SOBRE COHOMOLOGIA DE FORMAS QUADRÁTICAS

Antonio Paques

Dissertação apresentada ao Instituto
Matemática, Estatística e Ciência da C
putação da Universidade Estadual de C
pinas , como requisito parcial para a
tenção do título de Doutor em Matemáti

ORIENTADOR : PROF. DR. ARTIBANO MICALI

Dezembro de 1977

Agradecimentos

Sou imensamente grato ao Prof. Artibano Micali pela orientação e estímulos recebidos durante o transcorrer desta pesquisa.

Agradeço ao Prof. Ubiratan D'Ambrósio, Diretor do IMECC, que muito contribuiu para tornar possível a realização deste trabalho.

A minha gratidão aos professores Nelo S. Allan, Antonio J. Engler e John E. David pelas estimulantes discussões sobre o assunto da minha tese.

ÍNDICE

Introdução

E.Witt , em seu principal trabalho [W] sobre formas quadráticas , introduziu a noção de invariantes para classificação de formas quadráticas sobre corpos de característica distinta de 2 e para tanto utilizou resultados da teoria de álgebras simples . Um trabalho semelhante foi feito por C.Arf para corpos de característica igual a 2 (cf. [A]) . T.A. Springer (cf.[Sp]) tratou o mesmo problema , porém sob um ponto de vista de cohomologia de grupos.

O objetivo deste trabalho é , essencialmente , a generalização para anéis locais das técnicas e resultados , sobre a cohomologia de formas quadráticas , obtidos por Springer em seu referido artigo . Nestas notas todo anel é comutativo com elemento unidade e todo módulo e unitário . A palavra álgebra significa álgebra associativa (não necessariamente comutativa) com elemento unidade . Além disso , todo homomorfismo de anéis (resp. álgebras) transforma elemento unidade em elemento unidade .

Inicialmente , demonstramos que se R é um anel local e (M,q) e (M,q_1) são R-espaços quadráticos , então q e q_1 são "S-equivalentes" , para alguma extensão galoisiana S de R ; isto é , é sempre possível construir uma extensão galoisiana S de R tal que os S-espaços quadráticos $(S\otimes_R M,q_1^S)$ e $(S\otimes_R M,q^S)$ sejam isomorfos (cf. Teor. 1.1) . Além disso , se R for também hen seliano , S poderá ser construida de forma a ser uma álgebra local (cf. Teor. 1.4) . Para a demonstração deste último fato utilizamos a seguinte caracterização de um anel local quadraticamente henseliano : "Toda extensão quadrática $R[x]$ de um anel local R , com $x^2 = bx + c$ e o polinômio $X^2 - bX - c$, de $R[X]$, irredutível sobre R , é local se , e somente se , R é quadraticamente henseliano" (cf. Prop. 1.2) . Também utilizamos , para as demonstrações dos Teoremas 1.1 e 1.4 , vários resultados da teoria de Galois para anéis comutativos segundo [AG] , [CHR] e [V].

No §2 introduzimos as noções de álgebra de Clifford $C(M,q)$, grupo de Clifford $CL(M,q)$, grupo ortogonal $O(M,q)$ e grupo ortogonal unimodular $SO(M,q)$ de um espaço quadrático (M,q) sobre um anel local R . Também mostramos , neste parágrafo , que a sequência de grupos

$$1 \longrightarrow U(R) \longrightarrow CL(M,q) \longrightarrow O(M,q) \longrightarrow 1$$

é exata . (cf. Teor. 2.1) . Este teorema é fundamental para a obtenção dos resultados do §5.

Os resultados do §3 , com exceção do Teorema 3.4 , podem ser encontrados em [KO] , Chap. II . O Teorema 3.4 é uma generalização , para anéis locais , do mesmo resultado demonstrado por Springer , para corpos (cf. [Sp] , Teorema do Apêndice).

No §4 , dado um espaço quadrático (M,q) sobre um anel local R , descrevemos as classes de equivalência de formas quadráticas q_1 , sobre M , que são S-equivalentes à q , para alguma extensão galoisiana S de R , com grupo G , como sendo elementos $c_S(q,q_1)$ do conjunto $H^1(G, O(S\otimes_R M,q^S))$ de 1-cohomologia (não abeliana) de G em $O(S\otimes_R M,q^S)$ (cf. Teor. 4.1) . Demonstramos também que se S é local e q e q_1 têm mesmo discriminante $\Delta(q) = \Delta(q_1)$ então $c_S(q,q_1) \in H^1(G, SO(S\otimes_R M,q^S))$,(cf. Teor. 4.2) .

No §5 , usando álgebras de Clifford e mais particularmente o Teorema 2.1 do §2 , mostramos como passar do conjunto $H^1(G, O(S\otimes_R M,q^S))$ para o grupo de 2-cohomologia $H^2(G, U(S))$ associando $c_S(q,q_1)$ a um elemento $\alpha_S(q,q_1) \in H^2(G, U(S))$. Mostramos aí que se S é local de corpo residual infinito , $\Delta(q) = \Delta(q_1)$ e $\alpha_S(q,q_1) = 1$, então as álgebras de Clifford $C(M,q)$ e $C(M,q_1)$ são isomorfas , (cf. Teor. 5.4) . Como consequência disto , mantidas as mesmas hipóteses sobre S e se o posto de M sobre R for 2 ou 3 , segue-se que os R-espaços quadráticos (M,q) e (M,q_1) são isomorfos se , e somente se , $\Delta(q) = \Delta(q_1)$ e $\alpha_S(q,q_1) = 1$,(cf. Teor. 5.6) .

No §6 , nos restringimos somente a anéis locais henselianos . Damos aí a noção de invariante de Hasse $h(q)$ de uma forma quadrática q , sobre um anel local henseliano R , como sendo um certo elemento do grupo $H^2(G, U(S))$ para uma certa extensão galoisiana local S de R , com grupo G e descrevemos á classe $\alpha_S(q,q_1)$ em termos de $\Delta(q)$, $\Delta(q_1)$, $h(q)$ e $h(q_1)$, para duas formas quadráticas q e q_1 S-equivalentes (cf. Lema 6.3) . Se , agora , o corpo residual de S for infinito , decorrerá deste Lema e do Teorema 5.6 que dois R-espaços quadráticos (M,q) e (M,q_1) com posto de M igual a 2 ou 3 , são isomorfos se , e somente se , as formas quadráticas q e q_1 têm mesmo discriminante e mesmo invariante de Hasse , (cf. Teor. 6.4).

1. <u>Módulos</u> <u>quadráticos</u>.

Sejam R um anel e M um R-módulo. Uma <u>forma</u> <u>quadrática</u> sobre M é uma aplicação $q: M \longrightarrow R$ tal que :

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

ii) a aplicação $\phi: M \times M \longrightarrow R$, definida por $\phi(x,y) = q(x+y)-q(x)-q(y)$ é R-bilinear e necessariamente simétrica. Todo R-módulo M munido de uma forma quadrática q será chamado um R-<u>módulo</u> <u>quadrático</u> e denotado por (M,q).

Dado um R-módulo quadrático (M,q) , indiquemos por M^* o dual de M(i.é. , $M^* = \mathrm{Hom}_R(M,R)$) e consideremos a aplicação $\varphi : M \longrightarrow M^*$, definida por $\varphi(x)(y) = \phi(x,y)$; $x,y \in M$. Quando φ é um isomorfismo de R-módulos dizemos que q é <u>não</u> <u>degenerada</u>. Todo R-módulo quadrático (M,q) , com M projetivo de tipo finito e q não degenerada , será chamado um R-<u>espaço</u> <u>quadrático</u>.

Se $f: R \longrightarrow S$ é um homomorfismo de anéis e (M,q) é um R-módulo quadrático , existe uma única forma quadrática $q^S: S\otimes_R M \longrightarrow S$ que torna comutativo o seguinte diagrama:

$$\begin{array}{ccc} M & \longrightarrow & R \\ {\scriptstyle f\otimes id_M}\downarrow & & \downarrow{\scriptstyle f} \\ S\otimes_R M & \longrightarrow & S \end{array}$$

, (ver [MR] , Chap.1,§3) .

A noção de discriminante de uma forma quadrática será descrita localmente.

Indiquemos por U(R) o grupo multiplicativo dos elemen-

tos inversíveis de R e consideremos os subconjuntos de R,
$R^o = \{x : x \in R \text{ e } 1-4x \in U(R)\}$ e $J = \{x-x^2 : x \in R \text{ e } 1-2x \in U(R)\}$.
O conjunto R^o, munido da operação $(x,y) \longmapsto x \circ y = x+y-4xy$, é um grupo abeliano e é imediato que J é um subgrupo de R^o. Indicamos por $G(R)$ o grupo quociente $R^o/_J$ de R^o por J. Se $2 \in U(R)$, $G(R) = U(R)/_{U^2(R)}$ e se $2 \notin U(R)$, $G(R) = R/_{\{x-x^2 \,:\, x \in R\}}$ (cf. $[MV]_1$ §7).

Admitamos, agora, que R é local e seja (M,q) um R-espaço quadrático. Se $2 \in U(R)$, existe uma base $\{x_1,..,x_n\}$ de M tal que

$$q\left(\sum_{i=1}^{n} \xi_i x_i\right) = \sum_{i=1}^{n} \alpha_i \xi_i^2 \quad , \text{ com } \alpha_i \in U(R),\ 1 \leq i \leq n ,$$

(cf. $[MV]_1$, §2, Lema 1). Se $2 \notin U(R)$, o posto de M é par e existe uma base $\{x_1,..,x_{2m}\}$ de M tal que

$$q\left(\sum_{i=1}^{2m} \xi_i x_i\right) = \sum_{i=1}^{m} \left(\alpha_i \xi_i^2 + \beta_i \xi_i \xi_{i+m} + \gamma_i \xi_{i+m}^2 \right)$$

com $\beta_i \in U(R)$, $1 \leq i \leq m$, (cf. $[MV]_1$, §3, Lema 2). O <u>discriminante</u> $\Delta(q)$ da forma quadrática q é um elemento de $G(R)$ descrito por:

$$\Delta(q) = \prod_{i=1}^{n} \alpha_i \pmod{U^2(R)} \ , \text{ se } 2 \in U(R)$$

e

$$\Delta(q) = \alpha_1\gamma_1 \circ \dots \circ \alpha_m\gamma_m \pmod{J} \ , \text{ se } 2 \notin U(R).$$

Um homomorfismo de R-módulos quadráticos (M,q) e (M_1,q_1) é uma aplicação R-linear $t: M_1 \longrightarrow M$ que torna comutativo o seguinte diagrama:

$$\begin{tikzcd} M_1 \arrow[r, "t"] \arrow[dr, "q_1"'] & M \arrow[d, "q"] \\ & R \end{tikzcd}$$

Quando t é um isomorfismo de R-módulos dizemos que q e q_1 são equivalentes e denotamos $(M_1,q_1) \cong (M,q)$ ou simplesmente $q_1 \cong q$, caso não haja confusão possível.

A seguir , trataremos essencialmente do seguinte problema : dados dois R-espaços quadráticos (M,q) e (M,q_1) , estudar a existência de extensões galoisianas S de R tais que q_1^S e q^S sejam equivalentes.

Sejam S um anel, G um grupo finito de automorfismos de S e $R = S^G$. Dizemos que S é uma extensão galoisiana de R , com grupo G , se S é uma R-álgebra separável que , como R-módulo , é projetivo de tipo finito e posto igual a $[G:1]$. Outra noção fortemente utilizada nos resultados que apresentaremos neste parágrafo é a de extensão quadrática de um anel R . Uma R-álgebra S é uma extensão quadrática de R se S é separável e , como R-módulo é projetivo de tipo finito e posto 2. Toda extensão quadrática de um anel R é também uma extensão galoisiana de R(cf. [Sm], §0 e [MR], Cap. 2 ,§4). No cso em que R é local , uma extensão quadrática de R é do tipo $R[x]$, com $x^2=bx+c$, onde b e c são elementos de R tais que $b^2+4c \in U(R)$. O grupo de Galois de $R[x]$ sobre R é cíclico de ordem 2 e gerado por $\sigma : x \longmapsto b-x$. Para mais detalhes sobre extensões galoisianas e extensões quadráticas de um anel, enviamos o leitor à bibliografia (ver, por exemplo, [AG], [CHR] e [V] para extensões galoisianas e [MR], $[MV]_3$ e [Sm] para extensões quadráticas).

Para os resultados que se seguirão assumiremos que R é um anel local .

<u>Teorema 1.1</u> - Sejam (M,q) e (M,q_1) dois R-espaços quadráticos. Então, sempre existe uma extensão galoisiana S de R , tal que $(S\otimes_R M, q_1^S) \simeq (S\otimes_R M, q^S)$.

<u>Demonstração</u> : Em toda a demonstração $\otimes$ significará $\otimes_R$.

i) <u>$2 \in U(R)$</u>:

Neste caso existem bases $\{x_1,..,x_n\}$ e $\{y_1,..,y_n\}$ de M tais que

$$q\left(\sum_{i=1}^{n} \xi_i x_i\right) = \sum_{i=1}^{n} \alpha_i \xi_i^2 .$$

e

$$q\left(\sum_{i=1}^{n} \xi_i y_i\right) = \sum_{i=1}^{n} \beta_i \xi_i^2 \quad , \text{ com } \alpha_i,\ \beta_i \in U(R), (\text{cf. } [MV]_1 ,$$

§2,Lema 1).

