EXTENSÕES DE CLIFFORD
E
VALORES DE CARACTERES

Henrique Salvador Salazar Panzarelli

DISSERTAÇÃO APRESENTADA AO
INSTITUTO DE MATEMÁTICA E
ESTATÍSTICA DA UNIVERSIDA-
DE DE SÃO PAULO, PARA OB-
TENÇÃO DO GRAU DE MESTRE
EM MATEMÁTICA.

ORIENTADOR: Prof. Dr. HÉCTOR A. MERKLEN G.

Durante a elaboração deste trabalho o autor recebeu
apoio financeiro do C.N.Pq.

São Paulo, Julho de 1981

À Celina, Andrés e Adriana

AGRADECIMENTOS:

Agradecemos às várias pessoas que, de uma forma ou de outra, nos auxiliaram no decorrer de nosso trabalho.

Em particular,

ao professor Héctor A. Merklen que sugeriu o tema desta dissertação e que, com seu apoio, contribuiu de modo decisivo para sua execução;

aos colegas Iracema Martin Bund, Seiji Hariki e Jorge Aragona pelo espontâneo e constante incentivo;

à equipe da Biblioteca que com gentil presteza nos auxiliou em nossas pesquisas;

à Srta. Regina Helena, pelo atento trabalho datilográfico.

ÍNDICE

	Página
INTRODUÇÃO	(i)
CAPÍTULO 0 - PRÉ-REQUISITOS.	1
§ 1 - Álgebras e ideais Minimais.	1
§ 2 - Representações, caracteres e <u>idem</u> potentes.	4
§ 3 - Push-out e pull-back.	6
§ 4 - Factor sets e álgebra de grupo "twisted".	7
§ 5 - O homomorfismo transfer	9
§ 6 - H^2 , extensões e soma de Baer.	10
§ 7 - Complexos, cohomologia, Ext^n e H^n	12
§ 8 - O homomorfismo inflação.	15
CAPÍTULO I - Sistemas de Clifford.	18
§ 9 - A teoria de Clifford.	18
§10 - Ações de G	24
§11 - Idempotentes de A_1	30
§12 - Sub-álgebra centrais simples de A	36
§13 - A_1 -constituintes.	40
§14 - A correspondência de Clifford	44
§15 - A_1 -unidimensionais.	47
CAPÍTULO II- CARACTERES E EXTENSÕES DE CLIFFORD	53
§16 - Extensão de Clifford <u>correspon</u> <u>de</u> a um caráter.	53
§17 - Extensões centrais.	58
§18 - Modificações de H	63

	pág.
§19 - Extensões ciclotômicas.	66
§20 - Expoentes.	69
Bibliografia.	77

INTRODUÇÃO

Seguindo as linhas estabelecidas por A.H. Clifford no ano de 1937 no artigo [2], recentemente diversos autores tem investigado a relação existente entre representações de um grupo e representações de um seu subgrupo normal. Essa relação é estendida de alguma maneira a uma situação envolvendo uma álgebra e uma sub-álgebra.

Em 1964, K.Yamakazi estudando representações projetivas introduz em [24] o conceito de "extensão de anel de um grupo finito sobre um corpo" da seguinte maneira: Sejam K um corpo arbitrário e A um anel sobre K , isto é, $K \subseteq A$ e $1_K = 1_A$, e seja H um grupo finito. Uma extensão de anel de H sobre K é um objeto que consiste de um anel A sobre K e uma decomposição em soma direta, $A = \bigoplus_{h \in H} A_h$, numa família de K -submódulos A_h , $h \in H$, de A , tal que

$$1) \quad A_h = K e_h = e_h K, \text{ para algum } e_h \neq 0, \quad \forall h \in H$$

$$2) \quad A_g A_h = A_{gh}, \quad \forall g, h \in H$$

Na mesma época, S.B.Conlon em [3] e P.A.Tucker em [19] a [22], estudaram a decomposição de representações induzidas de representações indecomponíveis (e irredutíveis)

de um subgrupo normal através de uma análise do anel de endomorfismos da representação induzida em termos do anel de endomorfismos da representação original.

