{i=2}^{s} a_i \otimes (\lambda_i b_1 + b_i) +$

$+\sum_{i=s+1}^{r} a_i \otimes b_i$, o que contradiz a minimalidade de r.

Nosso próximo passo é "fazer" $a_1 = 1$. Desde que $a_1 \neq 0$, Aa_1A é um ideal bilateral não nulo de A, e portanto $Aa_1A = A$, pois A é simples sobre K. Logo obtemos uma somatória finita $1 = \sum_j c_j a_1 d_j$, com $c_j, d_j \in A$ não nulos. Desde que $z = \sum_{i=1}^{r} a_i \otimes b_i \in$ $\in I$, então $c_j z d_j \in I$, para todo j e tomando-se a somatória em j obtemos um elemento de I $z_1 = \sum_j c_j z d_j = 1 \otimes b_1 + \sum_{i=2}^{r} a_i' \otimes b_i$, com $a_i' = \sum_j c_j a_i d_j$. O elemento z_1 é não nulo pois os b_i são linearmente independentes sobre K.

Notemos que na passagem de z para z_1 não alteramos os b_i. Agora, fazendo um raciocínio análogo para b_1 obteremos, através de z_1, um elemento não nulo de I da forma $z_2 =$ $= 1 \otimes 1 + \sum_{i=2}^{r} a_i' \otimes b_i'$, com $a_i' \in A$ e $b_i' \in B$ não nulos. Para todo $a \in A$ temos $az_2 - z_2 a \in I$, ou seja $\sum_{i=2}^{r} (aa_i' - a_i' a) \otimes b_i' \in I$. Assim, da minimalidade de r segue-se que $\sum_{i=2}^{r} (aa_i' - a_i' a) \otimes b_i' = 0$. É fácil ver que os b_i' (respectivamente os a_i') são linearmente independentes sobre K usando o fato de que os b_i (respectivamente os a_i) o são. Assim vemos que $a_i' \in Z(A) = K$, para $2 \leq$ $\leq i \leq r$. Consequentemente $r = 1$ e $z_2 = 1 \otimes 1 \in I$, como queríamos. Em particular, se A e B são K-álgebras centrais simples, então $A \otimes B$ também o é, o que demonstra (2).□

É nosso interesse agora classificar todas as K-álgebras centrais simples através de uma conveniente relação de similaridade e então introduzir uma estrutura de grupo no conjunto das classes de similaridades através do produto tensorial. Mais formalmente, procedemos como segue.

Sejam A e A' duas K-álgebras centrais simples. Dizemos que A é *similar* a A' se existem dois K-espaços vetoriais de dimensão finita, V e V', tais que $A \otimes \mathrm{End}(V) \cong A' \otimes \mathrm{End}(V')$, como K-álgebras, onde $\mathrm{End}(V)$ é a álgebra dos endomorfismos de V. Observemos que a álgebra dos endomorfismos de um K-espaço vetorial de dimensão finita V, é isomorfa à álgebra de matrizes $M_{\dim V}(K)$. É fácil ver que similaridade é uma relação de equivalência (para a transitividade usamos o fato que $\mathrm{End}(V \otimes V') \cong \mathrm{End}(V) \otimes \mathrm{End}(V')$).

A classe de equivalência de A será denotada por $[A]$ ou simplesmente por A quando não existir problema de notação. É imediato que a operação $[A_1] \cdot [A_2] = [A_1 \otimes A_2]$ está bem definida e que o conjunto das classes de similaridades de K-álgebras centrais simples forma um semigrupo multiplicativo, cujo elemento identidade é representado pela classe $[K]$. Denotaremos este semigrupo por $B_r(K)$.

(1.4) PROPOSIÇÃO E DEFINIÇÃO - Para qualquer K-álgebra A, seja A^{op} a álgebra oposta. Se A é uma K-álgebra central simples , então A^{op} também o é, e $A \otimes A^{op} \cong \mathrm{End}(A)$. Em particular, $B_r(K)$ é um grupo abeliano com $[A]^{-1} = [A^{op}]$ para qualquer K-álgebra central simples A. $Br(K)$ é chamado o *grupo de Brauer de* K.

<u>Dem.</u> - Lembremos que $A^{op} = \{a^{op};\ a \in A\}$, com as seguintes ope

rações: $a^{op}+b^{op} = (a+b)^{op}$, $\lambda a^{op} = (\lambda a)^{op}$ e $a^{op}\,b^{op} = (b\,a)^{op}$ é a álgebra oposta de A. Claramente vemos que $Z(A^{op}) = \{a^{op}; a \in Z(A)\}$ e consequentemente A^{op} é central se e somente se A o é. Se I é um ideal bilateral de A^{op}, então $\{a; a^{op} \in I\}$ é um ideal bilateral de A. Logo, se A é simples então A^{op} também o é.

Definimos agora a aplicação $\Theta : A \otimes A^{op} \to \mathrm{End}_K(A)$, dada por $\Theta(a \otimes b^{op})(c) = acb$; para quaisquer $a,b,c \in A$. É imediato que Θ é um homomorfismo de K-álgebras. Observemos que A e A^{op} são K-álgebras centrais simples. Consequentemente $A \otimes A^{op}$ também o é (cf.(1.3)), e portanto Θ é injetora. Desde que $\dim_K (A \otimes A^{op}) = (\dim_K A)^2 = \dim_K (M_{\dim_K A}(K)) = \dim_K(\mathrm{End}_K(A))$, concluímos que Θ é sobrejetora, isto é, Θ é um isomorfismo de K-álgebras centrais simples. Disto segue trivialmente que $B_r(K)$ é um grupo, necessariamente abeliano.$\square$

Do teorema de Wedderburn sabemos que qualquer K-álgebra central simples é da forma $M_n(D)$, onde D é uma K-álgebra central com divisão. Por outro lado, $M_n(D) \cong D \otimes M_n(K)$. Assim em $B_r(K)$ temos $[A] = [M_n(D)] = [D \otimes M_n(K)] = [D]$. Da unicidade da K-álgebra D, também assegurada pelo Teorema de Wedderburn, concluimos que os elementos de $B_r(K)$ estão em correspondência 1-1 com as classes de isomorfismos das K-álgebras centrais com divisão.

§ 2 - ÁLGEBRAS DE CLIFFORD

Antes de definirmos uma álgebra de Clifford daremos as noções de álgebra $\mathbb{Z}_2$-graduada e de produto tensorial de álgebras $\mathbb{Z}_2$-graduadas sobre um corpo K, o que nos será útil no que se seguirá.

(2.1) DEFINIÇÃO - Dado um corpo K, uma K-*álgebra* $\mathbb{Z}_2$-*graduada* A é uma K-álgebra que se decompõe numa soma direta do tipo $A = A_o \oplus A_1$, onde A_o e A_1 são K-espaços vetoriais tais que $K \subseteq A_o$ e $A_iA_j = A_{i+j(\mathrm{mod}.2)}$. Em particular A_o é uma subálgebra de A.

Para uma K-álgebra $\mathbb{Z}_2$-graduada A, como acima, os elementos em $h(A)=A_o \cup A_1$ são chamados de *elementos homogêneos de* A. Se $a \in h(A)$, dizemos que o *grau de a* (e o denotamos $\partial(a)$) é i se $a \in A_i$, $i = 0,1$.

Dadas duas K-álgebras $\mathbb{Z}_2$-graduadas A e B, o produto tensorial graduado de A e B sobre K, será denotado simplesmente por $A \hat{\otimes} B$ e é uma K-álgebra $\mathbb{Z}_2$-graduada cuja i-ésima componente é definida por $\sum_{j+\ell \equiv i (\mathrm{mod} 2)} A_j \otimes B_\ell$; ou seja $(A \hat{\otimes} B)_o = A_o \otimes B_o + A_1 \otimes B_1$ e $(A \hat{\otimes} B)_1 = A_o \otimes B_1 + A_1 \otimes B_o$. A multiplicação em $A \hat{\otimes} B$ é induzida por $(a \otimes b)(a' \otimes b') = (-1)^{\partial(b)\partial(a')} aa' \otimes bb'$; $a,a' \in h(A)$ e $b,b' \in h(B)$.

NOTA: Se $\mathrm{car}(K)=2$, então $A \hat{\otimes} B = A \otimes B$.

(2.2) - DEFINIÇÃO - Sejam K um corpo e (E,q) um espaço quadrático sobre K. Uma K-álgebra A contendo (E,q) como subespaço vetorial é dita *compatível* com q, se $x^2=q(x)\, 1_A \in A$, para qualquer $x \in E$.

Em uma K-álgebra A como acima, a estrutura quadrática de (E,q) está intimamente relacionada com a estrutura algébrica de A. Para ver este ponto mais claramente calculemos para $x,y \in E$, $q(x+y)-q(x)-q(y)=(x+y)^2-x^2-y^2=xy+yx$.

Logo, obtemos a equação $b_q(x,y)=xy+yx$, para todo x, $y \in E$. Em particular, x e y são ortogonais em E, se e somente se, $xy=-yx$ em A.

(2.3) - DEFINIÇÃO - Seja (E,q) um espaço quadrático sobre um corpo K. Uma K-álgebra $C \supseteq E$ compatível com q é dita ser uma *álgebra de Clifford* para (E,q), se ela satisfaz a seguinte propriedade universal: dada qualquer K-álgebra $A \supseteq E$, compatível com q, existe um único homomorfismo de K-álgebras $\phi: C \to A$, tal que $\phi(x) = x$, para qualquer $x \in E$.

Decorre desta propriedade universal que se existe uma álgebra de Clifford para (E,q), então, ela é única a menos de isomorfismos.

Para provar a existência, seja $T(E)$ a álgebra tensorial de E; isto é, $T(E) = K \oplus E \oplus \ldots \oplus E^{\otimes n} \oplus \ldots$, onde $E^{\otimes n} = E \otimes E \otimes \ldots \otimes E$, n vezes. Em $T(E)$ consideremos o ideal $I(q)$, gerado pelos elementos da forma $x \otimes x - q(x)1 \in T(E)$. Indicamos por $C(E,q) = C(E) = C(q)$ a álgebra quociente $T(E)/I(q)$. Claramente E é levado injetivamente em $C(E)$, via o homomorfismo canônico $T(E) \to T(E)/I(q) = C(E)$. Identificando E com sua imagem em $C(E)$, pode ser visto facilmente que $C(E,q)$ é uma álgebra de Clifford para (E,q).

A multiplicação em $C(E)$ pode ser vista como justaposição de elementos e com isto eliminamos o símbolo tensor $\otimes$; simplificando a notação. Observemos que E gera $C(E)$ como K-álgebra.

Consideremos agora $T(E)_o = \bigoplus_o^\infty E^{\otimes 2n}$ e $T(E)_1 = \bigoplus_o^\infty E^{\otimes(2n+1)}$ e $C_i(E)$ a imagem de $T(E)_i$ em $C(E)$ pelo homomorfismo canônico $\pi: T(E) \to C(E) = T(E)/I(q)$, $(i=0,1)$. Notemos que $C_i\, C_j \subseteq C_{i+j\,(\mathrm{mod}\,2)}$, ou seja $C(E)$ também tem uma estrutura de K-álgebra $\mathbb{Z}_2$-graduada. $C_o(E)$ é chamada a *parte par* de $C(E)$ e $C_1(E)$ a *parte ímpar*.

(2.4) - EXEMPLO - Sejam K um corpo com $\mathrm{car}(K) \neq 2$, $E = Kx$ e $q(x) = a \in \dot{K}$. Identificando a K-álgebra tensorial $T(E)$ com o anel dos polinômios $K[X]$, $I(q)$ é, então, o ideal gerado por $X^2 - a$. Logo, $C(E) = K[X]\ /(X^2-a) = K[\sqrt{a}]$.

Dado um espaço quadrático (E,q) sobre um corpo K, passaremos agora a analisar mais intimamente a estrutura da álgebra de Clifford $C(E,q)$. Comecemos por determinar uma base de $C(E,q)$ em termos de uma base de E sobre K. Para tanto, seja $\{x_1,\ldots,x_n\}$ uma base de E sobre K. Em $C(E,q)$, temos $x_i^2 = q(x_i)$ (NOTA: para simplificar notação, doravante identificaremos $K1_{C(E,q)}$ com K) e $x_i x_j + x_j x_i = b_q(x_i,x_j)$, $i \neq j$, $1 \leq i,j \leq n$. Desde que E gera $C(E,q)$, é imediato ver que $C(E,q)$ é gerada, como K-espaço vetorial, pelos elementos da forma $x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$, com $\varepsilon_i = 0,1$, $i = 1,\ldots,n$. Em particular $\dim_K C(E,q) \leq 2^n$. Para mostrar que os elementos $x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$, $\varepsilon_i = 0,1$, $i = 1,\ldots,n$, constituem de fato uma base do K-espaço vetorial $C(E,q)$, necessitare mos da seguinte proposição.

(2.5) - PROPOSIÇÃO - Sejam (E_1,q_1) e (E_2,q_2) espaços quadráticos sobre um corpo K. Então existe um homomorfismo sobrejetor de álgebras $\mathbb{Z}_2$-graduadas $f:C(E_1 \perp E_2) \to C(E_1) \hat{\otimes} C(E_2)$.