Consideremos $S = \bigotimes_{1\leq i\leq n} (R[\sqrt{\alpha_i}] \otimes R[\sqrt{\beta_i}])$; $R[\sqrt{\alpha_i}]$ e $R[\sqrt{\beta_i}]$ são extensões quadráticas de R e , consequentemente , S é uma extensão galoisiana de R , como produto tensorial de extensões galoisianas de R.(cf. [AG],Prop.A8). Vemos, então que a extensão S, assim construida , possue elementos z_i, $1 \leq i \leq n$, tais que $z_i^2 = \alpha_i^{-1}\beta_i$. O isomorfismo de S-espaços quadráticos procurado é a aplicação S-linear $t:S\otimes M \longrightarrow S\otimes M$, tal que $t(1\otimes y_i) = z_i\otimes x_i$, $1\leq i\leq n$.

ii) $2\notin U(R)$:

Neste caso o posto de M é par e existem bases $\{x_1,\ldots,x_{2m}\}$ e $\{y_1,\ldots,y_{2m}\}$ tais que

$$q(\sum_{i=1}^{2m}\xi_i x_i) = \sum_{i=1}^{m}(\alpha_i\xi_i^2 + \beta_i\xi_i\xi_{i+m} + \gamma_i\xi_{i+m}^2)$$

e

$$q_1(\sum_{i=1}^{2m}\xi_i y_i) = \sum_{i=1}^{m}(\lambda_i\xi_i^2 + \mu_i\xi_i\xi_{i+m} + \nu_i\xi_{i+m}^2),$$ com

$\beta_i, \mu_i \in U(R)$, $1\leq i\leq m$,(cf. [MV]$_1$,§3,Lema 2). Pode supor-se , sem perda de generalidade , que os α_i e λ_i , $1\leq i\leq m$, também são inversíveis em R. Como $2\notin U(R)$ então $(\alpha_i^{-1}\beta_i)^2 + 4(-\alpha_i^{-1}\gamma_i)$ e $(\lambda_i^{-1}\mu_i)^2 + 4(-\lambda_i^{-1}\nu_i)$ são inversíveis em R, e consequentemente podemos considerar as extensões quadráticas $R[v_i]$ e $R[w_i]$ de R , onde $v_i^2 = -\alpha_i^{-1}\beta_i v_i - \alpha_i^{-1}\gamma_i$ e $w_i^2 = -\lambda_i^{-1}\mu_i w_i - \lambda_i^{-1}\nu_i$, $1\leq i\leq m$. Basta então , considerarmos $S = \bigotimes_{1\leq i\leq m}(R[v_i]\otimes R[w_i])$ e teremos o resultado desejado ; isto é , pode verificar-se facilmente que S, assim construida, é uma extensão galoisiana de R(cf. [AG] ,Prop.A8) e que $(S\otimes M, q_1^S) \simeq (S\otimes M, q^S)$. ∎

A extensão galoisiana S de R , construida no Teorema 1.1 é,em geral , semi-local. No entanto, é também possível mostrar a existência de uma extensão galoisiana local S de R que satisfaça à mesma exigência do Teorema 1.1 . Para tanto, iremos supor que R, além de local , seja também henseliano e necessitaremos da seguinte proposição:

<u>Proposição 1.2</u> - Toda extensão quadrática $R[x]$ de R , com $x^2=bx+c$ e o polinômio X^2-bX+c, de $R[X]$, irredutível sobre R, é local se, e somente se R é quadraticamente henseliano.

Antes de demonstrarmos esta proposição, observamos que um anel local R, de ideal maximal $\mathfrak{m}$, é <u>quadraticamente henseliano</u> se todo polinômio da forma $X^2+\alpha X+\beta \in R[X]$ que admite duas raízes distintas em $R/\mathfrak{m}$, módulo $\mathfrak{m}R[X]$, também admite duas raízes (necessariamente distintas) em R. Obviamente , todo anel local henseliano é quadraticamente henseliano.

<u>Demonstração</u> :(daProp.1.2)

Indiquemos por $\mathfrak{m}$ o único ideal maximal do anel local R e seja $R[x]$, com $x^2=bx+c$, uma extensão quadrática de R. Admitamos que R seja quadraticamente henseliano e que o polinômio X^2-bX-c, de $R[X]$, seja irredutível sobre R. Mostraremos que $R[x]$ é local verificando que $\mathrm{rad}(R[x]) = \mathfrak{m}R[x]$ é o seu único ideal maximal ou , equivalentemente , que todo elemento de $R[x] - \mathfrak{m}R[x]$ é inversível em $R[x]$.

Um elemento $z \in R[x]$ é inversível em $R[x]$ se, e somente se , sua <u>norma</u> $N(z) = z\sigma(z) \in R$ é inversível em R(σ é o R-automorfismo de $R[x]$, dado por $\sigma: x \longmapsto b-x$). Seja $\alpha-\beta x \in R[x] - \mathfrak{m}R[x]$ $N(\alpha-\beta x) = (\alpha-\beta x)(\alpha-\beta(b-x)) = \alpha^2-\alpha\beta b-\beta^2 c$. Se $c \in \mathfrak{m}$, então $X^2-\bar{b}X-\bar{c}$ é redutível sobre $R/\mathfrak{m}$ e, consequentemente $X^2-\bar{b}X-\bar{c}$ tem duas raízes em $R/\mathfrak{m}$, necessariamente distintas, pois $\bar{b}^2+4\bar{c} \neq 0$. Logo, X^2-bX-c tem duas raízes em R , pois R é quadraticamente henseliano, o que significa que X^2-bX-c é redutível sobre R, o que é absurdo. Portanto $c \notin \mathfrak{m}$. Se $\alpha \in \mathfrak{m}$, então $\beta \notin \mathfrak{m}$, de onde segue-se que $N(\alpha - \beta x) \notin \mathfrak{m}$, e consequentemente , $\alpha - \beta x$ é inversível em $R[x]$. Analogamente , se $\beta \in \mathfrak{m}$, então $\alpha \notin \mathfrak{m}$ e novamente teremos $\alpha - \beta x$ inversível em $R[x]$.

Assumimos , finalmente, que $\alpha \notin \mathfrak{m}$ e $\beta \notin \mathfrak{m}$. Neste caso, se $N(\alpha - \beta x) \in \mathfrak{m}$ então $\bar{\alpha}^2-\bar{b}\bar{\alpha}\bar{\beta}-\bar{\beta}^2\bar{c} = \bar{0}$ em $R/\mathfrak{m}$, de onde segue-se que $(\frac{\bar{\alpha}}{\bar{\beta}})^2-\bar{b}(\frac{\bar{\alpha}}{\bar{\beta}})-\bar{c} = \bar{0}$, ou seja X^2-bX-c é redutível sobre $R/\mathfrak{m}$ e, consequentemente , X^2-bX-c é redutível sobre R ,o que é absurdo. Logo ,$N(\alpha - \beta x) \notin \mathfrak{m}$ e portanto $\alpha - \beta x$ é inversível em $R[x]$.

Reciprocamente , seja $X^2+\alpha X+\beta \in R[X]$ um polinômio que admite raízes distintas em $R/\mathfrak{m}$, módulo $\mathfrak{m}R[X]$. Logo, $\bar{\alpha}^2-4\bar{\beta} \neq \bar{0}$ ou, equivalentemente , $\alpha^2-4\beta \in U(R)$ e, consequentemente o anel $R[x]$ com $x^2=-\alpha x-\beta$, é uma extensão quadrática de R. Por outro lado, se $\bar{a}$ é uma das raízes de $X^2+\bar{\alpha}X+\bar{\beta}$ em $R/\mathfrak{m}$, então o elemento $(a-x)$ de $R[x]-\mathfrak{m}R[x]$ não é inversível em $R[x]$, o que significa que $R[x]$ não é local. Logo, o polinômio $X^2+\alpha X+\beta$ não pode ser irredutível sobre R (pois, caso contrário , $R[x]$ seria local), ou seja $X^2+\alpha X+\beta$ admite duas raízes (necessariamente distintas) em R e isto mostra que R é quadraticamente henseliano. ∎

<u>Corolário 1.3</u> - Seja $R[x]$, com $x^2=bx+c$, uma extensão

quadrática de R. Se R é henseliano e o polinômio X^2-bX-c , de $R[X]$, é irredutível sobre R , então $R[x]$ é local e henseliano.

Demonstração :

Como R é henseliano , e , portanto, quadraticamente henseliano , segue-se da Prop.1.2 que $R[x]$ é local. Do fato de $R[x]$ ser inteiro sobre R , pois $R[x]$ é um R-módulo livre de posto 2 , segue-se que $R[x]$ é henseliano(cf. [N], Chap.VII,§43,Cor.16). ∎

Teorema 1.4 - Sejam (M,q) e (M,q_1) dois R-espaços quadráticos. Se R é henseliano, existe sempre uma extensão galoisiana local S de R tal que $(S\otimes_R M,q_1^S) \simeq (S\otimes_R M,q^S)$.

Demonstração:

Repetimos aqui um raciocínio análogo ao visto no Teorema 1.1 . Observamos , também, que em toda a demonstração $\otimes$ significará $\otimes_R$.

i) $2 \in U(R)$:

Sejam $\{x_1,\ldots,x_n\}$ e $\{y_1,\ldots,y_n\}$ bases de M tais que

$$q\left(\sum_{j=1}^n \xi_j x_j\right) = \sum_{j=1}^n \alpha_j \xi_j^2$$

e

$$q_1\left(\sum_{j=1}^n \xi_j y_j\right) = \sum_{j=1}^n \beta_j \xi_j^2 \quad , \text{ com } \alpha_j,\ \beta_j \in U(R)\ ,(\text{cf.}$$

$[MV]_1$,§2,Lema 1) e consideremos as extensões quadráticas $R[\gamma_j]$ e $R[\gamma_{n+j}]$ de R , com $\gamma_j^2 = \alpha_j$ e $\gamma_{n+j}^2 = \beta_j$, $1 \leq j \leq n$. Seja I o conjunto de índices i tais que $X^2-\gamma_i^2$ seja irredutível sobre $\bigotimes_{k\neq i} R[\gamma_k]$ e seja $S = \bigotimes_{i\in I} R[\gamma_i]$. A R-álgebra S, assim construida , é uma extensão galoisiana de R (cf. [AG],Prop.A8) e pode verificar-se facilmente que $(S\otimes M, q_1^S) \simeq (S\otimes M, q^S)$.

Resta apenas a verificação de que S é local e isto será feito por indução sobre o cardinal de I. Se $I = \{i_1,\dots,i_r\}$, com $1 \leq r \leq 2n$, então $S = R[\gamma_{i_1}]\otimes \dots \otimes R[\gamma_{i_r}]$. $R[\gamma_{i_1}]$ é, claramente , uma extensão quadrática de R , local e henseliana , pois $X^2-\gamma_{i_1}^2$ é irredutível sobre $\bigotimes_{k\neq 1} R[\gamma_{i_k}]$ e , em particular , sobre R (cf. Cor. 1.3) . Admitamos (hipótese de indução) que $S' = R[\gamma_{i_1}]\otimes \dots \otimes R[\gamma_{i_s}]$, com $1 \leq s \leq r$, seja local e henseliana. A R-álgebra $S'\otimes R[\gamma_{i_{s+1}}] \simeq S'\otimes R[X]/(X^2-\gamma_{i_{s+1}}^2) \simeq S'[X]/(X^2-\gamma_{i_{s+1}}^2)$ é uma extensão quadrática de S' e como $X^2-\gamma_{i_{s+1}}^2$ é irredutível sobre S' (pois é irredutível sobre $\bigotimes_{k\neq s+1} R[\gamma_{i_k}]$) , concluimos que $S'\otimes R[\gamma_{i_{s+1}}]$ é local e henseliana (cf. Cor. 1.3) . Portanto $S = R[\gamma_{i_1}]\otimes \dots \otimes R[\gamma_{i_r}]$ é uma extensão galoisiana local de R.

ii) $2 \notin U(R)$:

Neste caso o posto de M é par e sejam $\{x_1,\dots,x_{2m}\}$ e $\{y_1,\dots,y_{2m}\}$ bases de M tais que

$$q\left(\sum_{j=1}^{2m} \xi_j x_j\right) = \sum_{j=1}^{m}\left(\alpha_j \xi_j^2 + \beta_j \xi_j \xi_{j+m} + \gamma_j \xi_{j+m}^2\right)$$

e

$$q_1\left(\sum_{j=1}^{2m} \xi_j y_j\right) = \sum_{j=1}^{m}\left(\lambda_j \xi_j^2 + \mu_j \xi_j \xi_{j+m} + \nu_j \xi_{j+m}^2\right) , \text{ com}$$

$\alpha_j, \lambda_j, \beta_j$ e μ_j inversíveis em R, $1 \leq j \leq m$, (cf. $[MV]_1$, §3 ,Lema 2) . Consideremos as extensões quadráticas $R[w_j]$ e $R[w_{j+m}]$ de R com $w_j^2 = (-\alpha_j^{-1}\beta_j)\, w_j + (-\alpha_j^{-1}\gamma_j)$ e $w_{j+m}^2 = (-\lambda_j^{-1}\mu_j) w_{j+m} + (-\lambda_j^{-1}\nu_j)$, $1 \leqslant j \leqslant m$.

Seja I o conjunto de índices i tais que $X^2 + \alpha_j^{-1}\beta_j X + \alpha_j^{-1}\gamma_j$ (se i=j) ou $X^2 + \lambda_j^{-1}\mu_j X + \lambda_j^{-1}\nu_j$ (se i=j+m) seja irredutível sobre $\bigotimes_{k \neq i} R[w_k]$. Seja $S = \bigotimes_{i \in I} R[w_i]$. Verifica-se , como em i), que S é uma extensão galoisiana local de R tal que $(S \otimes M, q_1^S) \simeq (S \otimes M, q^S)$. ∎

<u>Observação</u> : A extensão galoisiana S de R , construida no Teorema 1.4 , além de local , é também henseliana.

2. <u>Grupos ortogonais e álgebras de Clifford</u>.

Sejam R um anel e (M,q) um R-módulo quadrático . A <u>álgebra de Clifford</u> de (M,q) , que indicaremos por C(M,q) , é o quociente da álgebra tensorial T(M) pelo ideal bilátero I(q) , de T(M) , gerado pelos elementos da forma $x^2 - q(x)1_{T(M)}$, para todo $x \in M$.

Observamos que C(M,q) é solução do problema universal posto pelas aplicações R-lineares $g: M \longrightarrow A$, onde A é uma R-álgebra , tais que $(g(x))^2 = q(x)1_A$, para todo $x \in M$.