Em 1968, H.N.Ward publica [23], no qual amplia os resultados obtidos por Conlon e Tucker simplificando as demonstrações. Nesse trabalho ele generaliza o conceito de ex ten são de anel introduzido por Yamazaki tomando uma K-álgebra A (de dimensão finita) tal que:

- 1) $A_g = a_g A_1 = A_1 a_g$, para algum $a_g \in A$, $\forall g \in G$,
- 2) $A_g A_h = A_{gh}$, $\forall g, h \in G$,
- 3) A é soma direta dos A_g ,
- 4) o elemento 1 de A pertence a A_1 , (logo A_1 é uma sub-álgebra de A).

Em 1967, E.C.Dade em [6] apresenta uma primeira axiomatização da teoria de Clifford que posteriormente é ex pandida e apresentada de maneira muito mais limpa e clara em [7], no ano de 1970, introduzindo o conceito de "sistema de Clifford" onde, fundamentalmente, se tomam como axiomas as mes mas propriedades exigidas por Ward, sem nenhuma restrição so bre a dimensão da álgebra. A força dessa teoria é comprovada plenamente no mesmo ano com a publicação do extenso arti go [8] de Dade, onde é demonstrado o seguinte fato: dados um grupo finito G , um subgrupo normal N de G , um corpo F al

gebricamente fechado de característica p arbitrária e ψ um $\mathbb{F}$ -caráter de N irreduzível G -invariante, se $[G:N]$ é relativamente primo com $|N|$, então ψ pode ser estendido a um $\mathbb{F}$ -caráter irreduzível ϕ de G . Nesse tipo de problema já tinham trabalhado I.M.Isaacs, ver [15] e G.Glauberman, ver [13], onde o único caso não coberto pelo resultado de G.Glauberman sobre a correspondência bijetora entre $\text{Irr}_N(G)$, o conjunto de todos os caracteres complexos irreduzíveis N -fixos de G , e $\text{Irr}(\mathbb{C})$, o conjunto de todos os caracteres complexos irreduzíveis de G , é quando G é solúvel e de ordem ímpar, problema, este, estudado e resolvido por Dade.

Coincidentemente, em 1969, J.M.G.Fell, analista, inspirado nas idéias de Mackey, estuda em [11] "fibrados algébricos homogêneos sobre um grupo G ", considerando também representações de dimensão infinita desses fibrados. No caso de ser G um grupo finito esses fibrados constituem o que Dade chama de álgebra de Clifford G -graduada. Interessante é comprovar como matemáticos de áreas diferentes acabam, cada um a sua maneira, captando e aproveitando idéias que num certo momento estão pairando no ar.

No nosso trabalho aproveitamos as apresentações de Dade feitas em [7] e [3] para analisarmos as aplicações feitas em [9], onde o autor estuda a seguinte situação: dados dois grupos finitos G e H e um epimorfismo $\eta : H \rightarrow G$ com núcleo N , seja $\mathbb{K}$ um subcorpo dos complexos que contém

$\chi(N)$, onde χ é um caráter complexo irredutível H -estável de N ; as extensões de χ a H são governadas por uma extensão central $H \langle \chi \rangle$ de G pelo grupo multiplicativo K de $\mathbb{K}$. Essa extensão, por sua vez, corresponde a um elemento $\alpha = (\chi, K)$ de $H^2(G, K)$. Estuda-se esse elemento α com detalhe. Denotando por $\text{tor}(K)$ o grupo das raízes da unidade de $\mathbb{K}$, o quociente $K/\text{tor}(K)$ é sem torção e a sequência exata $1 \rightarrow \text{tor}(K) \rightarrow K \rightarrow F(K) \rightarrow 1$ induz (não naturalmente) uma sequência exata cindida nos seguintes grupos de cohomologia

$$1 \rightarrow H^2(G, \text{tor}(K)) \rightarrow H^2(G, K) \rightarrow H^2(G, F(K)) \rightarrow 1$$