Dem. - A aplicação $\varepsilon : E_1 \perp E_2 \to C(E_1) \hat{\otimes} C(E_2)$ tal que $\varepsilon(x_1+x_2) = x_1 \otimes 1 + 1 \otimes x_2$; $x_i \in E_i$, $(i = 1,2)$ é injetora e

$$(x_1 \otimes 1 + 1 \otimes x_2)^2 = x_1^2 \otimes 1 + 1 \otimes x_2^2 + x_1 \otimes x_2 + (-1)x_1 \otimes x_2 =$$

$$= (q_1 \perp q_2)(x_1 + x_2).$$

Pela propriedade universal da álgebra de Clifford, existe um único homomorfismo de álgebras $f:C(E_1 \perp E_2) \to C(E_1) \hat{\otimes} C(E_2)$, que coincide com ε em $E_1 \perp E_2$. A verificação de que f preserva a graduação é imediata. Como a K-álgebra $C(E_1) \hat{\otimes} C(E_2)$ é gerada por elementos da forma $x_1 \otimes 1$ e $1 \otimes x_2$; $x_i \in E_i$, $(i=1,2)$, e tais elementos estão na imagem de f, então f é sobrejetora.□

(2.6) - TEOREMA - Se (E,q) é um espaço quadrático não singular de dimensão n sobre um corpo K, então $\dim_K C(E) = 2^n$. Em particular se $\{x_1,\ldots,x_n\}$ é uma base de E sobre K, então $\{x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}; \varepsilon_i = 0,1\}$ constitui uma base de $C(E)$ sobre K.

Dem. - A segunda parte do teorema segue claramente da primeira. Mostraremos a primeira por indução sobre n.

Se $n=1$, claramente $\mathrm{car}(K) \neq 2$ e, pelo exemplo (2.4), temos $\dim_K C(E) = 2$.

Se $n=2$, seja $\{x_1,x_2\}$ uma base de E sobre K. Desde que (E,q) é não singular podemos supor que $q(x_1) \neq 0$ e $b_q(x_1, x_2) = 1$ (ver I, (1.10)). Já vimos que os elementos $1, x_1, x_2$ e x_1x_2 geram $C(E,q)$. Mostraremos então que $1, x_1, x_2$ e x_1x_2 são linearmente independentes sobre K. Seja $a_0+a_1x_1+a_2x_2+a_3x_1x_2 = 0$ com $a_i \in K$. Observemos que $a_1x_1+a_2x_2=-(a_0+a_3x_1x_2) \in C_0(E) \cap C_1(E) = \{0\}$. Desde que $\{x_1, x_2\}$ é base de E sobre K temos $a_1=a_2=0$. Se $a_3 \neq 0$ então $x_1x_2 \in K$ e, consequentemente, obtemos $q(x_1)\ x_2 = x_1^2x_2 = x_1(x_1x_2) = (x_1x_2)x_1$ ou ainda $q(x_1)=0$ (pois x_1 e x_2 são linearmente independentes sobre K), o que é uma contradição. Portanto, $a_0=a_1=a_2=a_3=0$, ou seja $\{1, x_1, x_2, x_1x_2\}$ é uma base de $C(E)$ sobre K e $\dim_K C(E) = 4 = 2^2$.

Se $n > 2$, escrevemos $E = E_0 \perp E_1$, com $\dim_K E_0 = 2$. Segue da proposição (2.5) que $\dim_K C(E) \geq \dim_K C(E_0)\ \dim_K C(E_1)$. Por hipótese de indução temos $\dim_K C(E_1) = 2^{n-2}$ e assim $\dim_K C(E) \geq 2^n$ o que completa a demonstração.□

(2.7) - COROLÁRIO - Para um espaço quadrático (E,q) não singular sobre K tem-se $\dim_K C_0(E) = \dim_K C_1(E) = 2^{n-1}$.

Dem.- Imediata.□

No que se seguirá analisaremos as condições sob as quais uma álgebra de Clifford é central simples. Começaremos pela descrição de seu centro. Para tanto necessitamos do conceito de extensão quadrática de um corpo.

(2.8) - DEFINIÇÃO - Uma extensão quadrática (separável) de um corpo K é uma K-álgebra do tipo $K[x]$, com $x^2=bx+c$, $b,c \in K$,

$b^2+4c \neq 0$.

Se A é uma extensão quadrática de K, podemos ver facilmente que $A = K[X]/(X^2-a)=K[\sqrt{a}]$, para algum $a \in \dot{K}$, se $car(K) \neq 2$ ou $A = K[X]/(X^2+X+a) = K[\wp^{-1}(a)]$, para algum $a \in K$, se $car(K)=2$.

(2.9) - OBSERVAÇÕES

(1) Uma extensão quadrática de um corpo K é um corpo ou,é isomorfa à $K \times K$.

(2) $K[\sqrt{a}] \cong K[\sqrt{b}]$, se e somente se, $a \equiv b \pmod{\dot{K}^2}$.

(3) $K[\wp^{-1}(a)] \cong K[\wp^{-1}(b)]$, se e somente se, $a \equiv b \pmod{\wp(K)}$ onde $\wp(K)$ é o subgrupo aditivo de K, dado por $\wp(K)=\{a^2+a; a \in K\}$.

(2.10) - PROPOSIÇÃO - Seja (E,q) um espaço quadrático não singular sobre um corpo K.

(a) Se $\dim_K E$ é par, então $Z(C(E))=F$ e $Z(C_o(E))$ é uma extensão quadrática de K.

(b) Se $\dim_K E$ é ímpar, então $Z(C(E))$ é uma extensão quadrática de K e $Z(C_o(E))=K$.

<u>Dem.</u> - Veremos primeiro o caso em que $car(K)\neq 2$. Sejam $\{x_1,\ldots x_n\}$ uma base ortogonal de E sobre K (ver I,(1.10)) e $z=x_1\ldots x_n$. Observemos que $x_i z=(-1)^{i-1}q(x_i)(x_1\ldots x_{i-1}x_{i+1}\ldots x_n)$ e $zx_i = (-1)^{n-i}q(x_i)(x_1\ldots x_{i-1}x_{i+1}\ldots x_n)$. Portanto $zx_i=x_iz$ para todo $i=1,\ldots n$, se e somente se $n-i=i-1$, isto é, se e somente se n é ímpar. Com isso mostramos que $z \in Z(C(E))$ se e somente se n é ímpar. Desde que $K \subseteq Z(C(E))$ obtemos $K \oplus Kz \subseteq Z(C(E))$ para n

ímpar e somente $K \subseteq Z(C(E))$ para n par.

Para $C_o(E)$ temos, $z \in Z(C_o(E))$ se n é par e $z \notin Z(C_o(E))$ se n é ímpar. Com isso mostramos que $K \oplus Kz \subseteq Z(C_o(E))$ se n é par e somente $K \subseteq Z(C_o(E))$ se n é ímpar.

Para demonstrar as inclusões opostas, procedemos como segue.

Observemos que um elemento $x \in Z(C(E))$, se e somente se $xx_i = x_i x$, para $i=1,\ldots,n$. Escrevemos, um elemento $x \in C(E)$, na forma $x = \Sigma a_{\varepsilon_1,\ldots,\varepsilon_n} x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$, onde $\varepsilon_i = 0,1$ e $a_{\varepsilon_1,\ldots,\varepsilon_n} \in K$. Para mostrarmos que $x \in Z(C(E))$, é suficiente verificar que os termos $x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$, $\varepsilon_i = 0,1 (i=1,\ldots,n)$ estão em $Z(C(E))$. Se $\sum_{i=1}^{n} \varepsilon_i$ é ímpar e $\varepsilon_j = 0$, temos $x_j(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}) = -(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})x_j$ e se $\sum_{i=1}^{n} \varepsilon_i$ é par e $\varepsilon_j = 1$, temos $x_j(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}) = -(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})x_j$. Disto concluímos que, se n é par, $Z(C(E)) \subseteq K$ e se n é ímpar, $Z(C(E)) \subseteq K \oplus Kz$. Para $C_o(E)$ basta verificarmos a comutatividade dos termos $x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$, tais que $\sum_{i=1}^{n} \varepsilon_i$ é par, com os termos $x_i x_j$. Desde que:

(i) se $\varepsilon_i = 0$ e $\varepsilon_j = 1$, então $(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})x_i x_j = x_i x_j(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})$,

(ii) se $\varepsilon_i = \varepsilon_j = 0$, então $(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})x_i x_j = -x_i x_j(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})$ e

(iii) se $\varepsilon_i = \varepsilon_j = 1$, então $(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})x_i x_j = x_i x_j(x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n})$,

concluimos que $K \oplus Kz \supseteq Z(C_o(E))$, quando n é par e $K \supseteq Z(C_o(E))$, quando n é ímpar, o que demonstra (2.10) para $car(K) \neq 2$.

Quando $car(K)=2$ temos somente que mostrar o item (a) de (2.10), pois $\dim_K E$ é sempre par (ver I, (1.10)).

Suponhamos primeiro que $n=\dim_K E=2$. Seja $\{x_1,x_2\}$ uma base de E sobre K. Uma base de $C(E)$ sobre K é formada pelos vetores $\{1,x_1,x_2,x_1x_2\}$, com $q(x_i)=x_i^2, i=1,2$ e $b_q(x_1,x_2) = x_1x_2+x_2x_1$. Seja $u = a_0+a_1x_1+a_2x_2+a_3x_1x_2 \in Z(C(E))$; $a_i \in K$. De $0 = ux_1 - x_1u$, obtemos $a_2 = a_3 = 0$. Por outro lado, de $0 = ux_2 - x_2u$, temos $a_1=0$, ou seja $u \in K$. Assim $Z(C(E))=K$.

Se $n > 2$, (E,q) admite uma decomposição ortogonal do tipo $(E,q)=(E_1,q_1)\perp\ldots\perp(E_{n/2},q_{n/2})$, onde $\dim_K E_i=2$; $(i=1,\ldots,\frac{n}{2})$ (ver I, (1.10)) e, consequentemente, $C(E,q) = \hat{\bigotimes}_i C(E_i,q_i)$ (ver (2.5),(2.6)). Desde que $car(K)=2$, temos que $\hat{\otimes} = \otimes$, ou seja $C(E)$ é um produto tensorial ordinário de álgebras centrais sobre K. Portanto $C(E)$ é central sobre K(ver, (1.3)).

Finalmente, mostraremos que $Z(C_o(E))$ é uma extensão quadrática de K.

Escrevemos $C(E,q)=\bigotimes_{i=1}^{m} C(E_i,q_i)$, onde $m = \frac{n}{2}$ e cada (E_i,q_i) é um espaço quadrático não singular de dimensão 2 sobre K. Para cada i, seja $\{x_{i_1},x_{i_2}\}$ uma base de E_i sobre K tal que $b_q(x_{i_1},x_{i_2})=1$ e $b_q(x_{i_r},x_{j_s})=0$ para $i\neq j$. Tomando $z_i=x_{i_1}x_{i_2}$, temos $z_ix + xz_i = x$, $\forall x\in E_i$ e $z_iy = yz_i$, $\forall y\in E_j$; $j \neq i$, de onde segue-se que $z_i \in Z(C_o(E_i))$ e z_i comuta com cada $C(E_j)$ para $j \neq i$.

Seja agora $z = \sum_{i=1}^{m} z_i$. Queremos mostrar que $z \in Z(C_o(E))$; o que faremos por indução sobre m.

Se $m = 1$, temos $z=z_1\in Z(C_o(E_1))$. Suponhamos que $m>1$ e sejam $z' = \sum_{i=1}^{m-1} z_i \in Z(C_o(E'))$, onde $E'= \bigoplus_{i=1}^{m-1} E_i$ e $z_m \in Z(C_o(E_m))$.

Sabemos que z_m comuta com os elementos de E' e $z'x+xz'=x, \forall x \in E'$. Agora, se $x \in E'$, temos $zx+xz=(z'+z_m)x + x(z'+z_m)=x$ e se $x \in E_m$ $zx+xz = x$. Logo $zx + xz = x, \forall x \in E$ e assim z comuta com os produtos xy tais que $x,y \in E$, o que mostra que $z \in Z(C_o(E))$ e consequentemente $K \oplus Kz \subseteq Z(C_o(E))$.

Para mostrarmos que $K \oplus Kz \supseteq Z(C_o(E))$, observamos inicialmente que o resultado é evidente se $\dim_K E=2$, pois, neste caso $C_o(E) = K \oplus Kz$. Novamente por indução sobre m, suponhamos que $m > 1$ e que para $m-1$ $Z(C_o(E'))=K \oplus Kz'$, onde E' e z' são dados como acima. Observemos que $C_o(E)=C_o(E') \otimes C_o(E_m) \oplus C_1(E') \otimes C_1(E_m)$. Afirmamos que $Z(C_o(E)) \subseteq Z(C_o(E') \otimes C_o(E_m))=Z(C_o(E')) \otimes Z(C_o(E_m))$.