Se graduamos T(M) sobre $\mathbb{Z}/_{2\mathbb{Z}}$, fazendo $T(M) = T_o(M) \oplus T_1(M)$, onde $T_o(M) = \bigoplus_{i \geqslant 0} T^{2i}(M)$ e

$T_1(M) = \bigoplus_{i \geq 0} T^{2i+1}(M)$, com $T^j(M) = \otimes^j_R(M)$, então o ideal $I(q)$ é homogêneo em relação a essa graduação e consequentemente $C(M,q)$, como álgebra graduada sobre $\mathbb{Z}/_{2\mathbb{Z}}$, é descrita por $C(M,q) = C_0(M,q) \oplus C_1(M,q)$, onde $C_0(M,q)$ é a subálgebra gerada pelos elementos da forma $xy(\text{mod } I(q))$, com $x,y \in M$.

O conjunto dos elementos $x \in C(M,q)$ tais que $xy=yx$, para todo $y \in C(M,q)$, é uma subálgebra de $C(M,q)$ chamada <u>centro</u> de $C(M,q)$ e denotada por $Z(C(M,q))$. O centro de $C_0(M,q)$ é definido de modo análogo e denotado por $Z(C_0(M,q))$.

Se (M,q) é um R-espaço quadrático , onde o posto de M é par , então $Z(C(M,q)) = R$ e $Z(C_0(M,q))$ é um R-módulo projetivo de tipo finito e posto 2 . Se o posto de M é ímpar então $Z(C(M,q))$ é um R-módulo projetivo de tipo finito e posto 2 e $Z(C_0(M,q)) = R$ (cf. $[MV]_1$,§4). Localmente , se $2 \notin U(R)$ então $Z(C_0(M,q))$ é uma extensão quadrática de R , do tipo $R[x]$, com $x^2=x-\Delta(q)$. Além disso, se (M,q) e (M,q_1) são dois R-espaços quadráticos , então $Z(C_0(M,q_1)) \cong Z(C_0(M,q))$, como R-álgebras , se, e somente se $\Delta(q_1) = \Delta(q)$ em $G(R)$, (cf. [H],§2 e §3).

Um elemento $x \in C(M,q)$ será chamado <u>homogêneo de grau</u> $\partial x = i$, se $x \in C_i(M,q)$. Para qualquer subconjunto E de $C(M,q)$ denotamos por hE o conjunto $(E \cap C_0(M,q)) \cup (E \cap C_1(M,q))$ dos elementos homogêneos de E .

Se (M,q) é um R-espaço quadrático , pode mostrar-se que M se identifica à um subespaço de $C_1(M,q)$. Se M é um R-módulo li vre de posto n, então $C(M,q)$ é também um R-módulo livre e seu posto é 2^n. Todo homomorfismo $t:(M_1,q_1) \longrightarrow (M,q)$ de R-espaços quadráticos se estende a um homomorfismo de R-álgebras $C(t):C(M_1,q_1) \longrightarrow C(M,q)$ tal que $C(t)(M_1) \subset M$. Reciprocamente, todo homomorfismo de R-álgebras $t':C(M_1,q_1) \longrightarrow C(M,q)$, tal que $t'(M_1) \subset M$, dá origem , por restrição a M_1 , a um homomorfismo de R-espaços quadráticos $t=t'|_{M_1} :(M_1,q_1) \longrightarrow (M,q)$ tal que $C(t)=t'$. Ainda , devido q e q_1 serem não degeneradas (ver [MVL],Lema 1.4) , podemos também afirmar que $C(t)$ é injetivo, sobrejetivo ou bijetivo se, e somente se t é, respectivamente , injetivo, sobrejetivo ou bijetivo.

Se $R \longrightarrow S$ é um homomorfismo de anéis e (M,q) é um R-módulo quadrático , então $(S\otimes_R M, q^S)$ é um S-módulo quadrático e $C(S\otimes_R M, q^S)$ se identifica naturalmente à S-álgebra $S\otimes_R C(M,q)$. Para mais detalhes sobre álgebras de Clifford enviamos o leitor à bibliografia , (ver, por exemplo , $[MV]_i$, i=1,2,3 , [MR], $[B]_i$, i=1,2 e [Bo]).

Em seguida , assumiremos que R seja um anel local e que (M,q) denotará sempre um R-espaço quadrático.

Um R-automorfismo $t:M \longrightarrow M$ será chamado <u>ortogonal</u> se o diagrama

$$\begin{tikzcd} M \arrow[rr, "t"] \arrow[dr, "q"'] & & M \arrow[dl, "q"] \\ & R & \end{tikzcd}$$

for comutativo.

O conjunto dos R-automorfismos ortogonais de (M,q) é dotado de uma estrutura natural de grupo chamado <u>grupo ortogonal</u> de (M,q) e será denotado por $O(M,q)$ ou simplesmente $O(q)$, caso não haja confusão possível. O <u>grupo ortogonal unimodular</u> (ou <u>especial</u>), denotado por $SO(M,q)$ ou simplesmente $SO(q)$, é um subgrupo de $O(q)$ definido por $SO(q)=\{t : t\in O(q)$ e $C(t)|_{Z(C_o(M,q))} = id\}$ se $2 \notin U(R)$. Se $2 \in U(R)$, observamos que se $t \in O(q)$ então $d(t) = \pm 1$, onde $d(t)$ denota o <u>determinante</u> da matriz de t em relação a uma base de M. Neste caso, definimos $SO(q) = \{t : t\ O(q)$ e $d(t) = 1\}$.

Se $u \in C(M,q)$ é um elemento homogêneo e inversível, definimos um R-automorfismo π_u de $C(M,q)$, dado por $\pi_u(x) = (-1)^{\partial u \partial x}\ uxu^{-1}$, para todo $x \in hC(M,q)$. Obviamente, se $\pi_u(M)\subset M$, $\pi_u \in O(q)$ e $\pi_u \in SO(q)$ se, e somente se $u \in C_o(M,q)$, (cf. $[MV]_2$ e $[B]_2$). O conjunto $CL(M,q)$ (ou simplesmente $CL(q)$) dos elementos $u \in U(hC(M,q))$ tais que $\pi_u \in O(q)$ tem uma estrutura de grupo, chamado <u>grupo de Clifford</u> de (M,q). Naturalmente, existe um homomorfismo de grupos $\pi : CL(q) \longrightarrow O(q)$ dado por $\pi(u) = \pi_u$, para todo $u \in CL(q)$.

<u>Teorema 2.1</u> - A sequência de grupos

$$1 \longrightarrow U(R) \longrightarrow CL(q) \longrightarrow O(q) \longrightarrow 1$$

é exata.

<u>Demonstração</u> : Ver $[B]_1$, Chap.V, Teor.3.9 e $[B]_2$, §3, Prop. 3.3.2. ∎

Contudo, observamos que este mesmo resultado foi obti_ do por Klingenberg (cf. [K]) para um anel local R , com $2 \in U(R)$ usando o fato , também por ele demonstrado , de que $O(q)$ é gerado por <u>isometrias</u> do tipo $\sigma_x : y \longmapsto y - \dfrac{\phi(x,y)}{q(x)}\, x$, com $x, y \in M$ e $q(x) \in U(R)$. Klingenberg demonstrou que se $t \in O(q)$, existem elementos $x_1, \ldots, x_r$ em M tais que $q(x_i) \in U(R)$, $1 \leq i \leq r$ e $C(t)(y) = (-1)^r (x_1 \ldots x_r) y (x_1 \ldots x_r)^{-1}$, para todo $y \in M$ em $C(M,q)$, onde $r \equiv 0 (\mathrm{mod}\ 2)$ se , e somente se $t \in SO(q)$. A verificação de que , para cada $t \in O(q)$, o elemento $a_t = x_1 \ldots x_r$ é unico , à menos de um fator em $U(R)$, é imediata.

No caso em que $2 \notin U(R)$, Knebusch [Kn] verificou que $O(q)$ também é gerado por isometrias , como descritas acima , exceto no caso em que o posto de M é 4 , o corpo residual $R/\mathfrak{m}$ ($\mathfrak{m}$ denota o único ideal maximal de R) de R é $\mathbb{Z}/_{2\mathbb{Z}}$ e $(R/\mathfrak{m} \otimes_R M, q^{R/\mathfrak{m}})$ é um <u>espaço hiperbólico</u>(isto é , $(R/\mathfrak{m} \otimes_R M, q^{R/\mathfrak{m}}) \cong (N \oplus N^*, q')$, com N um $R/\mathfrak{m}$ -submódulo de $R/\mathfrak{m} \otimes_R M$, $N^* = \mathrm{Hom}_{R/\mathfrak{m}}(N, R/\mathfrak{m})$ e $q' : N \oplus N^* \longrightarrow R/\mathfrak{m}$ dada por $q'(x,f) = f(x)$, para todo $x \in N$ e $f \in N^*$). Usando este fato, também pode obter-se resultados análogos aos obtidos por Klingenberg e descritos acima.

3. Cohomologia não abeliana.

Sejam G e G' dois grupos tais que G atua sobre G' como grupo de operadores ; isto é , existe uma aplicação $G \times G' \longrightarrow G'$ denotada por $(g,g') \longmapsto g * g'$ e que verifica as seguintes condições :

$$g * 1_{G'} = 1_{G'}$$
$$(g_1 g_2) * g' = g_1 * (g_2 * g')$$
$$g * (g'_1 g'_2) = (g * g'_1)(g * g'_2)$$

quaisquer que sejam $g_1, g_2, g \in G$ e $g'_1, g'_2, g' \in G'$.

Toda aplicação $f: G \longrightarrow G'$ que verifica $f(g_1 g_2) = (g_1 * f(g_2))f(g_1)$ é chamada um cociclo e dizemos que dois cociclos f e f' são cohomólogos se existe $g' \in G'$ tal que $f'(g) = (g * g')f(g)g'^{-1}$, para todo $g \in G$. Definimos assim uma relação de equivalência sobre o conjunto dos cociclos e o conjunto quociente será chamado conjunto de 1-cohomologia de G com valores em G' e denotado por $H^1(G, G')$. Observemos, ainda, que se G' é abeliano então o conjunto dos cociclos , munido da operação "multiplicação pontual" , é um grupo ; a relação de equivalência , acima descrita é compatível com essa operação e consequentemente $H^1(G, G')$ também tem uma estrutura de grupo abeliano e é , neste caso, chamado grupo de 1-cohomologia de G com valores em G'.

No que segue , assumiremos que R seja um anel e S uma extensão galoisiana de R , com grupo G.

Sejam (N) uma classe de isomorfismos de R-módulos re -

presentada por N e M um R-módulo livre de posto finito n . Dizemos que (N) é <u>uma forma torcida de M por S</u> se existir um isomorfismo de S-módulos $\beta : S\otimes_R M \longrightarrow S\otimes_R N$; isto é , se $S\otimes_R N$ for um S-módulo livre de posto n . Denotamos por $\mathcal{F}_S(M)$ o conjunto das formas torcidas de M por S.

<u>Proposição 3.1</u> - Se R é tal que todo R-módulo projetivo de tipo finito e posto constante é livre , então $\mathcal{F}_S(M) = \{(M)\}$, para todo R-módulo livre M de posto finito.

<u>Demonstração</u> : imediata. ■

Consideremos agora um R-módulo livre M , de posto finito $n \geqslant 1$ e denotemos por $Gl_n(S)$ o grupo dos automorfismos do S-módulo $S\otimes_R M$. O grupo G age naturalmente sobre $Gl_n(S)$ do seguinte modo:

$(\sigma t)(x) = \sigma(t(\sigma^{-1}(x)))$, quaisquer que sejam $\sigma \in G$, $t \in Gl_n(S)$ e $x \in S\otimes_R M$, onde $\sigma : S\otimes_R M \longrightarrow S\otimes_R M$ é dada por $\sigma(s\otimes m) = \sigma(s)\otimes m$, para todo $s \in S$ e $m \in M$.

O que tencionamos é mostrar que os conjuntos $\mathcal{F}_S(M)$ e $H^1(G, Gl_n(S))$ são equipotentes.

Seja $(N) \in \mathcal{F}_S(M)$. Sabemos que existe um isomorfismo de S-módulos $\beta : S\otimes_R M \longrightarrow S\otimes_R N$. Consideremos , para todo $\sigma \in G$, as aplicações $\theta_\sigma : S\otimes_R M \longrightarrow S\otimes_R M$ tais que $\theta_\sigma = \sigma.\beta^{-1}.\sigma^{-1}.\beta$. Observemos que $\sigma.\beta^{-1}.\sigma^{-1}$ é claramente um isomorfismo de $S\otimes_R N$ sobre $S\otimes_R M$ e , obviamente , $\theta_\sigma \in Gl_n(S)$ e $\theta_{\sigma.\tau} = (\sigma\theta_\tau).\theta_\sigma$, quaisquer que sejam $\sigma, \tau \in G$. Assim , a aplicação $f_\beta : G \longrightarrow Gl_n(S)$, definida por $f_\beta(\sigma) = \theta_\sigma = \sigma.\beta^{-1}.\sigma^{-1}.\beta$, para todo $\sigma \in G$, é um cociclo . Além disso , se $\beta' : S \otimes_R M \longrightarrow S \otimes_R N$ é um outro isomorfismo de S-módulos e $f_{\beta'}$ é o cociclo correspondente , tomando $\alpha = \beta'^{-1}.\beta \in Gl_n(S)$ temos :

$$\begin{aligned} f_{\beta'}(\sigma)\alpha &= \sigma.\beta'^{-1}.\sigma^{-1}\beta'.\beta'^{-1}.\beta = \sigma.\beta'^{-1}.\sigma^{-1}.\beta \\ &= (\sigma.\beta'^{-1}.\beta.\sigma^{-1})(\sigma\beta^{-1}.\sigma^{-1}.\beta) = (\sigma\alpha)f_\beta(\sigma) \quad , \end{aligned}$$

ou seja

$f_{\beta'}(\sigma) = (\sigma\alpha).f_\beta(\sigma).\alpha^{-1}$, para todo $\sigma \in G$, e isto mostra que f_β e $f_{\beta'}$, são cohomólogos .