Seja β a imagem de α em $H^2(G, F(K))$, então prova-se que existe um inteiro n tal que β pertence ao núcleo do homomorfismo natural $H^2(G, F(K)) \rightarrow H^2(G, F(K_n))$, induzido pela inclusão de $\mathbb{K}$ na extensão ciclotônica $\mathbb{K}_n$, obtida adjuntando a $\mathbb{K}$ uma raiz n -ésima da unidade. Esse fato é usado para obter majorações da ordem de α : se $r(\mathbb{K})$ e $m(\mathbb{K})$ denotam as ordens dos grupos das raízes $|G/G'|$ -ésimas e $|G|$ -ésimas da unidade em $\mathbb{K}$, então $\beta^{r(\mathbb{K})} = 1$ e $\alpha^{m(\mathbb{K})} = 1$. Esse resultado é demonstrado fazendo uma análise cuidadosa dos núcleos dos homomorfismos naturais $\psi : F(K)/F(K)^t \rightarrow F(L)/F(L)^t$, induzidos por inclusão de $\mathbb{K}$ em certas extensões $\mathbb{L}$.

No Capítulo 0, apresentamos uma miscelânea de resultados bastante conhecidos, indicando os textos onde se podem encontrar os detalhes.

No Capítulo I são introduzidos os "Sistemas de Clifford", e são demonstradas diversas propriedades que serão usadas no capítulo seguinte; é estabelecida a correspondência de Clifford para tais objetos e terminamos caracterizando os sistemas com A_1 $\mathbb{F}$ -unidimensionais como sendo naturalmente equivalentes a extensões centrais de K por G .

No Capítulo II abordamos as extensões de Clifford e suas relações com a extensibilidade de caracteres. No §16, aparece uma condição necessária e suficiente sobre a extensibilidade de X para que o elemento α seja trivial.

Usamos um pouco de Álgebra Homológica, no §17, para provar que a sequência exata $H^2(G, \text{tor}(A)) \rightarrow H^2(G, A) \rightarrow H^2(G, F(A))$ é cindida se A for abeliano; incidentalmente achamos um pequeno resultado sobre grupos. Continuamos, no §18, acumulando informações sobre o elemento α , $\alpha(1 \times X) = \alpha(1) \alpha(X)$, por exemplo, e uma breve incursão nas extensões ciclotômicas, no §19, nos permite provar a existência de um natural n tal que a imagem $\beta(\mathbb{K}_n)$ de β em $H^2(G, F(\mathbb{K}_n))$ é trivial. Finalizamos com o §20, onde são dadas condições suficientes para que $\mathbb{K}$ contenha uma raiz primitiva da unidade e para que α seja trivial.

CAPÍTULO 0

PRÉ-REQUISITOS

Neste capítulo serão reunidos vários resultados so
bre a teoria de álgebras, representações e álgebra homolôgica
que utilizaremos posteriormente.

Exposições de tais resultados podem ser encontra-
das em Felzenszwalb [12], Curtis-Reiner [5], Dornhoff [10],
Rotman [13] e Babakhanian [1].

§ 1 - ÁLGBRAS E IDEAIS MINIMAIS (Ver Felzenszwalb [12])

Seja A uma álgebra associativa com elemento unidada

CAPÍTULO 0

PRÉ-REQUISITOS

Neste capítulo serão reunidos vários resultados sobre a teoria de álgebras, representações e álgebra homológica que utilizaremos posteriormente.

Exposições de tais resultados podem ser encontradas em Felzenszwalb [12], Curtis-Reiner [5], Dornhoff [10], Rotman [18] e Babakhanian [1].

§ 1 - ÁLGBRAS E IDEAIS MINIMAIS (Ver Felzenszwalb [12])

Seja A uma álgebra associativa com elemento unida

de de dimensão finita sobre um corpo K .

Como $1 \in A$, os ideais de A como álgebra são exatamente os ideais de A como anel.

Definição 1.1 - Uma álgebra A é dita semi-simples se A não contém ideais nilpotentes não nulos. Equivalentemente, o radical de A , $\text{rad } A$, é nulo.

Teorema 1.2 - O quociente $A/\text{rad } A$ é semi-simples.

Definição 1.3 - Um elemento $e \in A$ é dito idempotente, se $e^2 = e$.

Se $A = V_1 \oplus \dots \oplus V_n$, como K -álgebras, então $1 = e_1 + \dots + e_n$, onde os e_i são idempotentes ortogonais dois a dois e $V_i = Ae_i$. Se os V_i são ideais bilaterais de A , então os e_i são idempotentes centrais.