De fato, mostraremos que se $y \in Z(C_o(E)) \cap (C_1(E') \otimes C_1(E_m))$ então $y = 0$. Escrevemos $y=y_1 \otimes x_{m_1}+y_2 \otimes x_{m_2}$, onde $y_1, y_2 \in C_1(E')$ e $\{x_{m_1}, x_{m_2}\}$ é uma base de E_m sobre K. Do fato que y comuta com $x \otimes x_{m_1}$ para todo $x \in E'$, segue que:

$$0 = (x \otimes x_{m_1})y-y(x \otimes x_{m_1})=(x_{m_1}^2 (xy_1-y_1x)+y_2x)\otimes 1 +$$
$$+ (xy_2 + y_2x) \otimes x_{m_1}x_{m_2} \quad \text{e portanto temos:}$$
$$x_{m_1}^2(xy_1-y_1x)+y_2x = 0 \quad \text{e} \quad xy_2 + y_2x = 0,$$

para todo $x \in E'$. Analogamente, do fato de y comutar com $x \otimes x_{m_2}$, para todo $x \in E'$, segue que:

$$x_{m_2}^2(xy_2 - y_2x) + y_1x = 0$$
$$xy_1 + y_1x = 0,$$

para todo $x \in E'$. Destes dois sistemas, obtemos:

$y_1x = y_2x=0$ para todo $x \in E'$.

Desde que (E',q') é não singular, existe $x \in E'$ tal que x é inversível em $C_1(E')$ e consequentemente obtemos $y_1 = y_2 = 0$, ou seja $y = 0$. Assim $Z(C_o(E)) \subseteq Z(C_o(E')) \otimes Z(C_o(E_m))$.

O produto tensorial $Z(C_o(E')) \otimes Z(C_o(E_m))$, como submódulo de $C_o(E)$, é gerado por $1, z', z_m$ e $z'z_m$. Se $x \in Z(C_o(E))$, $x = a_0 + a_1 z' + a_2 z_m + a_3 z' z_m$; $a_i \in K$, para $b \in E'$ e $d \in E_m$, temos $xbd - bdx = 0$, ou seja $0 = a_1(z'bd - bdz') + a_2(z_m bd - bdz_m) + a_3(z'z_m bd - bdz'z_m)$. Observando que $z'bd = bd + bdz'$, $z_m bd = bd + bdz_m$ e $z'z_m bd = bd + bdz_m + bdz' + bdz'z_m$; e que $car(K) = 2$, obtemos

$$bd(a_1 + a_2 + a_3(1 + z' + z_m + z'z_m)) = 0.$$

Desde que (E', q') e (E_m, q_m) são não singulares, existem $b \in E'$ e $d \in E_m$ inversíveis em $C(E)$ e, consequentemente, obtemos

$a_1 + a_2 + a_3(1 + z' + z_m + z'z_m) = 0$, ou seja $a_1 = a_2$ e $a_3 = 0$. Assim $x = a_0 + a_1(z' + z_m)$, isto é, $x = a_0 + a_1 z$, o que mostra que $Z(C_o(E)) \subseteq K \oplus Kz$, como queríamos. □

(2.11) - OBSERVAÇÕES - Sejam K um corpo e (E, q) um espaço quadrático não singular sobre K. Do que vimos na demonstração da proposição (2.10) podemos afirmar que:

(i) Se $car(K) \neq 2$, $n = \dim_K E$ é par e $q = \langle a_1, \ldots, a_n \rangle$, então $Z(C_o(E)) = K[z]$, com $z^2 = (-1)^{\frac{n(n+1)}{2}} a_1 \ldots a_n$ e $zx = -xz$ $\forall x \in C_1(E)$.

(ii) Se $car(K) \neq 2$, $n = \dim_K E$ é ímpar e $q = \langle a_1, \ldots, a_n \rangle$, então $Z(C(E)) = K[z]$, com $z^2 = (-1)^{\frac{n(n+1)}{2}} a_1 \ldots a_n$.

(iii) Se $car(K) = 2$, $\dim_K E = 2m$ e $q = [a_1, b_1] \perp \ldots \perp [a_n, b_n]$, então $Z(C_o(E)) = K[z]$, com $z^2 = z + \sum_{i=1}^{m} a_i b_i$.

Tais fatos nos serão úteis na demonstração do seguinte resultado:

(2.12) - PROPOSIÇÃO - Sejam (E,q) e (E',q') espaços quadráticos não singulares sobre um corpo K de característica distinta de 2. Então existe $\alpha \in \dot{K}$ tal que:

(1) $C(E,q) \hat{\otimes} C(E',q') \cong C(E,q) \otimes C(E',\alpha q')$, se $\dim_K E$ é par, ou

(2) $(C(E,q) \hat{\otimes} C(E',q'))_0 \cong C_0(E,q) \otimes C(E',-\alpha q')$ se $\dim_K E$ é ímpar.

Dem. -

(1) Desde que $\dim_K E$ é par, temos que existe $z \in Z(C_0(E))$ tal que $z^2 = \alpha \in \dot{K}$. (ver (2.10),(a)).

Seja B a K-álgebra $\mathbb{Z}_2$-graduada $C_0(E',q') \otimes z\, C_1(E,q)$ contida em $C(E,q) \hat{\otimes} C(E',q')$. Claramente B comuta com $C(E,q) \hat{\otimes} 1$ (ver (2.11),(i)) e B e $C(E,q)$ geram $C(E,q) \hat{\otimes} C(E',q')$ como álgebra. Analisando dimensões vemos facilmente que existe um isomorfismo de álgebras $\mathbb{Z}_2$-graduadas $C(E,q) \otimes B \cong C(E,q) \hat{\otimes} C(E',q')$. Se $x \in E'$, o quadrado de $zx = z \otimes x \in B$ é $z^2 \otimes x^2 = \alpha q'(x)$. Logo, a lei $x \to zx \in B$ induz um isomorfismo de álgebras $\mathbb{Z}_2$-graduadas $C(E',\alpha q') \cong B$. Assim $C(E,q) \hat{\otimes} C(E',q') \cong C(E,q) \otimes$ $\otimes\, C(E',\alpha q')$.

(2) Desde que $\dim_K E$ é ímpar, temos que existe $z \in C_1(E) \cap Z(C(E))$ tal que $z^2 = \alpha \in \dot{K}$. (ver (2.10), (b)). Seja B a subálgebra $C_0(E',q') \otimes zC_1(E',q')$ contida em $(C(E,q) \hat{\otimes} C(E',q'))_0$. Claramente, B comuta com $C_0(E,q) = C_0(E,q) \hat{\otimes} 1$ e, B e $C_0(E,q)$ geram $(C(E,q) \hat{\otimes} C(E',q'))_0$ como uma álgebra. Novamente, analisando as dimensões vemos que existe um isomorfismo de álgebras $C_0(E,q) \otimes B \cong (C(E,q) \hat{\otimes} C(E',q'))_0$. Se $x \in E'$, o quadrado de $zx = z \otimes x \in B$ é $-z^2 \otimes x^2 = -\alpha q'(x)$. Assim, a lei

$x \to zx \in B$ induz um isomorfismo de álgebras $C(E',-\alpha q') \cong B$ e, como queríamos, $(C(E,q) \hat{\otimes} C(E',q'))_o \cong C_o(E,q) \otimes C(E',-\alpha q')$.□

A seguir demonstraremos o resultado principal deste parágrafo:

(2.13) - TEOREMA - Seja (E,q) um espaço quadrático não singular sobre um corpo K.

(1) Se $\dim_K E$ é par, então $C(E)$ é central simples e $Z(C_o(E))$ é uma extensão quadrática de K.

(2) Se $\dim_K E$ é ímpar, então $C_o(E)$ é central simples e $Z(C(E))$ é uma extensão quadrática de K.

Dem.-Após a proposição (2.10) resta mostrar apenas que $C(E)$(resp. $C_o(E)$) é simples quando $\dim_K E$ é par (resp. $\dim_K E$ é ímpar).

Se $\dim_K E$ é par, então podemos decompor (E,q) numa soma ortogonal do tipo $(E,q) = (E_1,q_1) \perp \ldots \perp (E_n,q_n)$, onde cada (E_i,q_i) é um espaço quadrático não singular de dimensão 2 sobre K (ver I, (1.10)). De acordo com a proposição (2.12)(1), se $car(K) \neq 2$ e, devido ao fato de $\hat{\otimes} = \otimes$ se $car(K) = 2$, podemos afirmar que existem espaços quadráticos não singulares, binários $(E_1',q_1'),\ldots,(E_n',q_n')$, sobre K tais que:

$C(E,q) \cong C(E_1',q_1') \otimes \ldots \otimes C(E_n',q_n')$.

Se $\dim_K E$ é ímpar, então necessariamente $car(K) \neq 2$ e podemos obter uma decomposição de (E,q) em uma soma ortogonal do tipo $(E,q) = (E_1,q_1) \perp (E_2,q_2)$, com $\dim_K E_1 = 1$. De acordo com a proposição (2.12) (2) e o exemplo (2.4) temos:

$C_o(E,q) \cong C_o(E_1,q_1) \otimes C(E_2',q_2') \cong C(E_2',q_2')$, com $\dim_K E_2'$ par.

Após esta discussão, a demonstração do teorema se resume a mostrar que a álgebra de Clifford de um espaço quadrático não singular de dimensão 2 sobre um corpo K é simples, e isto veremos, a seguir, na seguinte proposição:

(2.14) - PROPOSIÇÃO - Seja (E,q) um espaço quadrático não singular, de dimensão 2, sobre um corpo K. Então $C(E,q)$ é uma K-álgebra central simples.

Dem.-A afirmação $C(E,q)$ é uma K-álgebra central, é consequência imediata da proposição (2.10)(a). Contudo, é também uma consequência trivial do que veremos nesta demonstração, pois mostraremos que $C(E,q)$ é uma K-álgebra (não comutativa) com divisão ou é uma álgebra de matrizes à coeficientes em K.

Para tanto, seja $\{e_1,e_2\}$ uma base de E sobre K e admitamos que $q(e_i) = a_i, i=1,2$, e $b_q(e_1,e_2) = 1$. Observamos que, independente da característica de K, é sempre possível exibir uma base deste tipo para E (ver I, (1.10)). Assim $C(E) = K \oplus Ke_1 \oplus Ke_2 \oplus Ke_1e_2$, com $e_i^2 = a_i, i=1,2$ e $e_1e_2+e_2e_1 = 1$. Dado um elemento $x = x_0 + x_1e_1 + x_2e_2 + x_3e_1e_2$ de $C(E)$, definimos o *conjugado* de x, a *norma* de x e o *traço* de x, respectivamente por

$$\bar{x} = x_0 - x_1e_1 - x_2e_2 + x_3e_1e_2,$$
$$N(x) = x\,\bar{x} = \bar{x}\,x = (x_0^2 + x_0x_3 + a_1a_2x_3^2) - (a_1x_1^2 + x_1x_2 + a_2x_2^2),$$

$$T(x) = x + \bar{x} = 2x_0 + x_3.$$

Notemos que $x^2 = T(x)x - N(x)$, qualquer que seja

$x \in C(E)$. Claramente T é uma forma linear e N é uma forma quadrática sobre K. É evidente também que x é inversível em $C(E)$ se e somente se $N(x) \neq 0$. Neste caso $x^{-1} = \frac{\bar{x}}{N(x)}$. Assim, a álgebra $C(E)$ é com divisão, se e somente se N é anisotrópica. Se $C(E)$ é com divisão, então $C(E)$ é obviamente uma K-álgebra simples.

Suponhamos então que $C(E)$ não seja com divisão, isto é, que N seja isotrópica. Neste caso mostraremos que existem elementos $e, z \in C(E)$ tais que $C(E) = K \oplus Ke \oplus Kz \oplus Kez$, com $e^2 = c \in \dot{K}$, $z^2 = z$ e $ez + ze = e$. A aplicação linear $\phi: C(E) \to M_2(K)$, tal que $\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\phi(e) = \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix}$, $\phi(z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $\phi(ez) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, nos dará o isomorfismo desejado.

Começaremos por mostrar a existência do elemento z. Isto é imediato se algum dos $a_i = 0$, pois neste caso, basta tomarmos $z = e_1e_2$. Admitamos então que a_1 e a_2 são não nulos. Desde que N é isotrópica, existe $0 \neq x \in C(E)$, $x = x_0 + x_1e_1 + x_2e_2 + x_3e_1e_2$, tal que $N(x) = 0$. Assim, obtemos $x_0^2 + x_0x_3 + a_1a_2x_3^2 = a_1x_1^2 + x_1x_2 + a_2x_2^2$. Se $T(x) = 2x_0 + x_3 \neq 0$, basta tomarmos $z = x/T(x)$. Se $2x_0 + x_3 = 0$ e $x_0 \neq 0$, então $x_0 + 2a_1a_2x_3 \neq 0$ pois, caso contrário, teríamos $1 - 4a_1a_2 = 0$, o que contradiz o fato de (E,q) ser não singular. Neste caso, o elemento

$$z = \frac{-a_1a_2}{x_0 + 2a_1a_2x_3} \left| x_0 + x_1e_1 + x_2e_2 + \left(x_3 - \frac{x_0 + 2a_1a_2x_3}{a_1a_2}\right) e_1e_2 \right| .$$

satisfaz $z^2 = z$. Finalmente, se $2x_0 + x_3 = 0$ e $x_0 = 0$, então

$x_3=0$ e consequentemente obtemos $x_1^2+x_1\frac{x_2}{a_1}+a_1a_2\left(\frac{x_2}{a_1}\right)^2=0$, com $x_1\neq 0$ e $x_2\neq 0$. Como $1-4a_1a_2\neq 0$, então $2x_1+\frac{x_2}{a_1}\neq 0$ e consideramos $z=\frac{a_1}{2a_1x_1+x_2}(x_1+\frac{x_2}{a_1}e_1e_2)$.