Com isto vemos que existe uma aplicação $F: \mathcal{J}_S(M) \longrightarrow H^1(G, Gl_n(S))$ dada por $F((N)) = [f_\beta]$, onde $\beta: S \otimes_R M \longrightarrow S \otimes_R N$ é um isomorfismo de S-módulos . Observamos ainda , pelo que vimos acima , que a aplicação F não depende da escolha do isomorfismo β .

Sejam (N) e (N') elementos de $\mathcal{J}_S(M)$ tais que $F((N)) = F((N'))$. Isto significa que existem isomorfismos de S-módulos $\beta: S \otimes_R M \longrightarrow S \otimes_R N$ e $\beta' : S \otimes_R M \longrightarrow S \otimes_R N$ tais que f_β e $f_{\beta'}$, são cociclos cohomólogos . Logo , existe $\alpha \in Gl_n(S)$ tal que $f_{\beta'}(\sigma) = (\sigma\alpha)f_\beta(\sigma)\alpha^{-1}$, para todo $\sigma \in G$, de onde tiramos $\sigma.\beta'^{-1}.\sigma^{-1}.\beta'.\alpha = \sigma.\alpha.\sigma^{-1}.\sigma.\beta^{-1}.\sigma^{-1}.\beta$ ou seja , $\sigma.\beta'.\alpha.\beta^{-1} = \beta'.\alpha.\beta^{-1}.\sigma$. Então , $\beta'.\alpha.\beta^{-1} = id_S \otimes \gamma$, onde $\gamma : N \longrightarrow N'$ é um isomorfismo de R-módulos ,(cf. [KO], Chap.II, Prop.5.2). Portanto (N') = (N) e consequentemente F é injetiva .

Seja $[f] \in H^1(G, Gl_n(S))$ e consideremos

$\sigma^* = (f(\sigma))^{-1}\cdot\sigma : S\otimes_R M \longrightarrow S\otimes_R M$, para todo $\sigma \in G$. É imediato que os σ^* são aplicações aditivas e semi-lineares em relação a S. Além disso , $(\sigma\tau)^* = (f(\sigma\tau))^{-1}\cdot\sigma\tau = ((\sigma f(\tau))f(\sigma))^{-1}\cdot\sigma\tau = (f(\sigma))^{-1}\cdot(\sigma f(\tau))^{-1}\cdot\sigma\tau$ $= (f(\sigma))^{-1}\cdot\sigma(f(\tau))^{-1}\cdot\sigma^{-1}\cdot\sigma\tau = ((f(\sigma))^{-1}\cdot\sigma).((f(\tau))^{-1}\cdot\tau) = \sigma^*\cdot\tau^*$, quais - quer que sejam $\sigma, \tau \in G$. Logo , existem um R-módulo N e um iso - morfismo de S-módulos $\eta : S\otimes_R N \longrightarrow S\otimes_R M$ tais que $\sigma^*\cdot\eta = \eta\sigma$, para todo $\sigma \in G$, (cf. [KO] , Chap.II, Prop.5.1). Disto deduz-se facilmente que (N) é uma forma torcida de M por S e que $F((N)) = [f_{\eta^{-1}}]$ $= [f]$, o que mostra que F é sobrejetiva. Demonstramos, assim o seguinte teorema.

<u>Teorema 3.2</u> - $H^1(G, Gl_n(S))$ e $\mathcal{F}_S(M)$ são conjuntos equipotentes.

Decorre imediatamente da Prop.3.1 e deste teorema o seguinte corolário .

<u>Corolário 3.3</u> - Se R é tal que todo R-módulo projetivo de tipo finito e posto constante é livre , então $H^1(G, Gl_n(S))$ $= 0$; isto é , para todo cociclo $f : G \longrightarrow Gl_n(S)$ existe um elemento $\alpha \in Gl_n(S)$ tal que $f(\sigma) = (\sigma\alpha)\alpha^{-1}$, para todo $\sigma \in G$.

Admitamos , agora , que R e S sejam locais , de ideais maximais $\mathfrak{m}$ e $\mathfrak{m}S$, respectivamente e cujos respectivos corpos residuais $R/\mathfrak{m}$ e $S/\mathfrak{m}S$ sejam infinitos . O teorema seguinte é , no caso de extensões galoisianas locais de um anel local , uma generalização do corolário acima enunciado .

Teorema 3.4 - Seja A uma S-álgebra, que como S-módulo é livre de posto finito. Se G se estende a um grupo de automorfismos de A, então $H^1(G, U(A)) = 0$.

Demonstração :

Seja $f \in H^1(G, U(A))$ e consideremos o elemento $\sum_{\sigma \in G} f(\sigma) X_\sigma$ da $S[X_\sigma : \sigma \in G]$-álgebra $A[X_\sigma : \sigma \in G]$. A norma deste elemento, em relação à $S[X_\sigma : \sigma \in G]$, denotada por $N(\sum_{\sigma \in G} f(\sigma) X_\sigma)$, é um polinômio de $S[X_\sigma : \sigma \in G]$, (cf. [Bo], Chap. 8, §12). Por outro lado, $S/\mathfrak{m}S$ é um corpo extensão de Galois de $R/\mathfrak{m}$, cujo grupo de Galois $\overline{G}$ consiste dos elementos $\overline{\sigma}$ dados por $\overline{\sigma}(\overline{s}) = \overline{\sigma(s)}$, para todo $s \in S$ e $\sigma \in G$ e tais que $\overline{\sigma} = \overline{\tau}$ se, e somente se, $\sigma = \tau$, quaisquer que sejam $\sigma, \tau \in G$ (cf. [CHR], §1, Lema 7). Além disso, é de verificação imediata que $N(\sum_{\overline{\sigma} \in \overline{G}} f(\overline{\sigma}) X_{\overline{\sigma}}) \in S/\mathfrak{m}S[X_{\overline{\sigma}} : \overline{\sigma} \in G]$ é um polinômio não identicamente nulo. Assim, da independência algébrica dos elementos de G sobre $S/\mathfrak{m}S$ (cf. [Bo], Chap.5, §10), segue-se que existe um elemento s_0 de S tal que $N(\sum_{\sigma \in G} f(\sigma) X_\sigma)(s_0) = N(\sum_{\overline{\sigma} \in \overline{G}} f(\overline{\sigma}) X_{\overline{\sigma}})(s_0) \neq \overline{0}$ em $S/\mathfrak{m}S$, o que significa que $N(\sum_{\sigma \in G} f(\sigma) X_\sigma)(s_0) \in U(S)$. Como, $N(\sum_{\sigma \in G} f(\sigma) X_\sigma)(s_0)$ é exatamente igual à norma do elemento $a = \sum_{\sigma \in G} f(\sigma)\sigma(s_0) \in A$, em relação à S, então $N(\sum_{\sigma \in G} f(\sigma)\sigma(s_0)) \in U(S)$ ou, equivalentemente, $a \in U(A)$.

Da propriedade que define os cociclos temos :

$$\sigma(a) = \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(s_0) = \sum_{\tau \in G} f(\sigma\tau)(f(\sigma))^{-1}\sigma\tau(s_0) =$$

$= (\sum_{\sigma,\tau \in G} f(\sigma\tau)\sigma\tau(s_o))(f(\sigma))^{-1} = a(f(\sigma))^{-1}$; ou seja , $f(\sigma) =$ $= \sigma(a^{-1})a$, para todo $\sigma \in G$. ∎

Os resultados demonstrados neste parágrafo , com exceção do teorema 3.4 , são também encontrados em [KO] , Chap, II . O teorema 3.4 é uma generalização para anéis locais , do mesmo resultado , demonstrado por Springer , para corpos (cf. [Sp] , Teorema do Apêndice).

4. O conjunto $H^1(G, O(q^S))$

Sejam R um anel , M um R-módulo e S uma extensão galoisiana de R , com grupo G . Para todo $\sigma \in G$ e para toda aplicação φ de $S \otimes_R M$ em S (ou em $S \otimes_R M$) definimos a aplicação $\sigma\varphi$ tal que $(\sigma\varphi)(x) = \sigma(\varphi(\sigma^{-1}(x)))$, para todo $x \in S \otimes_R M$, onde $\sigma : S \otimes_R M \longrightarrow S \otimes_R M$ é dada por $\sigma(s \otimes m) = \sigma(s) \otimes m$, quaisquer que sejam $s \in S$ e $m \in M$. É de verificação imediata que :

i) se $q' : S \otimes_R M \longrightarrow S$ é uma forma quadrática então $\sigma q' = q'$, para todo $\sigma \in G$, se, e somente se , $q' = q^S$, para alguma forma quadrática $q : M \longrightarrow R$;

ii) se $\varphi' : S \otimes_R M \longrightarrow S \otimes_R M$ é uma aplicação S-linear então $\sigma\varphi' = \varphi'$, para todo $\sigma \in G$, se , e somente se , $\varphi' = id_S \otimes \varphi$

para alguma aplicação R-linear $\varphi : M \longrightarrow M$, (cf. [KO] ,Chap.II , §5 , Cor.5.2).

Se (M,q) e (M,q_1) são dois R-módulos quadráticos , dizemos que q e q_1 são S-<u>equivalentes</u> , para alguma extensão galoisiana S de R , se q^S e q_1^S são equivalentes ; ou seja , se os S-módulos quadráticos $(S\otimes_R M, q^S)$ e $(S\otimes_R M, q_1^S)$ são isomorfos. Obviamente , se q e q_1 são equivalentes (ou R-equivalentes) então q e q_1 são S-equivalentes , para toda extensão galoisiana S de R.

Nos resultados seguintes , R denotará sempre um anel local e (M,q) e (M,q_1) dois R-espaços quadráticos . O Teorema 1.1 nos garante que q e q_1 são sempre S-equivalentes , para alguma extensão galoisiana S de R . Logo , existe um isomorfismo de S-módulos $t: S\otimes_R M \longrightarrow S\otimes_R M$ tal que $q^S(t(x)) = q_1^S(x)$, para todo $x \in S\otimes_R M$.

Denotemos por G o grupo de Galois de S sobre R . Como $q^S(t(x)) = q_1^S(x) = \sigma q_1^S(x) = \sigma(q_1^S(\sigma^{-1}(x))) = \sigma(q^S(t(\sigma^{-1}(x)))) = (\sigma q^S)((\sigma t)(x)) = q^S((\sigma t)(x))$, existe $u_\sigma \in O(q^S)$ tal que $u_\sigma \cdot t = \sigma t$, para todo $\sigma \in G$. Além disso ,$(\sigma\tau)(t) = \sigma(\tau t) = \sigma(u_\tau \cdot t) = (\sigma u_\tau).(\sigma t) = (\sigma u_\tau).u_\sigma \cdot t$, de onde segue-se $u_{\sigma\tau} = (\sigma u_\tau)u_\sigma$, quaisquer que sejam $\sigma, \tau \in G$.

Por outro lado , se $t': S\otimes_R M \longrightarrow S\otimes_R M$ é também um isomorfismo de S-módulos tal que $q^S(t'(x)) = q_1^S(x)$, para todo $x \in S\otimes_R M$, então $q^S(t'(x)) = q^S(t(x))$, de onde resulta $t'=ut$, para algum $u \in O(q^S)$. Logo , $\sigma t' = u'_\sigma t'$, para algum $u'_\sigma \in O(q^S)$, $\sigma t' = \sigma(ut) = (\sigma u).(\sigma t) = (\sigma u)u_\sigma u^{-1} t'$ e disto temos $u'_\sigma = (\sigma u)u_\sigma u^{-1}$, para todo $\sigma \in G$.

É necessário observar que se $u \in O(q^S)$ então $\sigma u \in O(q^S)$, para todo $\sigma \in G$, isto é , G age , à esquerda sobre $O(q^S)$.

Do que vimos acima , podemos , então , concluir que toda forma quadrática q_1 sobre M , que é S-equivalente à q , dá origem a uma classe de 1-cohomologia $c_S(q,q_1)$ de $H^1(G, O(q^S))$, representada pelo cociclo $f_t : G \longrightarrow O(q^S)$ tal que $f_t(\sigma) = (\sigma t)t^{-1}$, para todo $\sigma \in G$ onde $t:(S \otimes_R M, q_1^S) \longrightarrow (S \otimes_R M, q^S)$ é um isomorfismo de S-espaços quadráticos . Observemos também que a representação da classe $c_S(q,q_1)$ não depende da escolha do isomorfismo t .

<u>Teorema 4.1</u> - As classes de equivalência de formas quadráticas q_1 , que são S-equivalentes à q , estão em correspondência bijetiva com os elementos de $H^1(G, O(q^S))$.

<u>Demonstração</u> :

Inicialmente , mostremos que $c_S(q,q_1) = c_S(q,q_2)$ em $H^1(G, O(q^S))$ se , e somente se q_1 e q_2 são equivalentes .

Admitamos que $c_S(q,q_1) = c_S(q,q_2)$ e sejam $h_i : G \longrightarrow O(q^S)$ dadas por $h_i(\sigma) = (\sigma t_i)t_i^{-1}$, onde $t_i:(S \otimes_R M, q_i^S) \longrightarrow (S \otimes_R M, q^S)$ são isomorfismos de S-módulos quadráticos , os representantes de $c_S(q,q_i)$, $(i=1,2)$. Como $c_S(q,q_1) = c_S(q,q_2)$, podemos considerar , sem perda de generali dade , que $h_1 = h_2 = h$ ou que $h(\sigma) = (\sigma t_1).t_1^{-1} = (\sigma t_2).t_2^{-1}$, para todo $\sigma \in G$. Resulta daí que $\sigma(t_2^{-1}.t_1) = (\sigma t_2^{-1}).(\sigma t_1) = (\sigma t_2)^{-1}.(\sigma t_1)$ $= t_2^{-1}.(h(\sigma))^{-1}.h(\sigma).t_1 = t_2^{-1}.t_1$, para todo $\sigma \in G$ e , consequentemente , existe um isomorfismo de R-módulos $t:M \longrightarrow M$ tal que $t_2^{-1}.t_1 = id_S \otimes t = t^S$, ou $t_1 = t_2 t^S$(cf. [KO] , Chap.II , §5 , Cor. 5.2) . Logo ,$q_2(t(x)) = q_2^S(t^S(x)) = q^S(t_2 t^S(x)) = q^S(t_1(x)) =$ $= q_1^S(x) = q_1(x)$, para todo $x \in M$, o que mostra que q_1 e q_2 são equivalentes. Reciprocamente , se q_1 e q_2 são equivalentes e ambas são S-equivalentes à q , então é de verificação imediata que $c_S(q,q_1) = c_S(q,q_2)$.