Se $e \neq 1$ é um idempotente de A , então $\underline{e}$ e $1 - e$ são idempotentes ortogonais e $A = Ae \oplus A(1-e)$

Teorema 1.4 - Seja A uma álgebra semisimples e seja $J \neq 0$ um ideal à esquerda (respectivamente, direita), então $J = Ae$ (respectivamente, $J = eA$) para algum idempotente $e \in A$.

Corolário 1.5 - Se A é uma álgebra semi-simples e $J \neq 0$ é um ideal (bilateral) de A , então $J = eA = Ae$, onde $\underline{e}$ é um

idempotente central de A .

Definição 1.6 - Uma álgebra A é dita simples se os únicos ideais (bilaterais) de A são os triviais.

Definição 1.7 - Um ideal bilateral J , não nulo, de uma álgebra A é dito minimal se não existe nenhum ideal bilateral J' , não nulo, de A tal que $J' \subsetneq J$.

Lema 1.8 - Se J é um ideal minimal de uma álgebra semi-simples A , então J é uma álgebra simples.

Lema 1.9 - Se $B_1, \dots, B_r$ são ideais minimais de uma álgebra semi-simples A distintos dois a dois, então a soma $B_1 + \dots + B_r$ é direta. Em particular, A contém somente um número finito de ideais minimais.

Lema 1.10 - (Wedderburn). Se $B_1, \dots, B_r$ são todos os ideais minimais de uma álgebra semi-simples A , então $A = B_1 \oplus \dots \oplus B_r = Ae_1 \oplus \dots \oplus Ae_r$, onde os e_i são idempotentes centrais primitivos ortogonais.

Definição 1.11 - Uma álgebra A diz-se central simples sobre K , se A é uma álgebra simples de centro K .

Dentre as propriedades das álgebras simples rela-

tivamente do produto tensorial, temos:

Proposição 1.12 - Se A é uma álgebra simples central sobre K e B é uma álgebra simples sobre K , então $A \otimes_K B$ é simples.

Definição 1.13 - Dado $S \subset A$, o centralizador $C_S(A)$ de S em A é o conjunto $\{a \in A \mid as = sa, \forall s \in S\}$.

Proposição 1.14 - Sejam S e S' sub-álgebra de A e A' , respectivamente, contendo as unidades. Então

$$C_A \times_K A, (S \times_K T) = C_A(S) \times_K C_{A'}(T)$$

Proposição 1.15 - Se A e B são álgebras centrais simples sobre K então $A \otimes_K B$ é central simples sobre K .

§ 2 - REPRESENTAÇÕES, CARACTERES E IDEMPOTENTES

(Ver Dornhoff [10])

Para dar a conexão entre idempotentes centrais de uma álgebra de grupo KG e caracteres irredutíveis, lembramos várias definições.

Definição 2.1 - Sejam G um grupo, R um anel comutativo e V um R -módulo livre de dimensão finita. Uma representação de G em V é um homomorfismo de grupos

$$T : G \rightarrow GL(V)$$

Uma representação fornece uma representação matri
cial escolhendo uma base de V .

Lema 2.2 - Estudar representações de um grupo G é equiva-
lente a estudar RG -módulos livres sobre R .

Definição 2.3 - Sejam A um anel e M um A -módulo não nulo.

M é dito irredutível se ele não contém submódulos
próprios. M é dito completamente redutível (ou semi-simples)
 M é a soma direta de A -módulos irredutíveis.

Definição 2.4 - Uma representação $G \rightarrow GL(V)$ é dita irredu
tível (respectivamente, completamente redutível) se V é
irredutível (respectivamente, completamente redutível).

Definição 2.5 - Sejam k um corpo, G um grupo, V um k -espa
ço vetorial de dimensão finita e $T: G \rightarrow GL(V)$ uma representa-
ção. A função $\chi: G \rightarrow k$ definida por

$$\chi(x) = \text{tr } T(x), \quad \forall x \in G$$

é dita um caráter; que é dito irredutível se T o for.