Do que vimos acima, podemos, portanto, afirmar que existe $z\in C(E)-K$, $z=z_0+z_1e_1+z_2e_2+z_3e_1e_2$, tal que $z^2=z$.

Se $z_1=z_2=0$, tomamos $e=e_1+e_2$.

Se $z_1\neq 0$ ou $z_2\neq 0$ e $z_3=0$ (o que só ocorre se $car(K)\neq 2$, pois $T(z)=2z_0+z_3\neq 0$), tomamos $e=1-2e_1e_2$.

E, finalmente, se $z_1\neq 0$ ou $z_2\neq 0$ e $z_3\neq 0$, tomamos $e=z_1e_1+z_2e_2$, se $car(K)=2$ ou $e=\alpha+z_1e_1+z_2e_2-2\alpha e_1e_2$, com $\alpha=\frac{z_3(1-4a_1a_2)-1}{2z_3(1-4a_1a_2)}$, se $car(K)\neq 2$, o que demonstra a proposição. □

(2.15) - OBSERVAÇÃO - Observemos que da demonstração da proposição (2.14), segue-se imediatamente que $C(\mathbb{H})=M_2(K)$ e, consequentemente, $C(m\,\mathbb{H})=1$ em $Br(K)$ (ver (2.10) e (2.12)).

§3 - INVARIANTES

Neste parágrafo veremos alguns invariantes, de formas quadráticas, através dos quais nos será possível fazer a classificação de formas quadráticas não singulares sobre um corpo de Hilbert, conforme veremos no Cap. IV. São eles: dimensão, invariante de Arf e invariante de Witt.

(3.1) - DIMENSÃO - Como já vimos no Cap.I, se (E,q) é um espaço quadrático sobre um corpo K, então $\dim q = \dim_K E$ é um invariante da classe de isometria de (E,q).

Para os demais invariantes necessitaremos do seguinte resultado:

(3.2) - PROPOSIÇÃO - Sejam (E_1,q_1) e (E_2,q_2) espaços quadráticos não singulares sobre um corpo K. Se (E_1,q_1) e (E_2,q_2) são isométricos, então $C(E_1,q_1)$ e $C(E_2,q_2)$ são isomorfas como álgebras $\mathbb{Z}_2$-graduadas.

Dem. - Sejam $\phi:(E_1,q_1) \to (E_2,q_2)$ uma isometria e $\{x_1,\ldots,x_n\}$ uma base de E_1 sobre K. Então, $\{x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}; \varepsilon_i = 0,1\}$ e $\{\phi(x_1)^{\varepsilon_1}\ldots\phi(x_n)^{\varepsilon_n}; \varepsilon_i = 0,1\}$ são bases, respectivamente, de $C(E_1,q_1)$ e $C(E_2,q_2)$ sobre K (ver(2.6)). A aplicação $\phi: C(E_1,q_1) \to C(E_2,q_2)$ tal que $\phi(\sum_{(i_1,\ldots,i_n)} \lambda_{i_1\ldots i_n} x_{i}^{\varepsilon_{i_1}}\ldots x_n^{\varepsilon_{i_n}}) =$ $= \sum_{(i_1,\ldots,i_n)} \lambda_{i_1\ldots i_n} \phi(x_1)^{\varepsilon_{i_1}}\ldots\phi(x_n)^{\varepsilon_{i_n}}$ nos dá o isomorfismo desejado.□

(3.3) - INVARIANTE DE WITT - Sejam (E_1,q_1) e (E_2,q_2) espaços quadráticos não singulares isométricos sobre um corpo K. De acordo com a proposição (3.2) existe um isomorfismo de álgebras $\mathbb{Z}_2$-graduadas $\phi: C(E_1,q_1) \to C(E_2,q_2)$. Logo, a restrição ϕ_0 de ϕ à $C_0(E_1,q_1)$ nos dá um isomorfismo de álgebras $\phi_0: C_0(E_1,q_1) \to C_0(E_2,q_2)$. Estas observações nos permitem definir um novo invariante para formas quadráticas não singulares, via a noção de álgebras de Clifford.

Definimos o *invariante de Witt* de um espaço quadrático não singular (E,q) sobre K, como sendo a classe, em $Br(K)$, da álgebra central simples $w(E,q)$, dada por:

$$w(E,q) = \begin{cases} C(E,q) & \text{se } \dim q \text{ é par} \\ \text{ou} & \\ C_0(E,q) & \text{se } \dim q \text{ é ímpar.} \end{cases}$$

(3.4) - INVARIANTE de ARF - Novamente nos reportamos à proposição (3.2). O isomorfismo $\phi: C(E_1,q_1) \to C(E_2,q_2)$, por ser graduado, também induz um isomorfismo entre os centros $Z(C(E_1))$ e $Z(C(E_2))$, bem como entre os centros $Z(C_0(E_1))$ e $Z(C_0(E_2))$. Devido a isto e baseados nas informações dadas em (2.9) e (2.11), definimos, o *invariante de Arf* de um espaço quadrático não singular (E,q) sobre um corpo K, como sendo a classe em $\dot{K}/\dot{K}^2$ (resp. $K/\wp(K)$), se $car(K) \neq 2$ (resp. $car(K)=2$) representada pelo elemento $\Delta(q)$ dado por

$$\Delta(q) = \begin{cases} a_1 \cdots a_n & \text{se } car(K) \neq 2 \text{ e } q = \langle a_1,\ldots,a_n \rangle \\ \text{ou} & \\ \sum_{i=1}^{n} a_i b_i & \text{se } car(K)=2 \text{ e } q = [a_1,b_1] \perp \ldots \perp [a_n,b_n] \end{cases}$$

CAPÍTULO III

EXTENSÕES QUADRÁTICAS E ÁLGEBRAS DE QUATÉRNIOS

§ 1 - EXTENSÕES QUADRÁTICAS

Seja K um corpo. Como vimos no Cap.II, §2 (ver II, (2.7) e (2.8)), uma extensão quadrática separável de K é uma álgebra de dimensão 2 sobre K do tipo:

$K[\sqrt{a}] = K \oplus Kz$, com $z^2 = a \in \dot{K}$, se car$(K) \neq 2$

ou

$K[\wp^{-1}(a)] = K \oplus Kz$, com $z^2 = z+a$, $a \in K$, se car$(K)=2$.

Como trataremos apenas de extensões quadráticas separáveis, doravante as chamaremos simplesmente, extensões quadráticas.

Toda extensão quadrática A de K admite um único K-automorfismo $\sigma_A \neq 1_A$, a saber: $\sigma_A(z) = -z$ se car$(K) \neq 2$ e $\sigma_A(z) = 1+z$ se car$(K) = 2$. Observemos que para todo $x \in A$, o elemento $x\sigma_A(x) \in K$.

(1.1) - DEFINIÇÃO - A aplicação $N_A : A \to K$, dada por $N_A(x) = x\sigma_A(x)$, $x \in A$, será chamada *norma* da extensão quadrática A. É evidente que N_A é uma forma quadrática de A sobre K e, por essa razão, será também chamada de *forma norma* de A.

(1.2) - OBSERVAÇÕES

(a) Se $A = K[\sqrt{a}]$; então $N_A = \langle 1,-a \rangle$ e se $A=K[\wp^{-1}(a)]$, então $N_A = [1,a]$. É evidente que N_A é uma forma quadrática não singular. Indicaremos também $\langle 1,-a \rangle$ (resp. $[1,a]$) simplesmente por n_a.

(b) $D(N_A) \subseteq \dot{K}$ é um subgrupo multiplicativo de $\dot{K}$.

(1.3) - PROPOSIÇÃO - Sejam A e B extensões quadráticas de um corpo K. Então A e B são K-álgebras isomorfas se e somente se N_A e N_B são formas quadráticas isométricas.

Dem.- Sejam $\phi : A \to B$ um K-isomorfismo de álgebras e σ_B o único K-automorfismo não trivial de B. Então a aplicação $\phi^{-1} o \sigma_B o \phi$: $A \to A$, é um K-automorfismo não trivial de A e, consequentemente, $\phi^{-1} \circ \sigma_B \circ \phi = \sigma_A$ ou $\sigma_B \circ \phi = \phi \circ \sigma_A$. Assim, para todo $x \in A$, temos:

$$N_B(\phi(x)) = \phi(x)\sigma_B(\phi(x)) = \phi(x)\phi(\sigma_A(x)) = \phi(x\ \sigma_A(x)) =$$
$$= \phi(N_A(x)) = N_A(x),$$

o que mostra que N_A e N_B são isométricas.

Reciprocamente, se N_A e N_B são isométricas então $\Delta(N_A) = \Delta(N_B)$ (cf. II,(3.4)). Logo se car(K) $\neq 2$, $N_A = \langle 1,-a \rangle$ e $N_B = \langle 1,-b \rangle$, então $a \equiv b \pmod{\dot{K}^2}$ (cf.II,(3.4)) e, consequentemente, A e B são isomorfas (cf. II,(2.8) (b)). Analogamente, se car(K) $= 2$, $N_A = [1,a]$ e $N_B = [1,b]$, então $a \equiv b$ (mod$\wp$(K)) (cf. II, (3.4)) e, portanto, A e B são isomorfas (cf. II, (2.8) (b)).□

(1.4) - COROLÁRIO - Uma extensão quadrática A de um corpo K é isomorfa à $K \times K$ se e somente se N_A é isotrópica.

Dem.- É uma consequência imediata de II,(2.9) e (1.3) acima.□

§2 - ÁLGEBRAS DE QUATÉRNIOS

(2.1) - DEFINIÇÃO - Sejam K um corpo, B uma extensão quadrática de K e σ_B o único K-automorfismo não trivial de B. Uma *álgebra de quatérnios* sobre K é um K-espaço vetorial do tipo $Q = B \oplus Be$, munido de estrutura de álgebra dada por:

$e^2 = a \in \dot{K}$ e $ex = \sigma_B(x)e$, para todo $x \in B$.

Se car(K) $\neq 2$, a extensão quadrática B é do tipo $B = K \oplus Kz$, com $z^2 = b \in \dot{K}$ e, consequentemente, $Q = K \oplus Ke \oplus \oplus Kz \oplus Kez$, com a seguinte tábua de multiplicação:

$e^2 = a \in \dot{K}$, $z^2 = b \in \dot{K}$ e $ez + ze = 0$.

Neste caso, indicamos Q simplesmente por (a,b).

Analogamente, se car(K)=2, então $B = K \oplus Kz$, com $z^2 = z + b$, $b \in K$ e $Q = K \oplus Ke \oplus Kz \oplus Kez$, com $e^2 = a \in \dot{K}$, $z^2 = z + b$ e $ez + ze = e$.

Neste caso, indicamos $Q = (a,b]$.

(2.2) - OBSERVAÇÕES

(1) Uma álgebra de quatérnios sobre um corpo K é simplesmente a álgebra de Clifford de um espaço quadrático não singular de dimensão 2 sobre K. De fato, se car(K) $\neq 2$, podemos ver

trivialmente que $C(\langle a,b\rangle)=(a,b)$. Se $car(K)=2$, $C(\langle a\rangle[1,b])=$ $K \oplus Kx_1 \oplus Kx_2 \oplus Kx_1x_2$, com $x_1^2 = a$, $x_2^2 = ab$ e $x_1x_2+x_2x_1 = 1$. Tomando-se $e = x_1$, $z = \frac{1}{a} x_1x_2$ obtemos $C(\langle a\rangle [1,b])=K \oplus Ke \oplus Kz\oplus$ $\oplus Kez$, com $e^2 = a, z^2 = z + b$ e $ez + ze = e$; ou seja, $C(\langle a\rangle [1,b]) = (a,b]$.

(2) De II,(2.13), decorre que toda álgebra de quatérnios sobre um corpo K é central simples.

(3) Decorre trivialmente do Teorema de Wedderburn que uma álgebra de quatérnios sobre um corpo K é com divisão ou, é isomorfa à álgebra de matrizes $M_2(K)$.

(2.3) - DEFINIÇÃO - Sejam B uma extensão quadrática sobre um corpo K e $Q = B \oplus Be$, com $e^2 = a \in \dot{K}$, uma álgebra de quatérnios sobre K. Se σ_B indica o único K-automorfismo não trivial de B, diremos que o *conjugado* de um elemento $x = x_1+x_2e$ de Q, $x_i \in B$, $i = 1,2$, é um elemento de Q dado por $\bar{x} =\sigma_B(x_1)-$ $- e\sigma_B(x_2)$. Notemos que $x\bar{x} = N_B(x_1) - a\, N_B(x_2) \in K$. A aplicação $N_Q : Q \to K$, tal que $N_Q(x) = x\bar{x}$, $x \in Q$, será chamada *norma* da álgebra de quatérnios Q. Podemos ver, imediatamente, que N_Q é uma forma quadrática de Q em K, também chamada *forma norma* de Q.

(2.4) - OBSERVAÇÕES

(1) Se $car(K) \neq 2$, então $Q = (a,b)$, com $a,b \in \dot{K}$ e $N_Q =$ $\langle 1,-a\rangle\langle 1,-b\rangle = \langle 1,-a,-b,ab\rangle$ a qual passaremos a denotar também por $\langle\langle a,b\rangle\rangle$. Se $car(K) = 2$, então $Q = (a,b]$, com $a \in \dot{K}$ e $b \in K$,

e $N_Q = \langle 1,-a\rangle [1,b] = [1,b] \perp \langle -a\rangle [1,b]$, a qual passaremos a denotar também por $\langle\langle a,b]]$. Observemos também que, em ambos os casos, $N_Q = n_b \perp \langle -a\rangle n_b$. Evidentemente, N_Q é uma forma quadrática não singular.