Finalmente se $c \in H^1(G, O(q^S))$, cujo representante é $h:G \longrightarrow O(q^S)$, existe $t \in \mathrm{Aut}_S(S\otimes_R M)$ tal que $h(\sigma) = (\sigma t).t^{-1}$, para todo $\sigma \in G$ (cf. Cor.3.3) . Seja $q':S\otimes_R M \longrightarrow S$ a forma quadrática dada por $q'(x) = q^S(t(x))$, para todo $x \in S\otimes_R M$. Como , $(\sigma q')(x) = \sigma(q'(\sigma^{-1}(x))) = \sigma(q^S(t(\sigma^{-1}(x)))) = (\sigma q^S)((\sigma t)(x)) =$

$$= q^S(h(\sigma)(t(x))) = q^S(t(x)) = q'(x) \quad \text{, para todo } x \in$$

$S\otimes_R M$, então $q' = q_1^S$ para alguma forma quadrática $q_1:M \longrightarrow R$. De $q_1^S(x) = q'(x) = q^S(t(x))$, para todo $x \in S\otimes_R M$, vemos que h é também um cociclo representante de $c_S(q,q_1)$, o que mostra que $c = c_S(q,q_1)$.

Para o teorema seguinte assumiremos que a extensão galoisiana S de R , mencionada no Teorema 4.1 , é também local.

<u>Teorema 4.2</u> - As classes de equivalência de formas

quadráticas q_1 sobre M, que são S-equivalentes à q e tem mesmo discriminante que q, estão em correspondência bijetiva com os elementos de $H^1(G, SO(q^S))$.

Demonstração :

Seja q_1 uma forma quadrática S-equivalente a q e consideremos a classe de 1-cohomologia $c_S(q,q_1) \in H^1(G, O(q^S))$, representada pelo cociclo $f:G \longrightarrow O(q^S)$ dado por $f(\sigma) = (\sigma t).t^{-1}$, onde $t:S\otimes_R M \longrightarrow S\otimes_R M$ é um automorfismo do S-módulo $S\otimes_R M$ tal que $q^S(t(x)) = q_1^S(x)$, para todo $x \in S\otimes_R M$.

Devemos mostrar que $f(\sigma) \in SO(q^S)$, para todo $\sigma \in G$, se, e somente se, $\Delta(q_1) = \Delta(q)$ em $G(R)$. Para tanto distinguiremos dois casos, segundo 2 seja ou não inversível em R.

i) $2 \in U(R)$:

Neste caso, $G(R) = U(R)/U^2(R)$ e admitamos que $\Delta(q_1) = \Delta(q) (\mathrm{mod}\ U^2(R))$. Logo, existe $\lambda \in U(R)$ tal que $\Delta(q_1) = \Delta(q)\lambda^2$. Além disso, $q_1^S(x) = q^S(t(x))$, para todo $x \in S\otimes_R M$, e, então, $\Delta(q_1^S) = \Delta(q^S)(d(t))^2$, onde $d(t)$ é o determinante da matriz de t em relação a uma base de M. Como, $\Delta(q^S) = \Delta(q)$ e $\Delta(q_1^S) = \Delta(q_1)$, obtemos :

$\Delta(q)\lambda^2 = \Delta(q_1) = \Delta(q_1^S) = \Delta(q^S)(d(t))^2 = \Delta(q)(d(t))^2$ e do fato de S ser local segue-se que $d(t) = \pm\lambda \in U(R)$. Assim, $\sigma(d(t)) = d(t)$ para todo $\sigma \in G$ e, como $d(\sigma t) = \sigma(d(t))$, obtemos $d(f(\sigma)) = d((\sigma t).t^{-1}) = d(\sigma t)(d(t))^{-1} = d(t)(d(t))^{-1} = 1$, o que mostra que $f(\sigma) \in SO(q^S)$, para todo $\sigma \in G$.

Reciprocamente , se $f(\sigma) \in SO(q^S)$, para todo $\sigma \in G$, então $d(f(\sigma)) = 1$ e $\sigma(d(t)) = d(\sigma t) = d(f(\sigma)t) = d(t)$, o que mostra que $d(t) \in U(R)$. Por outro lado , de $q_1^S(x) = q^S(t(x))$, para todo $x \in S \otimes_R M$, obtemos $\Delta(q_1) = \Delta(q_1^S) = \Delta(q^S)(d(t))^2 = \Delta(q)(d(t))^2$ ou $\Delta(q_1) = \Delta(q) (\mathrm{mod}\ U^2(R))$.

ii) <u>$2 \notin U(R)$</u> :

Admitamos que $\Delta(q_1) = \Delta(q)$ em $G(R)$. Logo , existe $\lambda \in R$ tal que $\Delta(q_1) = \Delta(q) + (\lambda - \lambda^2)(1-4\Delta(q))$. De $q_1^S(x) = q^S(t(x))$, para todo $x \in S \otimes_R M$, segue que $C(t): S \otimes_R C(M,q_1) \longrightarrow S \otimes_R C(M,q)$ é um isomorfismo de S-álgebras e consequentemente $C_o(t) = C(t)\Big|_{Z(S \otimes_R C_o(M,q_1))} : Z(S \otimes_R C_o(M,q_1)) \longrightarrow Z(S \otimes_R C_o(M,q))$ é também um isomorfismo de S-álgebras. Como $Z(C_o(M,q_1))$ e $Z(C_o(M,q))$ são, respectivamente ,as extensões quadráticas de R , $R[x]$, com $x^2 = x - \Delta(q_1)$ e $R[y]$, com $y^2 = y - \Delta(q)$ e , além disso , $Z(S \otimes_R C_o(M,q_1)) = S \otimes_R Z(C_o(M,q_1))$ e $Z(S \otimes_R C_o(M,q)) = S \otimes_R Z(C_o(M,q))$, então $C_o(t)$ fica perfeitamente caracterizado por $C_o(t)(1 \otimes x) = \alpha 1 \otimes 1 + \beta 1 \otimes y$, com $\alpha, \beta \in S$ e $\beta \in U(S)$. Como $C_o(t)$ é um isomorfismo de S-álgebras , a equação $x^2 - x + \Delta(q_1) = 0$ nos dá :

$$(\alpha 1 \otimes 1 + \beta 1 \otimes y)^2 - (\alpha 1 \otimes 1 + \beta 1 \otimes y) + \Delta(q_1)\, 1 \otimes 1 = 0$$

ou ainda ,

$$\alpha^2\, 1 \otimes 1 + 2\alpha\beta\, 1 \otimes y + \beta^2(1 \otimes y - \Delta(q)\, 1 \otimes 1) - (\alpha 1 \otimes 1 + \beta 1 \otimes y) + \left[\Delta(q) + (\lambda - \lambda^2)(1 - 4\Delta(q))\right] 1 \otimes 1 = 0$$

de onde se deduz que

$\beta(\beta + 2\alpha - 1) = 0$ e $(\alpha^2 - \alpha) - \Delta(q)(\beta^2 - 1) = (\lambda^2 - \lambda)(1 - 4\Delta(q))$. De $\beta \in U(S)$ segue-se que $\beta = 1 - 2\alpha$ e consequentemente obtemos $(\alpha - \lambda)(\alpha + \lambda - 1) = 0$. Do fato de S ser local segue-se que $\alpha = \lambda$ ou $\alpha = 1 - \lambda$. Em ambos os casos temos $\alpha, \beta \in R$ e portanto $C_o(t)(1 \otimes x) = 1 \otimes (\alpha + \beta y)$. Então $C_o(\sigma t) = \sigma C_o(t) = C_o(t)$ ou $C(f(\sigma))\Big|_{Z(S \otimes_R C_o(M,q))} = id$, o que significa que $f(\sigma) \in SO(q^S)$, para todo $\sigma \in G$.

Reciprocamente , admitamos que $C(f(\sigma))\Big|_{Z(S \otimes_R C_o(M,q))} =$ $= id$. Isto significa que $\sigma C_o(t) = C_o(\sigma t) = C_o(t)$, para todo $\sigma \in G$, onde

$$C_o(t) = C(t)\Big|_{Z(S \otimes_R C_o(M,q_1))} : Z(S \otimes_R C_o(M,q_1)) \longrightarrow Z(S \otimes_R C_o(M,q))$$

é um isomorfismo de S-álgebras . Logo, existe um isomorfismo de R-álgebras $t' : Z(C_o(M,q_1)) \longrightarrow Z(C_o(M,q))$ tal que $C_o(t) = id_S \otimes t'$, (cf. [KO] , Chap.II , Teor. 5.3) e disto segue-se que $\Delta(q_1) =$ $= \Delta(q)$ em $G(R)$. ■

5. Um invariante cohomológico .

Sejam G um grupo e G' um grupo abeliano sobre o qual G atua como grupo de operadores e consideremos os conjuntos :

$Z^2(G,G')=\{f:G \times G' \longrightarrow G' : (\sigma f(\tau,\rho))f(\sigma,\tau\rho) = f(\sigma,\tau)f(\sigma\tau,\rho)$, quaisquer que sejam $\sigma,\tau,\rho \in G\}$ e

$B^2(G,G')=\{f\in Z^2(G,G')$: existe $\theta:G\to G'$ e $f(\sigma,\tau)=\theta(\sigma\tau)((\sigma\theta(\tau)\theta(\sigma))^{-1}$ quaisquer que sejam $\sigma,\tau \in G\}$.

Observemos que $Z^2(G,G')$ é um grupo abeliano com a operação multiplicação pontual e que $B^2(G,G')$ é um subgrupo de $Z^2(G,G')$. Denotamos por $H^2(G,G') = Z^2(G,G') / B^2(G,G')$ o grupo quociente de $Z^2(G,G')$ por $B^2(G,G')$, o qual é chamado 2º grupo de cohomologia (ou grupo de 2-cohomologia) de G em G' . Um elemento de $Z^2(G,G')$ é chamado de 2-cociclo de G em G' e um elemento de $B^2(G,G')$ é chamado 2-cobordo de G em G' . Dois 2-cociclos que diferem por um 2-cobordo são ditos cohomólogos e representam a mesma classe de 2-comologia em $H^2(G,G')$.

Em todo este parágrafo denotaremos por R um anel local de ideal maximal $\mathfrak{m}$.

No §1 mostramos que dados dois R-espaços quadráticos (M,q_1) e (M,q) sempre existe uma extensão galoisiana S de R , com grupo G , tal que q e q_1 são S-equivalentes (cf. Teor. 1.1 e Teor. 1.4). No §4 vimos uma descrição das classes de equivalencia de formas quadráticas q_1 , que são S-equivalentes à q , como elementos $c_S(q,q_1)$ do conjunto $H^1(G, O(q^S))$ de 1-cohomolo -

gia (não comutativa) de G em $O(q^S)$. Neste parágrafo passaremos ao grupo de 2-cohomologia $H^2(G, U(S))$, associando $c_S(q,q_1)$ a um elemento $\alpha_S(qq_1) \in H^2(G, U(S))$ e mostraremos que se S é local, de corpo residual S/m_S infinito , $\alpha_S(q,q_1)=1$ e $\Delta(q) = \Delta(q_1)$ então $C(M,q_1) \cong C(M,q)$ e $C_o(M,q_1) \cong C_o(M,q)$. Como consequência deste resultado , mantidas as mesmas hipóteses sobre S, mostraremos que se o posto de M é 2 ou 3 então $(M,q_1) \cong (M,q)$ se, e somente se $\Delta(q_1) = \Delta(q)$ e $\alpha_S(q,q_1) = 1$.

No que segue , assumiremos sempre que (M,q_1) e (M,q) são R-espaços quadráticos e que S é uma extensão galoisiana local de R , com grupo G e tal que $S\otimes_R(M,q_1) \cong S\otimes_R(M,q)$.

O Teorema 2.1 nos garante que para todo $t \in O(q^S)$ existe um elemento $a_t \in CL(q^S)$ tal que $t(x)=(-1)^{\partial a_t} a_t x a_t^{-1}$, para todo $x \in S\otimes_R M$ e que a_t é unico , à menos de um fator em $U(S)$. Pode-se verificar sem muita dificuldade que $(-1)^{\partial a_t} = d(t)$ (cf. $[MV]_2$, Chap.2 §2 e $[B]_2$, Prop. 4.42) onde $d(t)$ denota o determinante de t em relação a alguma base de $S\otimes_R M$. Logo, quaisquer que sejam $u,t \in O(q^S)$ temos:

$(tu)(x) = t(d(u)a_u x a_u^{-1}) = d(tu)(a_t a_u)x(a_t a_u)^{-1}$ e

$(tu)(x) = d(tu)a_{tu} x a_{tu}^{-1}$

de onde segue-se que existe $\gamma(t,u) \in U(S)$ tal que $a_{tu} = \gamma(t,u)a_t a_u$. Assim , para cada par de elementos $u,t \in O(q^S)$ escolhemos elementos a_u, a_t e a_{tu} em $CL(q^S)$ que satisfazem o Teorema 2.1 e definimos uma aplicação $\gamma : O(q^S) \times O(q^S) \longrightarrow U(S)$ tal que $\gamma(t,u) = a_{tu} a_u^{-1} a_t^{-1}$.