Lema 2.6 - Assuma que $\text{car } k \nmid |G|$ e seja $K \supset k$ um corpo
de decomposição de G (por exemplo, K algebricamente fecha-
do). Seja V um KG -módulo irredutível que fornece o caráter
 χ e seja

$$kG = \bigoplus_{i=1}^s A_i, \quad A_i \text{ algebra simples, } \forall i$$

Então:

- 1) existe um único j , $1 \leq j \leq s$, tal que $A_j \cap V = 0$;
- 2) para tal A_j , $Z(A_j) \cong k(X)$, onde $k(X)$ é a extensão de k por todos os $\chi(x)$, $x \in G$;
- 3) se e_j é o elemento unidade de A_j , então

$$e_j = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g$$

Demonstração Ver Lemas 24.7 e 24.13 de [6].

§ 3 - PUSH-OUT E PULL-BACK (Ver Rotman [13])

Definição 3.1 - Um push-out de $\begin{array}{c} A \xrightarrow{g} C \\ f \downarrow \\ B \end{array}$ é um diagrama comutativo

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ f \downarrow & & \downarrow \alpha \\ B & \xrightarrow{\beta} & X \end{array}, \text{ tal que se } X', \alpha', \beta' \text{ são tais que } \begin{array}{ccc} A & \xrightarrow{g} & C \\ f \downarrow & & \downarrow \alpha' \\ B & \xrightarrow{\beta'} & X' \end{array}$$

é comutativo, existe um único morfismo $X \rightarrow X'$ tal que

$$\begin{array}{ccc} & C & \\ \alpha \downarrow & & \alpha' \\ B \xrightarrow{\beta} X & \xrightarrow{\quad} & X' \\ \beta' \nearrow & & \end{array} \text{ é comutativo.}$$

A noção dual é a de pull-back, que completa o dia

$$\begin{array}{ccc} & C & \\ & \downarrow g & \\ \text{grama} & B \rightarrow A & \\ & f & \end{array}$$

Na categoria dos módulos e dos grupos tais objetos existem e são únicos a menos de isomorfismos.

Explicitamente, o push-out de $\begin{array}{ccc} & C & \\ & \downarrow g & \\ A & \xrightarrow{f} & B \end{array}$ é dado

por $X = (B \oplus C)/D$, onde $D = \{ (f(a), -g(a)) \mid a \in A \}$, junto com os morfismos canônicos de B e C em X.

O pull-back de $\begin{array}{ccc} & C & \\ & \downarrow g & \\ B & \xrightarrow{f} & A \end{array}$ é dado por

$Y = \{ (b, c) \in B \times C \mid f(b) = g(c) \}$ com as projeções canônicas de Y em B e C.

§ 4 - FACTOR SETS E ALGEBRAS DE GRUPOS "TWISTED" (Ver Dornhoff [10])

Definição 4.1 - Sejam A um grupo abeliano e G um grupo que age sobre A. Uma função $\alpha : G \times G \rightarrow A$ é dita um A-factor set de G se, somente se,

$$\alpha(xy, z) \alpha(x, y) = \alpha(x, yz) \cdot x\alpha(y, z) \quad , \quad \forall x, y, z \in G.$$

No caso da ação de G ser trivial, essa expressão

simplifica-se pois $x\alpha(y,z) = \alpha(y,z)$.

Definição 4.2 - Sejam G um grupo, $\mathbb{F}$ um corpo e α um F -factor set de G e seja $g \in G \mapsto \hat{g} \in G$ uma bijeção. Define-se a álgebra de grupo "twisted" $\mathbb{F}^\alpha[G]$ relativamente a α como sendo o F -espaço vetorial com base $\{\hat{g} \mid g \in G\}$ munido com a multiplicação

$$\hat{g} \hat{h} = gh \alpha(g,h), \quad \forall g,h \in G$$

estendida por distributividade a todo o espaço.

Observação 4.3 - Dados um corpo $\mathbb{F}$ e uma extensão central de F por um grupo G

$$F \rightarrowtail G^* \twoheadrightarrow G,$$

então $G \xrightarrow{\phi} G^*/F$ com $\phi(x) = h_x F$, para $x \in G$ e $h_x \in G^*$. Então, temos

$$h_x h_y = h_{xy} \alpha(x,y), \quad \text{para algum } \alpha(x,y) \in F.$$

Verifica-se, facilmente, que α é um F -factor set de G^* e podemos, em consequência construir a álgebra $\mathbb{F}^\alpha[G^*]$ relativamente a α .