(2) $D(N_Q) \subseteq \dot{K}$ é um subgrupo multiplicativo de $\dot{K}$.

(3) Para todo $x \in Q$, $x^2 = (x + \bar{x})x - N_Q(x)\ 1_Q = b_{N_Q}(x,1_Q)x - N_Q(x)\ 1_Q$.

(2.5) - PROPOSIÇÃO - Sejam Q_1 e Q_2 álgebras de quatérnios sobre um corpo K. Então Q_1 e Q_2 são K-álgebras isomorfas se, e somente se, N_{Q_1} e N_{Q_2} são formas quadráticas isométricas.

Dem. - Por simplicidade de notação, sejam $N_i = N_{Q_i}$, $b_i = b_{N_{Q_i}}$ e $K 1_{Q_i} = K$, $i = 1,2$.

Suponhamos, inicialmente, que existe um isomorfismo de K-álgebras $h : Q_1 \to Q_2$. Então, de $h(x^2) = h(x)^2$, obtemos $b_1(x,1)h(x) - N_1(x) = b_2(h(x),h(1))h(x) - N_2(h(x))$, ou ainda $[b_1(x,1) - b_2(h(x),h(1))]h(x) = [N_1(x) - N_2(h(x))]$; para todo $x \in Q_1$. Para $x \in Q_1 - K$, temos 1 e $h(x)$ linearmente independentes sobre K e, consequentemente, os coeficientes de ambos os membros da igualdade acima são nulos; ou seja, $b_2(h(x),h(1)) = b_1(x,1)$ e $N_2(h(x)) = N_1(x)$. Desde que $N_2(h(1)) = N_2(1) = 1 = N_1(1)$, concluimos que $N_2(h(x)) = N_1(x)$, para todo $x \in Q_1$; ou seja, N_1 e N_2 são isométricas.

Reciprocamente, suponhamos que N_1 e N_2 são isométricas. Logo, as álgebras de Clifford $C(Q_1,N_1)$ e $C(Q_2,N_2)$ são isomorfas (cf. II,(3,2)).

Por outro lado, para cada $i=1,2$, consideremos a aplicação $f_i: Q_i \to M_2(Q_i)$, dada por $f_i(x) = \begin{pmatrix} 0 & \bar{x} \\ x & 0 \end{pmatrix}$, $x \in Q_i$. É imediato que f_i é um homomorfismo injetor de K-espaços vetoriais tal que $f_i(x)^2 = N_i(x)\, I_2$, onde $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Da propriedade universal para álgebras de Clifford, decorre que cada f_i se estende a um homomorfismo de K-álgebras $\phi_i: C(Q_i,N_i) \to N_2(Q_i)$, $i=1,2$. Como $C(Q_i,N_i)$ é simples, segue-se que cada ϕ_i é injetor, $i = 1,2$. Analisando as dimensões dessas álgebras sobre K, concluímos que cada ϕ_i é um isomorfismo. Assim $M_2(Q_1)$ e $M_2(Q_2)$ são K-álgebras isomorfas e, consequentemente, Q_1 e Q_2 também o são (cf. II,(1.2)(2)).□

(2.6) - COROLÁRIO - Uma álgebra de quartérnios Q sobre um corpo K é isomorfa à álgebra de matrizes $M_2(K)$ se, e somente se, N_Q é hiperbólica.

<u>Dem</u>. - Imediata.□

Na realidade, temos para uma álgebra de quatérnios Q, um resultado exatamente análogo ao que vimos em (1.4) para extensões quadráticas. Isto é consequência imediata do seguinte resultado.

(2.7) - PROPOSIÇÃO - Seja Q uma álgebra de quatérnios sobre um corpo K. Então N_Q é isotrópica se, e somente se, N_Q é hiperbólica.

Dem. - Recordemos que se $Q = B \oplus Be$, com B uma extensão quadrática de K e $e^2 = a \in \dot{K}$, então $N_Q = N_B \perp \langle -a \rangle N_B$.

Suponhamos que N_Q seja isotrópica. Então existe $x = x_1 \oplus x_2 e$, $x_1, x_2 \in B$ não simultaneamente nulos, tal que $N_Q(x) = 0$. Então $N_B(x_1) = \langle a \rangle N_B(x_2)$. Se $N_B(x_2) = 0$ então $N_B(x_1) = 0$ e, consequentemente, N_B é isotrópica. De I,(1.6) decorre que N_B é hiperbólica e, portanto, N_Q também o é. Se $N_B(x_2) \neq 0$ então $a \in D(N_B)$, donde segue-se que $\langle a \rangle N_B \cong N_B$. Assim $N_Q = N_B \perp \langle -a \rangle N_B \cong N_B \perp -N_B$ que é hiperbólica (cf. I,(1.13) (ii)).

A recíproca é trivial.□

A seguir, passaremos a estudar algumas das propriedades das álgebras de quatérnios sobre um corpo K, vistas como elementos do grupo de Brauer, $Br(K)$. Tais propriedades nos serão úteis para a demonstração dos demais resultados deste e do capítulo seguinte. Por simplicidade de notação, indicaremos um elemento de $Br(K)$, representado por uma álgebra central simples A, simplesmente por A.

(2.8) - PROPOSIÇÃO - Em $Br(K)$ temos,

(a) para corpos K, com $car(K) \neq 2$:

(i) $(a,b) = (b,a)$

(ii) $(a,b)=1$ se, e somente se, $a \in D(n_b)$

(iii) $(aa',b) = (a,b)(a',b)$

(iv) $(a,a) = (a,-1)$

quaisquer que sejam $a, a', b \in \dot{K}$;

(b) para corpos K, com $car(K) = 2$:

(i) se $b \in \wp(K)$, então $(a,b] = 1$

(ii) $(a,b] = 1$ se, e somente se, $a \in D(n_b)$

(iii) $(aa',b] = (a,b]\ (a',b]$ e $(a,b+b'] = (a,b]\ (a,b']$ quaisquer que sejam $a,a' \in \dot{K}$ e $b,b' \in K$.

Dem.-(a) $car(K) \neq 2$

(i) É trivial

(ii) De (2.2)(3), (2.6) e (2.7) decorre que $Q = (a,b] = 1$ em $Br(K)$ se, e somente se, N_Q é isotrópica. Logo existem x_0, $x_1, x_2, x_3 \in K$, não todos nulos, tais que $x_0^2 - bx_1^2 = a(x_2^2 - bx_3^2)$. Se $x_2^2 - bx_3^2 = 0$, então $x_0^2 - bx_1^2 = 0$ e, consequentemente, n_b é isotrópica. Logo, n_b é universal (cf. I, (1.8)) e então $a \in \dot{K} = D(n_b)$. Se $x_2^2 - bx_3^2 \neq 0$, então $a = (x_0^2 - bx_1^2)\ (x_2^2 - bx_3^2)^{-1} \in D(n_b)$ (cf. (1.2)(b)).

Reciprocamente, se $a \in D(n_b)$ então $\langle a \rangle n_b \cong n_b$ (cf. I, (1.13)(i)) e, portanto, $N_Q = n_b \perp (-n_b)$ é hiperbólica. De (2.6) segue-se que $Q = (a,b) = 1$ em $Br(K)$.

(iii) Esta igualdade decorre trivialmente do seguinte isomorfismo de K-álgebras:

$(a,b) \otimes (a',b) \cong (aa',b) \otimes (a',-b^2a')$. De fato, desde que $-b^2a' \in D(n_{a'})$, por (ii) obtemos $(a',-b^2a') = 1$ e, portanto, $(a,b)(a',b) = (aa',b)$ em $Br(K)$. Assim, resta-nos apenas mostrar que as K-álgebras $(a,b) \otimes (a',b)$ e $(aa',b) \otimes$ $\otimes\ (a',-b^2a')$ são isomorfas. É suficiente mostrarmos que existem elementos $v_1, v_2, v_3, v_4 \in (a,b) \otimes (a',b)$ que geram

$(a,b) \otimes (a',b)$ como K-álgebra e sejam tais que $v_1^2 = aa'$, $v_2^2 = b$, $v_3^2 = a'$, $v_4^2 = -b^2a'$, $v_1v_2+v_2v_1=v_3v_4+v_4v_3 = 0$ e $v_iv_j = v_jv_i$, $i=1,2$, $j=3,4$. Se $(a,b) = K \oplus Ke_1 \oplus Kz_1 \oplus Ke_1z_1$ e $(a',b) = K \oplus Ke_2 \oplus Kz_2 \oplus Ke_2z_2$, com $e_1^2 = a$, $e_2^2 = a'$, $z_i^2 = b$ e $e_iz_i+z_ie_i = 0$, $i=1,2$, basta tomarmos $v_1 = e_1 \otimes e_2$, $v_2=z_1 \otimes 1$, $v_3 = 1 \otimes e_2$ e $v_4 = z_1 \otimes e_2z_2$.

(iv) Se N_1 e N_2 são as formas normas de (a,a) e $(a,-1)$, respectivamente, então $N_1 = \langle 1,-a,-a,a^2 \rangle \cong \langle 1,-a,-a,1 \rangle \cong \langle 1,-a,1,-a \rangle = N_2$ e, por (2.5), temos $(a,a) = (a,-1)$ em $Br(K)$.

(b) $car(K) = 2$

(i) Se $Q = (a,b]$, então $N_Q=[1,b] \perp \langle a \rangle [1,b]$. Como $b \in \wp(K)$ então $[1,b]$ é isotrópica e, consequentemente, N_Q também o é. Por (2.6) e (2.7) obtemos $(a,b]= 1$ em $Br(K)$.

(ii) A demonstração aqui é exatamente análoga à demonstração de (ii) em (a).

(iii) Analogamente ao que vimos na demonstração de (iii) em (a), aqui também o resultado decorre do seguinte isomorfismo de K-álgebras $(aa',b'] \otimes (a,b+b'] \cong (a,b] \otimes (a',b']$. De fato, para $a = a'$, obtemos $(a^2,b']\ (a,b+b'] = (a,b]\ (a,b']$ e como $(a^2,b'] = 1$ (ver (b)(ii)), então $(a,b+b'] = (a,b]\,(a,b']$ em $Br(K)$. De $b=b'$, obtemos $(aa',b]\ (a,0] = (a,b]\ (a',b]$ e, como $(a,0] = 1$ (ver (b)(i)), então $(aa',b] = (a,b]\ (a',b]$ em $Br(K)$.

Resta, portanto, mostrarmos que as K-álgebras $(aa',b'] \otimes (a,b + b']$ e $(a,b] \otimes (a',b']$ são isomorfas. Por um raciocínio análogo ao que vimos em (a) (iii), basta encontrarmos elementos $v_1,v_2,v_3,v_4 \in (a,b] \otimes (a',b']$ que gerem $(a,b] \otimes (a',b']$ como K-álgebra e sejam tais que $v_1^2=aa', v_2^2=v_2+b', v_3^2=a, v_4^2=v_4+b+b'$, $v_1v_2+v_2v_1=v_1$, $v_3v_4+v_4v_3=v_3$ e $v_iv_j=v_jv_i$, $i=1,2$, $j=3,4$. Se $(a,b] = K \oplus Ke_1 \oplus Kz_1 \oplus Ke_1z_1$ e $(a',b'] = K \oplus Ke_2 \oplus Kz_2 \oplus Ke_2z_2$, com $e_1^2=a, e_2^2=a', z_1^2=z_1+b, z_2^2=z_2+b', e_iz_i+z_ie_i=e_i, i=1,2$, então os elementos $v_1=e_1 \otimes e_2$, $v_2=1 \otimes z_2$, $v_3=e_1 \otimes 1$ e $v_4=z_1 \otimes 1 + 1 \otimes z_2$ satisfazem o requerido.□

(2.9) - COROLÁRIO - Em Br(K) temos,

(a) para corpos K, com car(K) $\neq$ 2:

(i) $(a,b)^2 = (a^2,b) = 1$, $(a,-a) = 1$

(ii) $(a,b) = (a',b)$ se, e somente se, $a \equiv a' \pmod{D(n_b)}$ quaisquer que sejam $a,a',b \in \dot{K}$;

(b) para corpos K, com car(K) = 2:

(i) $(a,b]^2 = (a^2,b] = 1$, $(a,a] = 1$

(ii) se $b \equiv b' \pmod{\wp(K)}$, então $(a,b] = (a,b']$

(iii) $(a,b] = (a',b]$ se, e somente se, $a \equiv a' \pmod{D(n_b)}$ quaisquer que sejam $a,a' \in \dot{K}$ e $b \in K$.

<u>Dem</u>. - Imediata.□

(2.10) PROPOSIÇÃO - Sejam Q_1 e Q_2 álgebras de quartérnios sobre um corpo K e N_1 e N_2 suas respectivas formas normas. Se $N_1 \perp -N_2$ contém pelo menos dois planos hiperbólicos, então existem $c_1, c_2, d \in \dot{K}$ (resp. $c_1 c_2 \in \dot{K}$ e $d \in K$) tais que $Q_i = (c_i, d)$ (resp. $Q_i = (c_i, d])$, $i = 1,2$, se car(K) $\neq 2$ (resp. car(K) $= 2$).