De,

$$a_{t(uv)} = \gamma(t,uv) a_t a_{uv} = \gamma(u,v)\, \gamma(t,uv) a_t a_u a_v$$

e

$$a_{(tu)v} = \gamma(tu,v) a_{tu} a_v = \gamma(t,u)\, \gamma(tu,v) a_t a_u a_v$$

obtemos $\gamma(u,v)\,\gamma(t,uv) = \gamma(t,u)\,\gamma(tu,v)$, o que mostra que γ é um 2-cociclo de $O(q^S)$ em $U(S)$ (com $O(q^S)$ atuando trivialmente sobre $U(S)$) . Além disso , se a'_{tu}, a'_t e a'_u são uma outra escolha de elementos de $CL(q^S)$ que satisfazem o Teorema 2.1 para o mesmo par de elementos $t,u \in O(q^S)$,obtemos um novo 2-cociclo $\gamma' : O(q^S) \times O(q^S) \longrightarrow U(S)$ tal que $\gamma'(t,u) = a'_{tu} a'^{-1}_u a'^{-1}_t$. Do Teorema 2.1 temos $a'_{tu} = \lambda_{tu} a_{tu}$, $a'_t = \lambda_t a_t$ e $a'_u = \lambda_u a_u$, com $\lambda_{tu}, \lambda_t, \lambda_u \in U(S)$ e é imediato que

$$\gamma'(t,u) = \theta(tu)((t\theta(u))\theta(t))^{-1}\gamma(t,u) ,$$

onde $\theta : O(q^S) \longrightarrow U(S)$ é tal que $\theta(t) = \lambda_t$, para todo $t \in O(q^S)$. Observemos que θ está bem definida pois os λ_t estão bem determinados pela relação $a'_t = \lambda_t a_t$. Isto mostra que γ e γ' determinam uma mesma classe de 2-cohomologia , denotada por γ_S no grupo $H^2(O(q^S), U(S))$, com $O(q^S)$ atuando trivialmente sobre $U(S)$.

<u>Proposição 5.1</u> - Os elementos $a_t \in CL(q^S)$ que satisfazem o Teorema 2.1 para $t \in O(q^S)$ podem ser escolhidos de maneira a verificarem $a_{\sigma t} = \sigma(a_t)$, para todo $\sigma \in G$.

Demonstração:

Se $t(x) = d(t)a_t x a_t^{-1}$ então $(\sigma t)(x) = \sigma(t(\sigma^{-1}(x)) = \sigma(d(t)a_t \sigma^{-1}(x)a_t^{-1}) = d(t)(\sigma(a_t))x(\sigma(a_t))^{-1}$, de onde segue-se que existe $\lambda_{\sigma,t} \in U(S)$ tal que $(a_t) = \lambda_{\sigma,t}a_{\sigma t}$, para todo $\sigma \in G$. Disto temos $\lambda_{\sigma\tau,t}a_{\sigma\tau t} = \sigma(\tau(a_t)) = \sigma(\lambda_{\tau,t}a_{\tau t}) = \sigma(\lambda_{\tau,t})\sigma(a_{\tau t}) = \sigma(\lambda_{\tau,t})\lambda_{\sigma,\tau t}a_{\sigma\tau t}$ ou $\lambda_{\sigma\tau,t} = \sigma(\lambda_{\tau,t})\lambda_{\sigma,\tau t}$, quaisquer que sejam $\sigma,\tau \in G$.

Como S e uma extensão galoisiana local de R, com grupo G, então $S/\mathfrak{m}_S = R/\mathfrak{m} \otimes_R S$ é um corpo extensão de Galois do corpo $R/\mathfrak{m}$, com grupo $\overline{G} = \{\overline{\sigma} = id_{R/\mathfrak{m}} \otimes \sigma : \sigma \in G\} \approx G$ (cf. [CHR] §1, Lema 7). Logo da independência linear dos $\overline{\sigma}$ sobre $S/\mathfrak{m}_S$ (cf. [Bo], Chap.5, §7, nº5, Teor.5) segue-se que existe $\lambda \in S$ tal que $\sum_{\tau \in G} \overline{\lambda}_{\tau,\tau^{-1}t}\,\overline{\tau}(\overline{\lambda}) \neq \overline{0}$ em $S/\mathfrak{m}_S$, o que significa que $\lambda_t = \sum_{\tau \in G} \lambda_{\tau,\tau^{-1}t}\,\tau(\lambda) \in U(S)$. Assim,

$$\sigma(\lambda_t) = \sum_{\tau \in G} \sigma(\lambda_{\tau,\tau^{-1}t})\sigma\tau(\lambda) = \sum_{\tau \in G} \lambda_{\sigma,t}^{-1}\,\lambda_{\sigma\tau,\tau^{-1}t}\,\sigma\tau(\lambda) =$$
$$= \lambda_{\sigma,t}^{-1}\Big(\sum_{\sigma\tau \in G} \lambda_{\sigma\tau,(\sigma\tau)^{-1}(\sigma t)}\,\sigma\tau(\lambda)\Big) = \lambda_{\sigma,t}^{-1}\,\lambda_{\sigma t},$$

de onde temos

$$\lambda_{\sigma t} = \lambda_{\sigma,t}\,\sigma(\lambda_t) \in U(S)$$

e

$$\sigma(\lambda_t a_t) = \sigma(\lambda_t)\sigma(a_t) = \lambda_{\sigma t}\lambda_{\sigma,t}^{-1}\,\lambda_{\sigma,t}a_{\sigma t} = \lambda_{\sigma t}a_{\sigma t},$$

para todo $\sigma \in G$. Logo substituindo os $\lambda_{\sigma t}a_{\sigma t}$ por $a_{\sigma t}$, para todo $\sigma \in G$ e $t \in O(q^S)$, podemos afirmar que $\sigma(a_t) = a_{\sigma t}$. ∎

Da Proposição 5.1 decorre facilmente que o 2-cociclo $\gamma : O(q^S) \times O(q^S) \longrightarrow U(S)$, definido anteriormente , satisfaz $\gamma(\sigma t, \sigma u) = \sigma(\gamma(t,u))$, para todo $\sigma \in G$ e quaisquer que sejam $t,u \in O(q^S)$.

Consideremos agora a classe $c_S(q,q_1) \in H^1(G,\ O(q^S))$ e seja $f: G \longrightarrow O(q^S)$, tal que $f(\sigma) = u_\sigma$, para todo $\sigma \in G$, um cociclo representante de $c_S(q,q_1)$. Existem elementos $a_{u_\sigma} \in CL(q^S)$ tais que $u_\sigma(x) = d(u_\sigma) a_{u_\sigma} x a_{u_\sigma}^{-1}$ e $a_{\sigma u_\tau} = \sigma(a_{u_\tau})$; para todo $x \in S \otimes_R M$ e quaisquer que sejam $\sigma, \tau \in G$. Assim podemos definir a aplicação $\alpha : G \times G \longrightarrow U(S)$ tal que $\alpha(\sigma,\tau) = \gamma(\sigma u_\tau, u_\sigma)$, quaisquer que sejam $\sigma, \tau \in G$. Como $\gamma(\sigma u_\tau, u_\sigma) = a_{(\sigma u_\tau) u_\sigma} a_{u_\sigma}^{-1} a_{\sigma u_\tau}^{-1}$ e $(\sigma u_\tau) . u_\sigma = u_{\sigma\tau}$, então podemos também escrever $\alpha(\sigma,\tau) = a_{u_{\sigma\tau}} a_{u_\sigma}^{-1} \sigma(a_{u_\tau}^{-1})$, quaisquer que sejam $\sigma, \tau \in G$. Agora , temos:

$$\sigma(\alpha(\tau,\rho)) = \sigma(\gamma(\tau u_\rho , u_\tau)) = \gamma(\sigma\tau u_\rho, \sigma u_\tau) ,$$

$$\alpha(\sigma, \tau\rho) = \gamma(\sigma u_{\tau\rho}, u_\sigma) ,$$

$$\alpha(\sigma,\tau) = \gamma(\sigma u_\tau,\ u_\sigma) ,$$

e $$\alpha(\sigma\tau, \rho) = \gamma(\sigma\tau u_\rho, u_{\sigma\tau}) ,$$ quaisquer que sejam $\sigma, \tau, \rho \in G$.

Fazendo $u_1 = \sigma\tau u_\rho$, $u_2 = \sigma u_\tau$ e $u_3 = u_\sigma$ e usando o fato de γ ser um 2-cociclo de $O(q^S)$ em $U(S)$ (com $O(q^S)$ atuando trivialmente sobre $U(S)$, obtemos

$$\gamma(u_1,u_2)\gamma(u_1 u_2, u_3) = \gamma(u_2,u_3)\gamma(u_1, u_2 u_3)$$

ou

$$\sigma(\alpha(\tau,\rho))\alpha(\sigma,\tau\rho) = \alpha(\sigma,\tau)\alpha(\sigma\tau,\rho) .$$

Isto mostra que α é um 2-cociclo de G em U(S) (com G atuando de modo usual sobre U(S)) . Se , agora , considerarmos um outro cociclo $f':G \longrightarrow O(q^S)$, tal que $f'(\sigma) = u'_\sigma$, para todo $\sigma \in G$, como representante da mesma classe $c_S(q,q_1)$, obteremos um novo 2-cociclo $\alpha':G \times G \longrightarrow U(S)$ tal que $\alpha'(\sigma,\tau) = \gamma(\sigma u'_\tau, u'_\sigma) = a_{u'_{\sigma\tau}} a^{-1}_{u'_\sigma} \sigma(a^{-1}_{u'_\tau})$. Mas os cociclos f e f' são cohomólogos e portanto existe $u \in O(q^S)$ tal que $u'_\sigma = (\sigma u)u_\sigma u^{-1}$ e , neste caso , temos :

$$\begin{aligned} a_{u'_\sigma} &= a_{(\sigma u)u_\sigma u^{-1}} = \gamma(\sigma u, u_\sigma u^{-1})a_{\sigma u}a_{u_\sigma u^{-1}} = \\ &= \gamma(\sigma u, u_\sigma u^{-1})a_{\sigma u}\gamma(u_\sigma, u^{-1})a_{u_\sigma}a_{u^{-1}} = \\ &= \theta(\sigma)\gamma(u^{-1},u)a_{\sigma u}a_{u_\sigma}a_{u^{-1}} \end{aligned}$$

, onde $\theta:G \longrightarrow U(S)$ é uma aplicação tal que

$$\theta(\sigma) = \gamma(\sigma u, u_\sigma u^{-1})\gamma(u_\sigma, u^{-1})(\gamma(u^{-1},u))^{-1} \quad , \text{ para todo } \sigma \in G.$$

Pode verificar-se facilmente que

$$\alpha'(\sigma,\tau) = \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1}\alpha(\sigma,\tau)$$

, quaisquer que sejam $\sigma, \tau \in G$, o que mostra que α e α' representam a mesma classe de 2-cohomologia $\alpha_S(q,q_1) \in H^2(G, U(S))$. Temos, assim , uma aplicação $c_S(q,q_1) \in H^1(G, O(q^S)) \longmapsto \alpha_S(q,q_1) \in H^2(G, U(S))$.

<u>Proposição 5.2</u> - $\alpha_S(q,q_1)^2 = 1$.

<u>Demonstração</u> :

Consideremos o anti-automorfismo de $C(S\otimes_R M, q^S)$ definido por $x = x_1 \dots x_r \longmapsto \bar{x} = x_r \dots x_1$. Seja $\alpha : G \times G \longrightarrow U(S)$ tal que $\alpha(\sigma,\tau) = a_{u_{\sigma\tau}} a_{u_\sigma}^{-1} \sigma(a_{u_\tau}^{-1})$, quaisquer que sejam $\sigma,\tau \in G$, o cociclo representante de $\alpha_S(q,q_1)$. Os elementos a_{u_σ} satisfazem $u_\sigma(x) = d(u_\sigma) a_{u_\sigma} x a_{u_\sigma}^{-1}$, para todo $x \in S \otimes_R M$. Então , $a_{u_\sigma} x = d(u_\sigma) u_\sigma(x) a_{u_\sigma}$ e consequentemente $x\bar{a}_{u_\sigma} = d(u_\sigma)\bar{a}_{u_\sigma} u_\sigma(x)$, de onde obtemos $x\bar{a}_{u_\sigma} a_{u_\sigma} = d(u_\sigma)\bar{a}_{u_\sigma} u_\sigma(x) a_{u_\sigma} = \bar{a}_{u_\sigma} a_{u_\sigma} x$, para todo $x \in S \otimes_R M$. Como $S \otimes_R M$ gera $C(S \otimes_R M, q^S)$ então $\bar{a}_{u_\sigma} a_{u_\sigma} x = x\bar{a}_{u_\sigma} a_{u_\sigma}$, para todo $x \in C(S \otimes_R M, q^S)$, o que significa que $\bar{a}_{u_\sigma} a_{u_\sigma} \in U(S)$. Disto decorre facilmente que $\alpha(\sigma,\tau)^2 = \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1}$, quaisquer que sejam $\sigma,\tau \in G$, onde $\theta : G \longrightarrow U(S)$ é tal que $\theta(\sigma) = \bar{a}_{u_\sigma} a_{u_\sigma}$, para todo $\sigma \in G$. Portanto $\alpha_S(q,q_1)^2 = 1$. ∎

<u>Proposição 5.3</u> - Se q e q_1 são equivalentes então $\alpha_S(q,q_1) = 1$.

A demonstração desta proposição é imediata .

<u>Teorema 5.4</u> - Seja $S/\mathfrak{m}_S$ infinito. Se $\Delta(q_1) = \Delta(q)$ e $\alpha_S(q,q_1) = 1$ então $C(M,q_1) \simeq C(M,q)$ e $C_0(M,q_1) \simeq C_0(M,q)$, como R-álgebras.