<u>Dem.</u> - Suponhamos, inicialmente, que car(K) $\neq 2$. Neste caso temos $N_1 = \langle 1, -a_1, -b_1, a_1 b_1 \rangle$ e $N_2 = \langle 1, -a_2, -b_2, a_2 b_2 \rangle$, com $a_i, b_i \in \dot{K}$, $i = 1,2$. Logo $N_1 \perp -N_2 = \langle 1,-1 \rangle \perp \langle -b_1, b_2 \rangle \perp \langle -a_1 \rangle \langle 1, -b_1 \rangle \perp \perp \langle a_2 \rangle \langle 1, -b_2 \rangle = \mathbb{H} \perp \langle -b_1, b_2 \rangle \perp q_1 \perp -q_2$, onde $q_i = \langle -a_i \rangle \langle 1, -b_i \rangle$, $i=1,2$. Se, por outro lado, $N_1 \perp - N_2$ contêm pelo menos dois planos hiperbólicos, então $N_1 \perp - N_2 = 2\mathbb{H} \perp q$ para alguma forma quadrática não singular q sobre K com dim $q = 4$. Assim, $2\mathbb{H} \perp q = N_1 \perp \perp -N_2 = \mathbb{H} \perp \langle -b_1, b_2 \rangle \perp q_1 \perp -q_2$ e, pelo Teorema do Cancelamento de Witt (cf. I, (2.3)), concluímos que $\langle -b_1, b_2 \rangle \perp q_1 \perp -q_2$ é isotrópica. Portanto, existem $\alpha, \beta \in K$ e $x_i \in Q_i$, $i=1,2$, não todos nulos, tais que $-\alpha^2 b_1 + \beta^2 b_\alpha + q_1(x_1) - q_2(x_2) = 0$, ou $-\alpha^2 b_1 + q_1(x_1) = \gamma = -\beta^2 b_2 + q_2(x_2)$. Se $\gamma = 0$, então as formas quadráticas $\langle -b_1 \rangle \perp q_1$ e $\langle -b_2 \rangle \perp q_2$ são isotrópicas e, consequentemente, universais (cf. I, (1.8)), o que nos permitiria escolher novos elementos $\alpha_1, \beta_1 \in K$ e $y_i \in Q_i$, $i = 1,2$, tais que $-\alpha_1^2 b_1 + q_1(y_1) = -\beta_1^2 b_2 + q_2(y_2) \neq 0$. Assim podemos supor, sem perda de generalidade, que $\gamma \neq 0$.

Sejam, agora, $e_i, f_i \in Q_i$ tais que $N_i(e_i) = 1$, $N_i(f_i) = -b_i$ e $b_{N_i}(e_i, f_i) = 1$, $i=1,2$. Considerando $u_1 = \alpha f_1 + x_1$ e $u_2 = \beta f_2 + x_2$, vemos que $N_1(u_1) = N_2(u_2) = \gamma$ e $b_{N_1}(e_1, u_1) = b_{N_2}(e_2, u_2)$; ou seja, os subespaços $(U_1 = Ke_1 \oplus Ku_1, N_1|_{U_1})$ e $(U_2 = Ke_2 \oplus Ku_2, N_2|_{U_2})$ de Q_1 e Q_2, respectivamente, são isométricos. Desde que $N_1(u_1) = N_2(u_2) = \gamma \neq 0$, estes subespaços são não singulares e, portanto, temos $N_i = \langle 1, \gamma \rangle \perp p_i$, onde cada p_i é uma forma qua drática de dimensão 2 sobre K, ou seja, da forma $p_i = \langle -c_i\rangle\langle 1,-d_i\rangle$, com $c_i, d_i \in \dot{K}$, $i = 1,2$. Como $\Delta(N_i)=1$ e $\Delta(N_i) = -\gamma d_i$ (mod. $\dot{K}^2$), então $d_i \equiv -\gamma(\text{mod } \dot{K}^2)$, $i = 1,2$. Tomando $d = -\gamma \in \dot{K}$, obtemos $N_i = \langle 1,-d\rangle \perp \langle -c_i\rangle\langle 1,-d\rangle = \langle\langle c_i,d\rangle\rangle$, $i=1,2$. De (2.5) decorre que $Q_i = (c_i,d)$, $i=1,2$.

Suponhamos, agora, que $car(K) = 2$. Neste caso, $N_i = [1,b_i] \perp \langle a_i\rangle[1,b_i]$, $i=1,2$. Se $b_1 \equiv b_2(\text{mod}\,\wp(K))$, nada há a demonstrar (cf. (2.9)(b)(ii)). Suponhamos, então, que $b_1 \not\equiv b_2$ $(\text{mod}\,\wp(K))$. Pode ser visto facilmente que $N_1 \perp - N_2 = N_1 \perp N_2 = \mathbb{H} \perp [1,b_1 + b_2] \perp q_1 \perp q_2$, com $q_i = \langle a_i\rangle[1,b_i]$, $i = 1,2$. Como $N_1 \perp N_2$ contém, por hipótese, pelo menos dois planos hiperbólicos, pelo mesmo argumento usado no caso de característica distinta de 2, concluimos que a forma quadrática $q = [1,b_1+b_2] \perp q_1 \perp q_2$ é isotrópica. Logo, existem elementos não todos nulos $\alpha,\beta \in K$ e $x_i \in Q_i$, $i=1,2$, tais que $\alpha^2 + \alpha\beta + (b_1 + b_2)\beta^2 + q_1(x_1) + q_2(x_2) = 0$.

Afirmamos que é sempre possível obter os elementos α,β,x_1 e x_2 satisfazendo a equação acima de forma que β seja não nulo. De fato, suponhamos que $\beta=0$ e sejam $e,f \in Q_1 \oplus Q_2$ tais que $q(e) = 1$, $q(f) = b_1 + b_2$ e $b_q(e,f)=1$. Consideremos o elemento $v = \alpha e + x_1 + x_2$. Da equação acima vemos que $q(v)=0$. O problema consiste em mostrar que é sempre possível obter um novo elemento $v' = \alpha' e + \beta' f + x_1' + x_2'$, com $\beta' \neq 0$, satisfazendo $q(v')=0$. Se $\alpha=0$, então $q_1 \perp q_2$ é isotrópica e, portanto universal, o que nos permite assegurar que existe $y_i \in Q_i$, $i=1,2$, tais que $q(y_1 + y_2) = q_1 \perp q_2(y_1 + y_2) = b_1 + b_2$. Logo, basta tomar $v' = f + y_1 + y_2$. Se $\alpha \neq 0$, como $b_1 \not\equiv b_2$ $(\text{mod}\,\wp(K)$, basta tomar $y' = \dfrac{1+b_1+b_2}{b_1+b_2}\,\alpha e + \dfrac{\alpha}{b_1+b_2}\, f + x_1 + x_2$.

Assim, podemos afirmar, sem perda de generalidade , que $\beta \neq 0$. Sejam $e_i, f_i \in Q_i$ tais que $N_i(e_i)=1, N_i(f_i) = b_i$ e $b_{N_i}(e_i,f_i) = 1$, $i = 1,2$ e consideremos os elementos $u_1 = \beta f_1 + x_1$ e $u_2 = \alpha e_2 + \beta f_2 + x_2$. Vemos que $N_1(u_1)=N_2(u_2)=d$ e $b_{N_i}(e_i,u_i) = \beta$; ou seja, analogamente ao que vimos no caso de característica distinta de 2, os subespaços $U_i=Ke_i \oplus Ku_i$ de Q_i, $i = 1,2$ respectivamente, são isométricos. Desde que $b_{N_i}(e_i, u_i) = \beta \neq 0$, $N_i|_{U_i}$ é não singular e, portanto, temos $N_i = [1,d] \perp \langle c_i\rangle [1,d_i]$ com $c_i \in \dot{K}$ e $d, d_i \in K$, $i=1,2$. De $\Delta(N_i)=0$ e $\Delta(N_i) = d + d_i \pmod{\wp(K)}$ obtemos $d_i \equiv d \pmod{\wp(K)}$, $i=1,2$. Assim, $N_i = [1,d] \perp \langle c_i\rangle [1,d] = \langle\langle c_i, d]]$ e, por (2.5), $Q_i = (c_i, d]$, $i = 1,2$. □

(2.11) - COROLÁRIO - Seja K um corpo tal que toda forma quadrática não singular de dimensão 4 é universal. Então quaisquer duas álgebras de quatérnios sobre K contêm uma extensão quadrática de K em comum.

Dem. - Imediata.□

(2.12) - OBSERVAÇÕES

(1) A recíproca do Corolário (2.11) não é verdadeira. Basta considerarmos $K = \mathbb{R}$.

(2) Indiquemos por Quat(K) o subconjunto do grupo de Brauer formado das classes representadas por álgebras de quatérnios sobre

um corpo K. A afirmação "quaisquer duas álgebras de quatérnios sobre K contém uma extensão quadrática de K em comum" é equivalente à "Quat(K) forma um subgrupo de Br(K)". Isto foi demonstrado por Albert [1] para corpos de característica distinta de 2 e generalizado por Baeza [2] para anéis semi-locais quaisquer.

CAPÍTULO IV

CORPOS HILBERTIANOS E FORMAS QUADRÁTICAS

O nosso objetivo, neste capítulo, é dar uma caracterização de corpos hilbertianos em termos de formas quadráticas e a consequente classificação de formas quadráticas sobre tais corpos.

§ 1 - DEFINIÇÃO E CARACTERIZAÇÃO DE CORPOS HILBERTIANOS

(1.1) DEFINIÇÃO - Um corpo K é dito ser hilbertiano (ou de Hilbert) se:

(i) $\dot{K} \neq \dot{K}^2$, se car(K) $\neq 2$

ou

$K \neq \wp(K)$, se car(K) $= 2$

(ii) Para todo corpo extensão quadrática separável L de K, tem-se: $[\dot{K};D(N_L)] = 2$, onde N_L indica a norma de L sobre K.

(1.2) OBSERVAÇÃO - Desde que toda extensão quadrática de um corpo K é um corpo ou, do tipo $K \times K$ (cf. II, (2.9)) então, se K é hilbertiano, a igualdade $[\dot{K};D(N_L)] = 1$ é equivalente à $L = K \times K$.

A noção de corpos hilbertianos foi introduzida por Fröhlich [5] , para corpos de característica distinta de 2 e estendida por Baeza [3] para corpos de característica 2. São corpos sobre os quais se desenvolve uma teoria de formas quadrá ticas idêntica a dos números racionais p-ádicos ou dos números reais. Os corpos dos números racionais p-ádicos e dos números reais, são, portanto, os primeiros exemplos, que podemos citar, de corpos hilbertianos. Contudo, para melhor conhecer a família dos corpos hilbertianos e, portanto, melhor exemplificá-los, demonstraremos, a seguir, alguns resultados que nos darão uma descrição de suas propriedades em termos de formas quadráticas.

(1.3) PROPOSIÇÃO - Seja K um corpo, com $car(K) = 2$. Se K é hilbertiano, então toda forma quadrática não singular de dimensão 4 sobre K é universal.

<u>Dem</u>.- Seja $q = \langle a_1\rangle[1,b_1] \perp \langle a_2\rangle[1,b_2]$ uma forma quadrática não singular de dimensão 4 sobre K. Basta mostrarmos que $1 \in D(q)$ pois, analogamente mostra-se que $1 \in D(\langle c\rangle q)$, para todo $c \in \dot{K}$ e, consequentemente, $c \in D(q)$, para todo $c \in \dot{K}$, isto é, q é universal.

Distinguiremos alguns casos:

(1) Seja $a_1 \equiv a_2 \pmod{D([1,b_1])}$. Temos então $a_1 = a_2 c$; $c \in D([1,b_1])$ e, consequentemente, $\langle c\rangle[1,b_1] \simeq [1,b_1]$ (cf. I, (1.13)). Assim, obtemos $q = \langle a_2c\rangle[1,b_1] \perp \langle a_2\rangle[1,b_2] \simeq \langle a_2\rangle[1,b_1] \perp \langle a_2\rangle[1,b_1]$, que é isotrópica e, portanto, universal (cf. I, (1.8)).

(2) Seja $a_1 \not\equiv a_2 \pmod{D([1,b_1])}$. Podemos também supor, sem restrições, que $a_1 \not\equiv a_2 \pmod{D([1,b_2])}$, devido ao caso (1). Mais ainda, podemos supor que $b_1, b_2 \notin \wp(K)$ pois, caso contrário, q seria isotrópica. Temos então $[\dot{K};D([1,b_i])] = 2, i = 1,2$, pois K é hilbertiano. Assim, $a_1 \in D([1,b_1])$ e $a_2 \notin D([1,b_1])$

ou, $a_1 \notin D([1,b_1])$ e $a_2 \in D([1,b_1])$. No primeiro caso temos $\langle a_1\rangle[1,b_1] \simeq [1,b_1]$ e, consequentemente, $1 \in D(q)$, pois $q \simeq [1,b_1] \perp \langle a_2\rangle[1,b_2]$. No segundo caso, $\langle a_2\rangle[1,b_1] \simeq [1,b_1]$ e, assim

$$q = \langle a_1\rangle[1,b_1] \perp \langle a_2\rangle[1,b_2] \simeq \langle a_2\rangle(\langle a_1 a_2\rangle[1,b_1] \perp [1,b_2]) \simeq$$

$$\simeq \langle a_2\rangle(\langle a_1\rangle[1,b_1] \perp [1,b_2]).$$

Por outro lado, se $a_2 \in D([1,b_2])$, temos que $1 \in D(q)$. Suponhamos então que $a_2 \notin D([1,b_2])$. Logo, $a_1 \in D([1,b_2])$ e, consequentemente $q \simeq \langle a_1 a_2\rangle([1,b_1] \perp [1,b_2])$ que é isotrópica e, como queríamos $1 \in D(q)$. $\square$

No caso de característica distinta de 2 existem corpos (não necessariamente hilbertianos) que não satisfazem a proposição acima. Por exemplo, os corpos ordenados. Dizemos que um corpo K é *ordenado*, se existe um subconjunto $P = P(K)$ de K satisfazendo as seguintes condições:

(1) $P \subseteq \dot{K}$ e $-1 \notin P$

(2) $P + P \subseteq P$

(3) $PP \subseteq P$

(4) $\dot{K} = P \cup (-1)P$

Os elementos de $P(K)$ são chamados elementos positivos de K.

No caso de corpos ordenados existe sempre, para cada dimensão n, pelo menos uma forma quadrática anisotrópica, a saber: $X_1^2 + \ldots + X_n^2$. A recíproca deste fato não é verdade em geral, como podemos ver através do seguinte exemplo.

Sejam $K_0 = \mathbb{F}_3$ e $K_1 = K_0((t_1))$ o corpo das séries formais à coeficientes em K_0. Consideramos $K_n = K_{n-1}((t_n))$ e $K = \bigcup_{i=0}^{\infty} K_i$. Obviamente K é um corpo não ordenado e, decorre de [6] Cap. 6, Prop. 1.9, que existe uma forma quadrática anisotrópica sobre K, para cada dimensão.

Contudo temos, no caso hilbertiano, a seguinte proposição:

(1.4) PROPOSIÇÃO - Seja K um corpo hilbertiano. Se existe uma forma quadrática não singular de dimensão 4 sobre K não universal, então K é ordenado e $P(K) = \dot{K}^2$.

Para a demonstração desta Proposição necessitamos de um resultado que nos vai ser útil também para outras demonstrações que se seguirão. Por essa razão o enunciaremos como um Lema.

(1.5) LEMA - Sejam K um corpo hilbertiano e q uma forma quadrática não singular de dimensão 4 sobre K. Se q é anisotrópica e $1 \in D(q)$ então q é da forma $\langle\langle a,b\rangle\rangle$, se $car(K) \neq 2$, ou $\langle\langle a,b]]$ se $car(K) = 2$.

<u>Dem.</u>- Como $1 \in D(q)$ podemos escrever

$$q = \begin{cases} \langle 1,-b\rangle \perp \langle -a\rangle \langle 1,-c\rangle\ , & \text{se } car(K) \neq 2 \\ \text{ou} & \\ [1,b] \perp \langle a\rangle [1,c]\ , & \text{se } car(K) = 2 \end{cases}$$

Claramente, as formas quadráticas $\langle 1,-b\rangle$ e $\langle 1,-c\rangle$ (resp. $[1,b]$ e $[1,c]$) são anisotrópicas pois, q o é. Podemos, portanto, afirmar que $\langle 1,-b\rangle = n_b$ e $\langle 1,-c\rangle = n_c$ (resp. $[1,b] = n_b$ e $[1,c] = n_c$) são as formas normas dos corpos extensões quadráticas de K, $K[\sqrt{b}]$ e $K[\sqrt{c}]$ (resp. $K[\wp^{-1}(b)]$ e $K[\wp^{-1}(c)]$). Resumidamente, $q = n_b \perp \langle -a\rangle n_c$. A demonstração deste lema consiste, portanto, em mostrar que $n_b = n_c$.

Desde que q é anisotrópica, temos $x \in D(n_c)$, implica que $ax \notin D(n_b)$, para todo $x \in \dot{K}$. Afirmamos que se $x \in D(n_c)$, então $x \in D(n_b)$, para todo $x \in \dot{K}$. De fato, se $x \in D(n_c)$ e $x \notin D(n_b)$ então, desde que $a \notin D(n_b)$ e K é hilbertiano, obteríamos $ax \in D(n_b)$, o que é uma contradição. Analogamente, aplicando o mesmo raciocínio para $\langle -a\rangle q = n_c \perp \perp \langle -a\rangle n_b$, a qual é também anisotrópica, obteremos $x \in D(n_b)$ implica que, $x \in D(n_c)$. Assim, temos que $D(n_b) = D(n_c)$. Em termos de álgebras de quatérnios (cf. III,(2.9)), isto significa que, em $Br(K)$, $(x,b) = (x,c)$ (resp. $(x,b] = (x,c]$) ou, equivalentemente, $(x,bc) = 1$ (resp. $(x,b+c] = 1$) se $car(K) \neq 2$ (resp. se $car(K) = 2$), para todo $x \in \dot{K}$. Assim, temos $x \in D(n_{cb})$ (resp. $x \in D(n_{c+b})$) para todo $x \in \dot{K}$, o que significa $\dot{K} = D(n_{cb})$ (resp. $\dot{K} = D(n_{c+b})$), ou (cf. (1.2)) $cb \in \dot{K}^2$ (resp. $c+b \in \wp(K)$). O isomorfismo $n_b \cong n_c$ decorre, agora, trivialmente de (II,(2.9)) e (III,(1.3)). □

<u>Dem. de (1.4)</u> - Desde que existe uma forma quadrática não singular de dimensão 4 sobre K não universal, temos por (1.3) que $car(K) \neq 2$. Seja q uma forma quadrática não singular sobre K não univer-

sal, com $\dim q = 4$. A forma quadrática q é do tipo $\langle c\rangle q'$, para algum $c \in \dot{K}$ e q' uma forma quadrática não singular, não universal que representa 1. Assim, podemos supor, sem perda de generalidade, que q representa 1. De (1.5) segue-se que q é da forma $\langle\langle a,b\rangle\rangle$. Portanto $D(q)$ é um subgrupo multiplicativo de $\dot{K}$ (cf. III, (2.4) (1) (2)).

Seja $P = D(q)$. Observemos que $D(n_a) \subseteq D(q) = P$ e $P \subsetneq \dot{K}$, pois q é não universal. Desde que $[\dot{K};D(n_a)] = 2$, obtemos $D(n_a) = P$. De $q = n_a \perp (-b)n_a = n_b \perp (-a)n_b$, segue-se também que $P = D(n_b)$. Então, em $Br(K)$, temos $(a,x) = (b,x)$, para todo $x \in \dot{K}$. Em particular, $(a,a) = (b,a) \neq 1$ pois q é anisotrópica. Como $(a,a) = (a,-1)$ (cf. III, (2.8) (a)), temos $(a,-1) = (b,a) \neq 1$, o que significa que, $-1 \notin D(n_a) = P$ (cf. III, (2.8)(a)). De $(a,-1) = (a,b)$ em $Br(K)$, segue-se também que $q \simeq n_{-1} \perp (-a)n_{-1}$ (cf. III, (2.5)) e, repetindo o mesmo raciocínio que acima, agora para -1, obteremos $(-1,-1) = (-1,a)$ em $Br(K)$ e, portanto, $q \simeq n_{-1} \perp n_{-1}$.

Assim, desde que $P = D(q) = D(n_{-1})$, temos $P + P = D(n_{-1}) + D(n_{-1}) \subseteq D(n_{-1} \perp n_{-1}) = D(q) = P$. De $-1 \notin P$, segue-se que $\dot{K} = P \cup (-1)P$ e $P \cap (-1)P = \emptyset$. Consequentemente, P define uma ordem sobre K e $\dot{K}^2 \subseteq P$, pois $(x^2,a) = 1$ em $Br(K)$ para todo $x \in \dot{K}$ e, $P = D(n_a)$.

Seja $b \in P = D(q) = D(n_{-1})$. Então $(b,-1) = 1$ em $Br(K)$ e, consequentemente $(-b,-1)(-1,-1) = 1$, ou seja, $(-b,-1) = (-1,-1)$ em $Br(K)$. Logo $q = n_{-1} \perp (b)n_{-1}$ e, novamente obtemos $D(n_{-b}) = P = D(n_{-1})$. Assim, $(-1,x) = (-b,x)$ para todo $x \in \dot{K}$, ou seja,

$(b,x) = 1$ para todo $x \in \dot{K}$, o que implica $\dot{K} = D(n_b)$, isto é, $b \in \dot{K}^2$ (cf.(1.2)). Isto mostra que $P = \dot{K}^2$. □

O teorema que demonstraremos a seguir, é o principal resultado deste parágrafo, o qual dará uma caracterização de corpos hilbertianos em termos de formas quadráticas.

(1.6) TEOREMA - Seja K um corpo hilbertiano. Então:

(A) K é ordenado e $P(K) = \dot{K}^2$

ou

(B) Existe, a menos de isometrias, uma única forma quadrática não singular anisotrópica e de dimensão 4 sobre K.

Reciprocamente, todo corpo K do tipo (A) ou (B) é hilbertiano.

Dem.- Seja K um corpo hilbertiano. Se existe uma forma quadrática não singular e não universal de dimensão 4 sobre K, então de (1.4) segue-se que K é do tipo (A).

Suponhamos, então, que toda forma quadrática não singular de dimensão 4 sobre K é universal. Recordemos que, no caso específico de $car(K) = 2$, isto já é uma consequência de K ser hilbertiano (cf.(1.3)). Por (III,(2.11)), podemos afirmar que dadas duas álgebras de quatérnios Q_1 e Q_2 sobre K, com $Q_i \neq 1$ em $Br(K), i = 1,2$, existem $d \in \dot{K} - \dot{K}^2$ (resp. $d \in K - \wp(K)$) e $c_1, c_2 \in \dot{K}$, se $car(K) \neq 2$ (resp. $car(K) = 2$), tais que $Q_i = (c_i, d)$ (resp. $Q_i = (c_i, d]$) e $c_i \notin D(n_d)$ (cf. III,(2.8)). Desde que K é hilbertiano, segue-se que $c_1 c_2 \in D(n_d)$; ou seja, existe $c \in D(n_d)$, com $c_1 = c_2 c$ e, desta forma, obtemos

$Q_1 = (c_1,d) = (c_2c,d) = (c_2,d) = Q_2$ (resp. $Q_1 = (c_1,d] = (c_2c,d] = (c_2,d] = Q_2$) em $Br(K)$. Isto mostra que existe, a menos de isomorfismo, uma única álgebra de quatérnios com divisão sobre K ou, equivalentemente, uma única forma quadrática anisotrópica do tipo $\langle\langle a,b\rangle\rangle$ (resp. $\langle\langle a,b]]$) sobre K (cf. III, (2.5)). Como toda forma quadrática não singular q de dimensão 4 sobre K é universal e, portanto $1 \in D(q)$, decorre do Lema (1.5) e do que vimos acima que existe, a menos de isometrias, uma única forma quadrática não singular anisotrópica de dimensão 4 sobre K. Isto mostra que K é do tipo (B).

Reciprocamente, suponhamos inicialmente que K é do tipo (A). Então $car(K) \neq 2$ e $\dot{K}/\dot{K}^2 = \{\pm 1\}$, o que implica $\dot{K} \neq \dot{K}^2$. Além disso, $D(n_{-1}) = \dot{K}^2$ e, consequentemente, $[\dot{K}; D(n_{-1})] = 2$. Como qualquer outro corpo extensão quadrática de K é isomorfo à $K[\sqrt{-1}]$, concluímos que K é hilbertiano.

Se K é do tipo (B), seja q a única forma quadrática anisotrópica de dimensão 4 sobre K.

Se $car(K) \neq 2$ e $\dot{K} = \dot{K}^2$ (resp. $car(K) = 2$ e $K = \wp(K)$) então todas as formas quadráticas de dimensão 2 sobre K seriam isotrópicas e, consequentemente, também q. Portanto $\dot{K} \neq \dot{K}^2$ no caso de $car(K) \neq 2$ e $K \neq \wp(K)$ no caso $car(K) = 2$.

Seja $\lambda \in D(q)$. Como q é anisotrópica, então λq também o é e, consequentemente, $\lambda q \simeq q$. Disto segue-se que $1 \in D(q)$. Logo podemos escrever q na forma $q = \langle 1,-d\rangle \perp q'$ (resp. $q = [1,d] \perp q'$) se $car(K) \neq 2$ (resp. $car(K) = 2$) para alguma forma quadrática não singular binária q' e algum $d \in \dot{K} - \dot{K}^2$ (resp. $d \in K - \wp(K)$).

Seja $L = K[\sqrt{d}]$ (resp. $L = K[\wp^{-1}(d)]$) . Assim, $q = N_L \perp q'$. Observemos que $D(N_L) \subsetneq \dot{K}$ pois, caso contrário, teríamos N_L universal e, consequentemente, q isotrópica.