<u>Demonstração</u> :

Como S é local , de $\Delta(q_1) = \Delta(q)$ temos $c_S(q,q_1) \in H^1(G, SO(q^S))$ (cf. o Teorema 4.2) . Seja $f : G \longrightarrow SO(q^S)$ tal que $f(\sigma) = u_\sigma$, para todo $\sigma \in G$, o cociclo representante de

$c_S(q,q_1)$. Recordemos que $u_\sigma = (\sigma t).t^{-1}$ onde $t:S\otimes_R M \longrightarrow S\otimes_R M$ é um isomorfismo de S-módulos tal que $q^S(t(x)) = q_1^S(x)$; para todo $x \in S\otimes_R M$. Seja $\alpha : G \times G \longrightarrow U(S)$ tal que $\alpha(\sigma,\tau) =$ $= a_{u_{\sigma\tau}} a_{u_\sigma}^{-1} \sigma(a_{u_\tau}^{-1})$, quaisquer que sejam $\sigma, \tau \in G$, o 2-cociclo representante de $\alpha_S(q,q_1) \in H^2(G, U(S))$. Como $\alpha_S(q,q_1) = 1$, podemos considerar , sem perda de generalidade , $\alpha(\sigma,\tau) = 1$ e então $a_{u_{\sigma\tau}} = \sigma(a_{u_\tau})a_{u_\sigma}$, quaisquer que sejam $\sigma,\tau \in G$. Por outro lado $S/\mathfrak{m}_S$ é infinito e do Teorema 3.4 segue-se que existe $a \in U(S\otimes_R C(M,q))$ tal que $a_{u_\sigma} = (\sigma(a))^{-1}a$, para todo $\sigma \in G$. Assim , $(\sigma t)(x) = u_\sigma(t(x)) = a_{u_\sigma} t(x) a_{u_\sigma}^{-1} = \sigma(a)(a^{-1}t(x)a)(\sigma(a))^{-1}$, para todo $x \in S\otimes_R M$, para todo $\sigma \in G$. Definimos $\psi : S\otimes_R M \longrightarrow S\otimes_R C(M,q)$ tal que $\psi(x) = a^{-1}t(x)a$, para todo $x \in S\otimes_R M$. A aplicação ψ é claramente S-linear e injetora. Como $(\psi(x))^2 = a^{-1}(t(x))^2a = q^S(t(x)) = q_1^S(x)$, para todo $x \in S\otimes_R M$, da propriedade universal das álgebras de Clifford segue-se que existe um homomorfismo de S-álgebras $\psi' : S\otimes_R C(M,q_1) \longrightarrow S\otimes_R C(M,q)$ tal que o diagrama

$$\begin{tikzcd} S\otimes_R M \arrow[rr] \arrow[dr, "\psi"'] & & S\otimes_R C(M,q_1) \arrow[dl, "\psi'"] \\ & S\otimes_R C(M,q) & \end{tikzcd}$$

é comutativo. Como $S\otimes_R M$ gera $S\otimes_R C(M,q)$ e ψ é injetiva então $\psi'(S\otimes_R M) = \psi(S\otimes_R M)$ gera $S\otimes_R C(M,q)$ e isto mostra que ψ' é sobrejetora. Mas , $S\otimes_R C(M,q)$ e $S\otimes_R C(M,q_1)$ são S-módulos livres de mesmo posto e então ψ' é um isomorfismo . Agora , observemos que $(\sigma\psi)(x) = \sigma(\psi(\sigma^{-1}(x))) = \sigma(a^{-1}t(\sigma^{-1}(x))a) =$ $= (\sigma(a))^{-1}(\sigma t)(x)\sigma(a) = a^{-1}t(x)a = \psi(x)$, para todo $x \in S\otimes_R M$ e para todo $\sigma \in G$ e , como $S\otimes_R M$ gera $S\otimes_R C(M,q_1)$, então $(\sigma\psi')(x) = \psi'(x)$, para todo $x \in S\otimes_R C(M,q_1)$ e para todo $\sigma \in G$. Consequentemente existe um isomorfismo de R-álgebras $\varphi: C(M,q_1) \longrightarrow C(M,q)$ tal que $\psi' = id_S \otimes \varphi$ (cf. [KO] , Chap.II, §5 , Teor.5.3). A verificação de que $C_0(M,q_1) \simeq C_0(M,q)$ é imediata. ∎

<u>Teorema 5.5</u> - Se o posto de M é 2 ou 3 , $C(M,q_1) \simeq C(M,q)$ e $\Delta(q_1) = \Delta(q)$ então $(M,q_1) \simeq (M,q)$.

<u>Demonstração</u> : Ver [R] , Chap.II , Teor.1.4 ∎

<u>Teorema 5.6</u> - Seja S com a mesma hipótese do Teorema 5.4 . Se o posto de M é 2 ou 3 então $(M,q_1) \simeq (M,q)$ se, e somente se , $\Delta(q_1) = \Delta(q)$ e $\alpha_S(q,q_1) = 1$.

A demonstração deste teorema decorre da Proposição 5.3 e dos Teoremas 5.4 e 5.5 .

6. O invariante de Hasse

Em todo este parágrafo R denotará um anel local henseliano , de ideal maximal $\mathfrak{m}$, com $2 \notin \mathfrak{m}$ e corpo residual $R/\mathfrak{m}$ infinito.

Consideremos $a,b \in U(R)$ e seja $A = R[\sqrt{a}]$ se $a \notin U^2(R)$ e $A = R$, caso contrário . Observemos que , em ambos os casos , A é uma extensão galoisiana local de R (cf. Prop. 1.2 e Cor. 1.3) e denotemos por H o seu grupo de Galois . Definimos a aplicação $f: H \times H \longrightarrow U(A)$ tal que :

$$f(\sigma,\tau) = b \text{ , se } \sigma \neq id_A \text{ e } \tau \neq id_A$$

e

$$f(\sigma,\tau) = 1 \text{ , caso contrário, quaisquer que sejam } \sigma,\tau \in$$

H ; f é,obviamente , um 2-cociclo de H em U(A) e denotemos por $(a,b) \in H^2(H, U(A))$ a classe de 2-cohomologia representada por f.

Se , agora , S e uma extensão galoisiana local de R , com grupo G , tal que $A \subset S$ como subálgebra , então existe um subgrupo normal G' de G tal que S é uma extensão galoisiana de A , com grupo G' e $G/_{G'} \approx H$ (cf. [CHR] , Teor.2.3 e Teor. 3.1) . Logo , de $H^1(G', U(S)) = 0$ (cf. Cor.3.3 para n=1) segue-se que

$$0 \longrightarrow H^2(H, U(A)) \longrightarrow H^2(G, U(S))$$

é uma sequência exata de grupos (cf. $[S]_1$, Chap.VII ,§6 ,Prop.5) Desta forma vemos que (a,b) é também uma classe de 2-cohomologia de G em U(S) e o cociclo f , que a representa , é agora descrito por

$$f(\sigma,\tau) = b \text{ , se } \sigma\big|_A \neq id_A \text{ e } \tau\big|_A \neq id_A$$

e $\quad f(\sigma,\tau) = 1$, caso contrário , quaisquer que sejam $\sigma,\tau \in G$.

<u>Proposição 6.1</u> Sejam a,b e c elementos de U(R). Então :

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

ii) $(a,b) = (b,a)$

iii) $(ab,c) = (a,c)(b,c)$

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

v) $(a,b) = 1$ se , e somente se , existem elementos x,y, z em R tais que $x^2-ay^2-bz^2 = 0$ e pelo menos um dentre x,y,z é inversível em R .

<u>Demonstração</u> :

Indiquemos $A = R[\sqrt{a}]$, $B = R[\sqrt{b}]$ e $C = R[\sqrt{c}]$ se a,b,c $\notin U^2(R)$ e $A = B = C = R$, caso contrário. Em toda a demonstração S denotará uma extensão galoisiana local de R , com grupo G e contendo A , B e C como subálgebras.

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

A demonstração desta igualdade é imediata.

ii) $(a,b) = (b,a)$

Se a ou b $\in U^2(R)$, o resultado é óbvio . Se a $\notin U^2(R)$ e b $\notin U^2(R)$ e se f e f' são os cociclos representantes de (a,b) e (b,a) , respectivamente , então :

$f'(\sigma,\tau) = \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1}f(\sigma,\tau)$, quaisquer que sejam σ,τ

$\in G$, onde $\theta: G \longrightarrow U(S)$ é dada por $\theta(\sigma) = \frac{\sqrt{b}}{\sqrt{a}}$, se $\sigma|_A \neq id_A$ e $\sigma|_B \neq id_B$; $\theta(\sigma) = \frac{1}{\sqrt{a}}$, se $\sigma|_A = id_A$ e $\sigma|_B \neq id_B$; $\theta(\sigma) = -\sqrt{b}$ se $\sigma|_A \neq id_A$ e $\sigma|_B = id_B$ e $\theta(\sigma) = 1$, se $\sigma|_A = id_A$ e $\sigma|_B = id_B$ para todo $\sigma \in G$. Disto segue-se a igualdade das classes (a,b) e (b,a) .

iii) $(ab,c) = (a,c)(b,c)$

Neste caso , se f , f' e f'' são , respectivamente os cociclos representantes de (a,c) , (b,c) e (ab,c) então $f''(\sigma,\tau) = \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1}f(\sigma,\tau)f'(\sigma,\tau)$, quaisquer que sejam $\sigma,\tau \in G$, onde $\theta: G \longrightarrow U(S)$ é dada por $\theta(\sigma) = c$, se $\sigma|_A \neq id_A$ e $\sigma|_B \neq id_B$ e $\theta(\sigma) = 1$, caso contrário , para todo $\sigma \in G$. Disto segue-se a igualdade proposta.

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

Se $a \in U^2(R)$, o resultado é óbvio. Se $a \notin U^2(R)$ e se f e f' são , respectivamente , os representantes de (a,a) e (a,-1) , então $f'(\sigma,\tau) = \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1}f(\sigma,\tau)$, quaisquer que sejam $\sigma,\tau \in G$, onde $\theta: G \longrightarrow U(S)$ é dada por $\theta(\sigma) = \sqrt{a}$, se $\sigma|_A \neq id_A$ e $\theta(\sigma) = 1$, caso contrário , para todo $\sigma \in G$. Disto segue-se a igualdade desejada.

v) Se $a \in U^2(R)$, o resultado é óbvio . Seja , então $a \notin U^2(R)$. Admitamos , inicialmente , que $(a,b) = 1$ em $H^2(G, U(S))$. Como a sêquencia $0 \longrightarrow H^2(H, U(A)) \longrightarrow H^2(G, U(S))$, onde H é o grupo de Galois de A sobre R, é exata , então $(a,b)=1$ em $H^2(H, U(A))$. Logo , existe uma aplicação $\theta: H \longrightarrow U(A)$ tal que $\theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1} = b$, se $\sigma \neq id_A$ e $\tau \neq id_A$ e $\theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1} = 1$, caso contrário , quaisquer que sejam $\sigma, \tau \in G$. Se $\sigma : \sqrt{a} \longmapsto -\sqrt{a}$ é o gerador de H , então $\theta(\sigma) = (x+y\sqrt{a})^{-1}$, para algum x e algum y em R tais que $(x+y\sqrt{a}) \in U(R)$ e $b = \theta(\sigma^2)(\sigma(\theta(\sigma))\theta(\sigma))^{-1} = (x+y\sqrt{a})(x-y\sqrt{a}) = x^2-ay^2$. Portanto existem elementos x,y e z = 1 em R tais que $x^2-y^2a - bz^2 = 0$ e $z = 1 \in U(R)$.

Reciprocamente , sejam x,y e z elementos de R tais que $x^2-ay^2-bz^2 = 0$ e x ou y ou z $\in U(R)$. Observemos que pelo menos dois dos elementos x,y e z estão em U(R) , pois , caso contrário o terceiro elemento também não estaria em U(R) , o que seria uma contradição . Devido (a,b) = (b,a) podemos supor , sem perda de generalidade , que $z \in U(R)$. Assim , temos
$b = (\frac{x}{z} + \frac{y}{z}\sqrt{a})(\frac{x}{z} - \frac{y}{z}\sqrt{a})$, com $(\frac{x}{z} + \frac{y}{z}\sqrt{a}), (\frac{x}{z} - \frac{y}{z}\sqrt{a}) \in U(S)$ pois $b \in U(R)$. Definindo $\theta : G \longrightarrow U(S)$ tal que $\theta(\sigma) = (\frac{x}{z} + \frac{y}{z}\sqrt{a})^{-1}$, se $\sigma|_A \neq id_A$ e $\theta(\sigma) = 1$, caso contrário , para todo $\sigma \in G$, obtemos

$$\theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1} = b \quad , \text{ se } \sigma, \tau|_A \neq id_A$$

e $\qquad \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1} = 1$, caso contrário , quaisquer que sejam $\sigma, \tau \in G$. Disto segue-se que (a,b) = 1 . ∎

Outras propriedades de (a,b) tais como $(ac^2,b) = (a,b)$ $(a,b)^2 = 1$, $(a,b) = (a^{-1},b)$, $(a,-a) = 1$ e $(a,1-a) = 1$ são facilmente verificadas a partir daquelas demonstradas na Prop.6.1.

Consideremos novamente $a,b \in U(R)$ e sejam $A = R[\sqrt{a}]$ e $B = R[\sqrt{b}]$ se $a,b \notin U^2(R)$ e $A = B = R$, caso contrário. Notemos que se $a \in U^2(R)$ (resp. $b \in U^2(R)$), existe $a' \in U(R)$ (resp. $b' \in U(R)$) tal que $a = a'^2$ (resp. $b = b'^2$). Por uma questão de uniformidade de notação também indicaremos a' (resp. b') por $\sqrt{a}$ (resp. $\sqrt{b}$). Seja S uma extensão galoisiana local de R, com grupo G, contendo A e B como subálgebras. Como A e B são também extensões galoisianas locais de R, pode ver-se facilmente que $\sigma(\sqrt{a}) = (-1)^{a_\sigma}\sqrt{a}$ e $\sigma(\sqrt{b}) = (-1)^{b_\sigma}\sqrt{b}$, para todo $\sigma \in G$, onde a_σ e b_σ são números inteiros iguais a 0 ou 1. Definimos a aplicação $g: G \times G \longrightarrow U(S)$ tal que $g(\sigma,\tau) = (-1)^{a_\sigma b_\tau}$, quaisquer que sejam $\sigma,\tau \in G$; g é um 2-cociclo de G em $U(S)$ e denotamos por $[a,b] \in H^2(G, U(S))$ a classe de 2-cohomologia representada por g.

<u>Proposição 6.2</u>: $[a,b] = (a,b)$ em $H^2(G, U(S))$.

<u>Demonstração</u>:

Sejam f e $g: G \times G \longrightarrow U(S)$ os cociclos representantes de (a,b) e $[a,b]$, respectivamente. Então $f(\sigma,\tau) = b$, se $\sigma,\tau|_A \neq id_A$ e $f(\sigma,\tau) = 1$, caso contrário e $g(\sigma,\tau) = (-1)^{a_\sigma b_\tau}$ quaisquer que sejam $\sigma,\tau \in G$. Observando que

$f(\sigma,\tau) = b^{\frac{1}{2}(a_\sigma + a_\tau - a_{\sigma\tau})}$ e que $\sigma(b^{\frac{1}{2}a_\tau}) = (-1)^{a_\tau b_\sigma} b^{\frac{1}{2}a_\tau}$,

podemos verificar facilmente que

$g(\sigma,\tau) = \theta(\sigma\tau)(\sigma(\theta(\tau))\theta(\sigma))^{-1}f(\sigma,\tau)$, quaisquer que sejam $\sigma,\tau \in G$ onde $\theta: G \longrightarrow U(S)$ é tal que

$\theta(\sigma) = (-1)^{a_\sigma b_\sigma} b^{\frac{1}{2} a_\sigma}$, para todo $\sigma \in G$. Portanto $[a,b] = (a,b)$.

Sejam (M,q) um R-espaço quadrático e $\{x_1,\ldots,x_n\}$ uma base de M , tal que

$$q\left(\sum_{i=1}^{n} \xi_i x_i\right) = \sum_{i=1}^{n} a_i \xi_i^2 \quad , \text{ com } a_i \in U(R) \ , \ 1 \leq i \leq n \ ,$$

(cf. $[MV]_1$, §2 , Lema 1) . O <u>invariante de Hasse</u> h(q) da forma quadrática q é definido como sendo $h(q) = \prod_{i<j} (a_i,a_j) \in H^2(G, U(S))$, onde S é uma extensão galoisiana local de R, com grupo G e contendo elementos α_i tais que $\alpha_i^2 = a_i$, $1 \leq i \leq n$.

Consideremos , agora , os R-espaços quadráticos (M,q) e (M,q_1) e seja $\{x_1,\ldots,x_n\}$ uma base de M tal que

$$q\left(\sum_{i=1}^{n} \xi_i x_i\right) = \sum_{i=1}^{n} a_i \xi_i^2 \quad , \text{ com } a_i \in U(R), \ 1 \leq i \leq n \ .$$

Substituindo q_1 por uma forma quadrática equivalente , podemos supor , sem perda de generalidade , que

$$q_1\left(\sum_{i=1}^{n} \xi_i x_i\right) = \sum_{i=1}^{n} b_i \xi_i^2 \quad , \text{ com } b_i \in U(R) \ , \ 1 \leq i \leq n \ .$$

Como R é local e henseliano sempre existe uma extensão galoisiana local S de R , com grupo G , contendo elementos α_i e β_i tais que $\alpha_i^2 = a_i$ e $\beta_i^2 = b_i$, $1 \leq i \leq n$ e que, consequentemente verifica $S \otimes_R (M,q_1) \simeq S \otimes_R (M,q)$ (cf. Teor. 1.4) . O isomorfismo de S-espaços quadráticos
$t: S \otimes_R (M,q_1) \longrightarrow S \otimes_R (M,q)$ é , neste caso, definido por
$t(1 \otimes x_i) = \gamma_i (1 \otimes x_i)$, onde $\gamma_i^2 = a_i^{-1} b_i$, $1 \leq i \leq n$. Como
$q^S(t(x)) = q_1^S(x)$, para todo $x \in S \otimes_R M$, vimos no §4 que existe

$u_\sigma \in O(q^S)$ tais que $u_\sigma t = \sigma t$, para todo $\sigma \in G$. (cf. Teor.4.1). Então,

$(\sigma t)(1 \otimes x_i) = u_\sigma(t(1 \otimes x_i)) = u_\sigma(\gamma_i\, 1 \otimes x_i) = \gamma_i u_\sigma(1 \otimes x_i)$ e

$(\sigma t)(1 \otimes x_i) = \sigma(t(\sigma^{-1}(1 \otimes x_i))) = \sigma(t(1 \otimes x_i)) = \sigma(\gamma_i\, 1 \otimes x_i) =$

$= \sigma(\gamma_i) 1 \otimes x_i = (-1)^{\varepsilon_{i,\sigma}} \gamma_i 1 \otimes x_i$, de onde obtemos $u_\sigma(1 \otimes x_i) =$
$= (-1)^{\varepsilon_{i,\sigma}} 1 \otimes x_i$, para todo $\sigma \in G$, $1 \leq i \leq n$. Denotemos $y_i = 1 \otimes x_i$ e sejam $s_i \in O(q^S)$ dadas por

$$s_i(x) = x - \frac{\phi^S(x, y_i)}{q^S(y_i)}\, y_i \quad , \text{ para todo } x \in S \otimes_R M \,,\ 1 \leq i \leq n \,,$$

onde ϕ^S é a forma bilinear associada à q^S. Como em $C(S \otimes_R M, q^S)$ $\phi^S(x, y_i) = xy_i + y_i x$ e y_i é inversível, então $s_i(x) = -y_i x y_i^{-1}$ para todo $x \in S \otimes_R M$, $1 \leq i \leq n$. Definimos

$s_i^{\varepsilon_{i,\sigma}}(x) = (-1)^{\varepsilon_{i,\sigma}} y_i^{\varepsilon_{i,\sigma}} x y_i^{-\varepsilon_{i,\sigma}}$, para todo $x \in S \otimes_R M$, para todo $\sigma \in G$, $1 \leq i \leq n$. Notemos que $s_i^{\varepsilon_{i,\sigma}} = s_i$, se $\varepsilon_{i,\sigma} = 1$ e $s_i^{\varepsilon_{i,\sigma}} = id$, se $\varepsilon_{i,\sigma} = 0$ e que $s_i(y_j) = y_j$, para todo $j \neq i$. Decorre disto que $u_\sigma = \prod_{i=1}^{n} s_i^{\varepsilon_{i,\sigma}}$ e consequentemente obtemos:

$$u_\sigma(x) = (-1)^{\sum_{i=1}^{n} \varepsilon_{i,\sigma}} \cdot \Big(\prod_{i=1}^{n} y_i^{\varepsilon_{i,\sigma}}\Big) x \Big(\prod_{i=1}^{n} y_i^{\varepsilon_{i,\sigma}}\Big)^{-1} =$$

$$= d(u_\sigma) \Big(\prod_{i=1}^{n} y_i^{\varepsilon_{i,\sigma}}\Big) x \Big(\prod_{i=1}^{n} y_i^{\varepsilon_{i,\sigma}}\Big)^{-1} \,,$$

para todo $x \in S \otimes_R M$, para todo $\sigma \in G$. Seja $a_{u_\sigma} = \prod_{i=1}^{n} y_i^{\varepsilon_{i,\sigma}}$ para todo $\sigma \in G$. O 2-cociclo $\alpha : G \times G \longrightarrow U(S)$ dado por $\alpha(\sigma, \tau)$

$= \sigma(a_{u_\tau})a_{u_\sigma}a_{u_{\sigma\tau}}^{-1}$, quaisquer que sejam $\sigma, \tau \in G$, é também um representante da classe $\alpha_S(q,q_1) \in H^2(G, U(S))$, construida no §5 (cf. Prop.5.2). Substituindo os a_{u_σ} na igualdade $\alpha(\sigma,\tau) = \sigma(a_{u_\tau})a_{u_\sigma}a_{u_{\sigma\tau}}^{-1}$ e observando que $y_j^{\varepsilon_{j,\tau}} \cdot y_i^{\varepsilon_{i,\sigma}} = (-1)^{\varepsilon_{i,\sigma}\varepsilon_{j,\tau}}\, y_i^{\varepsilon_{i,\sigma}}\, y_j^{\varepsilon_{j,\tau}}$, para todo $i \neq j$ e quaisquer que sejam $\sigma, \tau \in G$, obtemos:

$$\alpha(\sigma,\tau) = (-1)^{\sum_{i<j} \varepsilon_{i,\sigma}\varepsilon_{j,\tau}} \cdot \prod_{\varepsilon_{i,\sigma}=\varepsilon_{i,\tau}=1} a_i$$

ou $\alpha(\sigma,\tau) = \prod_{i<j} g_{ij}(\sigma,\tau) \cdot \prod_{i=1}^{n} f_i(\sigma,\tau)$,
onde $g_{ij}(\sigma,\tau) = (-1)^{\varepsilon_{i,\sigma}\varepsilon_{j,\tau}}$ e $f_i(\sigma,\tau) = a_i$, se $\sigma,\tau|_{R[\gamma_i]} \neq id_{R[\gamma_i]}$ e $f_i(\sigma,\tau) = 1$, caso contrário , são os cociclos representantes de $[a_i^{-1}b_i, a_j^{-1}b_j] = (a_i^{-1}b_i, a_j^{-1}b_j)$ (cf.Prop.6.2) e $(a_i^{-1}b_i, a_i)$, respectivamente . Então ,

$\alpha_S(q,q_1) = \prod_{i<j} (a_i^{-1}b_i, a_j^{-1}b_j) \prod_{i=1}^{n} (a_i^{-1}b_i, a_i)$ e desta igualdade, por aplicações sucessivas das propriedades de (a,b)(cf.Prop.6.1) obtemos o seguinte resultado .

<u>Lema 6.3</u> - $\alpha_S(q,q_1) = (\Delta(q) - \Delta(q_1))h(q)h(q_1)$.

<u>Teorema 6.4</u> - Sejam (M,q) e (M,q_1) R-espaços quadráticos. Se o posto de M é 2 ou 3 então $(M,q_1) \cong (M,q)$ se , e somente se , $\Delta(q_1) = \Delta(q)$ e $h(q_1) = h(q)$.

A demonstração deste teorema é uma consequência imedia ta do Lema 6.3 e do Teorema 5.6 .

Finalmente , observamos que , no caso em que R é local e henseliano , de corpo residual $R/\mathfrak{m}$ finito , $(M,q_1) \cong (M,q)$ se, e somente se , $(R/\mathfrak{m} \otimes_R M, \overline{q}_1) \cong (R/\mathfrak{m} \otimes_R M, \overline{q})$ (cf. [D], Chap.IV , Teor.4.5) se , e somente se , $\Delta(\overline{q}_1) = \Delta(\overline{q})$ (cf. $[S]_2$, Chap.IV, §1, Cor. da Prop. 5) se , e somente se $\Delta(q_1) = \Delta(q)$.

Bibliografia

[A] - Arf , C. - Untersuchungen uber quadratische Formen in Korpen der Carakterisk 2 - J.f.d. reine und angew. Math. 183 , (1941) , 148 - 167 .

[AG] - Auslander , M. , Goldman , O. - The Brauer group of a commutative ring - Trans. Amer. Math. Soc. , 97 (1960) 367 - 409 .

[B]$_1$ - Bass , H. - Lectures on topics in algebraic K-theory , Tata Inst. Fund. Research , Bombay (1967).

[B]$_2$ - Bass , H. - Clifford algebras and Spinor norms over a commutative ring - Am. J. Math. (1974) 156 - 206 .

[Bo] - Bourbaki , N. - Algèbre , Chap. 5,8 et 9 - Hermann ,Paris (1973) .

[CHR] - Chase , S.U. , Harrison , D.K. , Rosenberg , A. -Galois theory and Galois cohomology of commutative rings - Mem. Am. Math. Soc. 52 (1965) .

[D] - Dorboz ,M. - Autour du groupe de Witt - These de 3ème cycle , Math. Montpellier (1972).

[H] - Hornix , E.A.M. - Stiefel - Whitney invariants of quadratic forms over local rings - Journal of Algebra , 26 (1973) , 258 - 279 .

[K] - Klingenberg , W. - Orthogonalen Gruppen uber lokalen Ringen , Am. J. Math. , 83 (1961) , 281 - 320 .

[Kn] - Knebusch , M. -Isometrien uber semi-lokalen Ringen , Math. Z. , 108 (1969) 255 - 268 .

[KO] - Knus , M.A. , Ojanguren , M. - Theorie de la descente et Algèbres d'Azumaya - Lectures Notes in Math., 389 , Springer Verlag - Berlin (1974) .

[LMV] - Laratonda , A. Micali , A. Villamayor , O.E. - Sur le groupe de Witt - Symposia Matematica (1973) .

[MR] - Micali , A.,Revoy , Ph. - Modules quadratiques -- Cahiers de Mathematiques , Montpellier (1977).

[MV]$_1$ - Micali , A. , Villamayor , O.E. - Sur les algèbres de Clifford , Ann. Sc. Ec. Norm. Sup. 4ème Série (1968), 271 - 3044.

[MV]$_2$ - Micali , A. , Villamayor , O.E. - Sur les algèbres de Clifford II , J.f.d. reine und angew . Math. 242 (1970) , 61 - 90 .

[MV]$_3$ - Micali , A. , Villamayor , O.E. - Algèbres de Clifford et Groupe de Brauer - Ann. Sc. Ec. Norm. Sup. 4ème Série (1971) , 285 - 310 .

[N] - Nagata , M. - Local Rings - Interscience Publishers , New York (1962) .

[R] - Revoy , Ph. - Autour des Formes Quadratiques - Thèse de Doctorat d'État - Math. Montpellier (1975) .

[S]$_1$ - Serre , J.P. - Corps Locaux , Act. Sci. Ind. 1296 , Paris (1962) .

[S]$_2$ - Serre , J.P. - Cours d'arithmètique , P.U.F. , Paris (1970) .

[Sm] - Small , C. - The group of quadratic extensions . Journal of Pure and Applied Algebra 2 (1973) , 83 - 105 .

[Sp] - Springer , T.A. - On the equivalence of quadratic forms Kon.Ned.Akad.Wet.Proc., Ser A , 62 (1959) , 241 - 253.

[V] - Villamayor , O.E. - Separable algebras and Galois ex - tensions , Osaka J. Math. 4 (1963) , 161 - 171 .

[W] - Witt , E. - Theorie der quadratischen Formen in belie- bigen Korpen , J.f.d. reine und angew. Math. , 176 (1937) , 31 - 44 .