Para quaisquer $a,b \in \dot{K} - D(N_L)$, as formas quadráticas $\ll a,d \gg$ e $\ll b,d \gg$ (resp. $\ll a,d]]$ e $\ll b,d]]$) são anisotrópicas (cf. III, (2.8)) e, portanto, isométricas. Assim, temos $a \equiv b$ (mod $D(N_L)$) (cf. III, (2.5) e (2.9)); ou seja, $[\dot{K} ; D(N_L)] = 2$. Isto demonstra que K é hilbertiano. □

(1.7) OBSERVAÇÃO - Do que vimos, resulta que, quando K é hilbertiano, existe uma única álgebra de quatérnios Q distinta de 1 em Br(K) e tal que $Q^2 = 1$. Por essa razão, quando $car(K) \neq 2$, costumamos indicar $Quat(K) = \{\pm 1\}$. Consequentemente, a aplicação $(\ , \ ) : \dot{K}/\dot{K}^2 \times \dot{K}/\dot{K}^2 \to Quat(K)$, que a cada par de elementos $a,b \in \dot{K}$ associa a álgebra de quatérnios (a,b), pode ser vista como sendo a aplicação bilinear simétrica $(\ , \ ) : \dot{K}/\dot{K}^2 \times \dot{K}/\dot{K}^2 \to \{\pm 1\}$, dada por:

$$(a,b) = \begin{cases} 1 & \text{se } X^2 - aY^2 - bZ^2 = 0 \text{, tem solução não trivial em } K \\ -1 & \text{caso contrário,} \end{cases}$$

a qual é conhecida como sendo o *Símbolo de Hilbert* sobre K.

(1.8) EXEMPLOS DE CORPOS HILBERTIANOS

(1) O corpo dos números reais é um corpo hilbertiano, pois é do tipo (A).

(2) Todo corpo local, com corpo de classes de resíduos finito,

é do tipo (B) (cf.[7], Ch.II,Th 1.1). Em particular o corpo dos números racionais p-ádicos e o corpo das séries formais, com coeficientes num corpo finito, são hilbertianos.

Uma grande classe de corpos hilbertianos é obtida através da seguinte proposição:

(3) PROPOSIÇÃO - Sejam K um corpo hilbertiano local, com $car(K) \neq 2$ e K_0 um subcorpo denso em K tal que $\dot{K}_0 \cap \dot{K}^2 = \dot{K}_0^2$. Então, K_0 é hilbertiano.

<u>Dem</u>.- Observemos primeiro que se K é local e $car(K) \neq 2$, então $\dot{K}^2$ é um aberto de $\dot{K}$ (ver [6] Cap.6, (2.20)). Desde que $\dot{K}_0$ é denso em $\dot{K}$, segue-se $\dot{K}_0\dot{K}^2 = \dot{K}$. Portanto $\dot{K}/\dot{K}^2 \cong \dot{K}_0\dot{K}^2/\dot{K}^2 \cong \dot{K}_0/\dot{K}_0 \cap \dot{K}^2 \cong \dot{K}_0/\dot{K}_0^2$, e consequentemente, $\dot{K}_0 \neq \dot{K}_0^2$.

Seja L_0 um corpo extensão quadrática de K_0. Então $L=L_0K$ é um corpo extensão quadrática de K. Do fato que K é local, segue-se que L também o é (cf.[8] Th. 2.2.10). Mostraremos agora que L_0 é denso em L.

Seja $\hat{L}_0$ o completamento de L_0. Notemos que $K_0 \subseteq \hat{L}_0$ e ainda, se $\bar{K}_0$ é o fecho topológico de K_0, então $\bar{K}_0 \subseteq \hat{L}_0$. Observemos que $\bar{K}_0$ é completo pois, é um fechado em $\hat{L}_0$, que é completo. Assim, desde que K_0 é denso em K e K é completo, podemos identificar $\bar{K}_0$ com K. Consequentemente, $\hat{L}_0 \supseteq L_0K = L \supseteq L_0$, com L completo. Logo L contém o fecho de L_0 e, desde que L_0 é denso em $\hat{L}_0$, obtemos $L \supseteq \hat{L}_0$, ou seja $L = \hat{L}_0$ e, como queríamos L_0 é denso em L.

Agora, usando o fato de que L é local e L_0 é denso em L, obtemos $\dot{L}_0\dot{L}^2 = \dot{L}$. É fácil ver que $D(N_L) = \dot{K}^2 D(N_{L_0})$ e, consequentemente obtemos:

$$\dot{K}_0 \cap D(N_L) = \dot{K}_0 \cap (\dot{K}^2 D(N_{L_0})) = (\dot{K}_0 \cap \dot{K}^2) D(N_{L_0}) = \dot{K}_0^2 D(N_{L_0}) = D(N_{L_0}),$$

o que implica que a inclusão $\dot{K}_0/_{D(N_{L_0})} \to \dot{K}/_{D(N_L)}$ é injetiva. Mas $\dot{K} = \dot{K}_0\dot{K}^2$ e, consequentemente, para todo $x \in \dot{K}$, temos $x = x_0y^2$, com $x_0 \in \dot{K}_0$ e $y \in \dot{K}$. Desde que $D(N_L) = \dot{K}^2 D(N_{L_0})$ temos $x \in D(N_L)$ se, e somente se, $x_0 \in D(N_{L_0})$, com o que concluímos que a inclusão, dada acima, é sobrejetora. Portanto, $[\dot{K}_0; D(N_{L_0})] = [\dot{K}; D(N_L)] = 2$, ou seja, K_0 é um corpo hilbertiano. $\square$

Vejamos agora os exemplos de corpos hilbertianos devidos à Proposição(3).

Sejam F um corpo de números algébricos, com car$(F) \neq 2$ e K_0 a 2 - extensão algébrica maximal de F no completamento p-ádico $K = F_p$ de F.

O corpo K é hilbertiano, pois é local com corpo de classes de resíduos finito, e K_0 é denso em K pois, F o é. Observemos que $\dot{K}_0 \cap \dot{K}^2 = \dot{K}_0^2$ pois, se existisse $a \in \dot{K}_0 \cap \dot{K}^2$ e $a \notin \dot{K}_0^2$, então $K_0[\sqrt{a}]$ seria uma extensão algébrica de grau 2 sobre K_0, o que contradiz a maximalidade de K_0. Logo pela proposição acima, K_0 é também hilbertiano.

§2 - CLASSIFICAÇÃO DE FORMAS QUADRÁTICAS SOBRE CORPOS HILBERTIANOS

Devido ao teorema de caracterização (1.6) do parágrafo anterior classificarmos as formas quadráticas não singulares sobre corpos hilbertianos, é equivalente a classificá-las sobre corpos do tipo (A) e (B).

(2.1) TEOREMA - Seja K um corpo do tipo (A). Então:

(1) para cada dimensão n, $n\langle 1\rangle$ e $n\langle -1\rangle$ são, a menos de isometrias, as únicas formas quadráticas não singulares anisotrópicas desta dimensão.

(2) duas formas quadráticas não singulares sobre K são isométricas se, e somente se, elas tem a mesma dimensão e a mesma signatura.

Dem.- Sabemos que $\dot{K}/\dot{K}^2 = \{\pm 1\}$. Assim uma forma quadrática não singular sobre K é anisotrópica se, quando escrita na forma diagonal, os coeficientes são todos de um mesmo sinal. Logo (1) é imediato.

Para demonstrarmos (2), definiremos primeiro "signatura". Claramente, numa diagonalização de uma forma q, o número de coeficientes positivos (e também negativos) é unicamente determinado. De fato, se $r\langle 1\rangle \perp (n-r)\langle -1\rangle$ e $s\langle 1\rangle \perp (n-s)\langle -1\rangle$ são duas diagonalizações para $q(\dim q = n)$, onde $s \geq r$, então $r\langle 1\rangle \perp (n-r)\langle -1\rangle \approx s\langle 1\rangle \perp (n-s)\langle -1\rangle$ e, usando o Teorema do Cancelamento de Witt (cf.I,(2.3)), obtemos $(n-r)\langle -1\rangle \approx (s-r)\langle 1\rangle \perp$ $\perp (n-s)\langle -1\rangle$. Assim, se $s > r$, temos um absurdo, pois $(n-r)\langle -1\rangle$ é anisotrópica e $(s-r)\langle 1\rangle \perp (n-s)\langle -1\rangle$ seria isotrópica. Consequentemente $r = s$. Escreveremos, agora, $n_+ = r$ (número de coeficientes positivos) e $n_- = n - n_+$. A signatura de q é definida por $n_+ - n_-$. Agora é imediato verificar que duas formas são isométricas se, e somente se, elas tem a mesma dimensão e a mesma signatura. □

(2.2) TEOREMA - Seja K um corpo do tipo (B). Então duas formas quadráticas não singulares sobre K são isométricas se, e somente se, elas tem a mesma dimensão, o mesmo invariante de Arf e o mesmo invariante de Witt.

Dem.- Evidentemente, se duas formas quadráticas não singulares sobre K são isométricas, então elas tem a mesma dimensão, o mesmo invariante de Arf e o mesmo invariante de Witt.

Reciprocamente, sejam q_1 e q_2 formas quadráticas não singulares sobre K, tais que $\dim q_1 = \dim q_2$, $\Delta(q_1) = \Delta(q_2)$ e $w(q_1) = w(q_2)$.

Seja $n = \dim q_i$, $i = 1,2$. Se $n \geq 5$, então q_1 e q_2 são isotrópicas e, desde que $\dim q_1 = \dim q_2$ é fácil ver que q_1 e q_2 admitem uma decomposição ortogonal do tipo $q_i = q_i' \perp m\mathbb{H}$, com $\dim q_1' = \dim q_2' \leq 4$.

De $w(q_1) = w(q_2)$ segue-se imediatamente que $w(q_1') = w(q_2')$ (cf. II, (2.12), (2.15) e (3.3)), e de $\Delta(q_1) = \Delta(q_2)$ segue-se, pela definição do invariante de Arf, que $\Delta(q_1') = \Delta(q_2')$. Portanto, podemos supor, sem perda de generalidade, que $n \leq 4$.

Se $n = 1$, o resultado é imediato pois, $q_1 = \langle\Delta(q_1)\rangle$ e $q_2 = \langle\Delta(q_2)\rangle$.

Se $n = 2$ e $car(K) \neq 2$, temos:

$q_1 = \langle a,b\rangle \qquad\qquad q_2 = \langle c,d\rangle$

$\Delta(q_1) = ab$ $\qquad\qquad$ $\Delta(q_2) = cd$

$w(q_1) = (a,b)$ $\qquad\qquad$ $w(q_2) = (c,d)$

De $w(q_1) = w(q_2)$, obtemos $(a,b) \cong (c,d)$ e, consequentemente, $<1,-a,-b,ab> \simeq <1,-c,-d,cd>$ (cf.III,(2.5)), ou $<1,\Delta(q_1)> \perp$ $\perp <-1>\, q_1 \simeq <1,\Delta(q_2)> \perp <-1>\, q_2$. De $\Delta(q_1) = \Delta(q_2)$, via o Teorema do Cancelamento de Witt (cf.I,(2.3)), obtemos $q_1 \simeq q_2$.

No caso de $car(K) = 2$ e $n = 2$ o resultado segue-se por um raciocínio análogo.

Se $n = 3$, então necessariamente $car(K) \neq 2$. Desde que $w(<a>q) = w(q)$ quando dimensão de q é ímpar e $a \in \dot{K}$ (cf.II, (2.4),(2.12) e (2.13)), e $\Delta(q_1) = \Delta(q_2) = d$, trocando q_1 e q_2 por $<-d>\, q_1$ e $<-d>\, q_2$, podemos supor que $\Delta(q_1) = \Delta(q_2) = -1$. Assim, q_1 e q_2 admitem uma decomposição ortogonal do tipo: $q_1 =$ $= <a,b,-ab>$ e $q_2 = <c,d,-cd>$ com $a,b,c \in \dot{K}$. Como $w(q_1) = C_0(q_1) =$ $= (a,b)$ e $w(q_2) = C_0(q_2) = (c,d)$, de $w(q_1) = w(q_2)$ obtemos $(a,b) \cong$ $\cong (c,d)$ e, consequentemente, $<1,-a,-b,ab> \simeq <1,-c,-d,cd>$ (cf. III,(2.5)), ou seja, $<1> \perp <-1>q_1 \simeq <1> \perp <-1>q_2$. Assim, via o Teorema do Cancelamento de Witt, obtemos $q_1 \simeq q_2$.

Para $n = 4$ o resultado é imediato. Como existe uma única forma quadrática não singular anisotrópica de dimensão 4, se q_1 e q_2 são anisotrópicas de dimensão 4, necessariamente elas são isométricas e, se q_1 e q_2 são isotrópicas recaímos nos casos anteriores. □

BIBLIOGRAFIA

[1] ALBERT, A. A.; *Tensor Products of Quaternion Algebras*, Proc. Amer. Math. Soc., Vol. 35, Nº 1, (1972), 65-66.

[2] BAEZA, R.; *Quadratic Forms over semi-local Rings*, L. N. 655, Springer, Berlim - Heidelberg - New York, (1978).

[3] BAEZA, R.; *Algebras de cuaterniones, formas cuadraticas y un resultado de C. Arf*, Notas de la Sociedad Matemática de Chile, Vol. 2, 1-19.

[4] FELZENSZWALB, B.; *Álgebras de Dimensões Finitas*, IMPA, (1979).

[5] FRÖHLICH, A.; *Quadratic forms 'à la' local theory*, Proc.Camb. Phil. Soc., (1967), 579-586.

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

[7] VIGNÉRAS, M. F.: *Arithmétique des Álgebres de Quaternions*, L. N. 800, Springer - Verlag, (1980).

[8] WEISS, E.; *Algebraic Number Theory*, McGraw - Hill Book Company, (1963).