§ 5 - O HOMOMORFISMO TRANSFER (Ver Adilson [17])

Sejam G um grupo, H um subgrupo de G de índice n , H' o subgrupo derivado de H e $x_1, x_2, \dots, x_n$ representantes das classes laterais à esquerda de G , módulo H . Assim, G se escreve como união disjunta de $x_1H, x_2H, \dots, x_nH$.

Fixado $g \in G$ arbitrário, a relação

$$g x_i = x_j h_i, \text{ com } h_i \in H, \quad i, j = 1, 2, \dots, n$$

define uma permutação $\sigma = \sigma_g$ do conjunto $\{1, 2, \dots, n\}$ colocando

$$\sigma(i) = j.$$

Prova-se que a função $T : G \rightarrow H/H'$ definida por $T(g) = \prod_{i=1}^n h_i \pmod{H'}$, não depende dos representantes x_i e que é um homomorfismo, dito o homomorfismo transfer de G em H .

Observação 5.1 - Se $A \twoheadrightarrow E \twoheadrightarrow G$ é uma extensão central de um grupo abeliano A por um grupo finito G , então o homomorfismo transfer $T: E \rightarrow A$, verifica $T(a) = a^n$, $\forall a \in A$, onde $n = |E/A| = |G|$.

Com efeito, como $A' = 1$,

$$x_{\sigma(i)}^{-1} a x_i = h_i \in A, \quad i = 1, 2, \dots, n$$

e sendo A central, temos que existe $k \in \{1, 2, \dots, n\}$ tal que

$$\prod_{i=1}^n h_i = \prod_{i=1}^n x_{\sigma(i)} a x_i = x_k^{-1} a^n x_k = a^n, \quad \forall a \in A.$$

§ 6 - H², EXTENSÕES E SOMA DE BAER (Ver Rotman [18])

Seja $A \xrightarrow{i} E \xrightarrow{p} G$ uma sequência exata de grupos com A abeliano. Dada uma secção $s: G \rightarrow E$, podemos definir uma estrutura de G -módulo (isto é, $\mathbb{Z}G$ -módulo) sobre iA e, portanto, sobre A pela fórmula

$$x(ia) = (sx)(ia)(sx)^{-1}, \quad x \in G, \quad a \in A;$$

e verifica-se facilmente, usando o fato de que A é abeliano, que diferentes secções dão origem ao mesmo G -módulo.

Definição 6.1 - Dado um G -módulo A , definimos uma extensão de A por G como sendo uma sequência exata de grupos

$$A \xrightarrow{i} E \xrightarrow{p} G$$

tal que a estrutura de G -módulo de A coincide com a dada pela fórmula acima.

Observamos que se A é um G -módulo trivial, então a extensão é central, isto é, iA está contido no centro do

do grupo E . No nosso trabalho nos limitaremos a esse caso particular em que a ação de G sobre A é trivial.

Duas extensões de A por G , $A \twoheadrightarrow E_i \twoheadrightarrow G$, $i = 1, 2$, são ditas equivalentes se existir um homomorfismo de E_1 em E_2 que torna comutativo o diagrama

$$\begin{array}{ccccc} A & \twoheadrightarrow & E_1 & \twoheadrightarrow & G \\ \parallel & & \downarrow & & \parallel \\ A & \twoheadrightarrow & E_2 & \twoheadrightarrow & G \end{array}$$

Denota-se o conjunto dessas classes de equivalência por $E(G, A)$ e a classe de uma extensão $A \twoheadrightarrow E \twoheadrightarrow G$ por $[E]$. Pode-se definir a soma de duas extensões (dita soma de Baer) de modo a tornar $E(G, A)$ um grupo abeliano, no qual o elemento neutro é a classe de equivalência da extensão.

$$A \twoheadrightarrow A \times G \twoheadrightarrow G$$

onde $A \times G$ é o produto semi-direto de A por G , com

$(a, x)(a', x') = (a + xa', xx')$, $a \in A$, $x \in G$ no caso geral, e, simplesmente, o produto direto no caso da ação de G sobre A ser trivial.

Indicamos a seguir como se constroi a soma de Baer de elementos de $E(G, A)$: sejam $A \twoheadrightarrow E \twoheadrightarrow G$ e $A \twoheadrightarrow E' \twoheadrightarrow G$ representantes, respectivamente, das classes $[E]$ e $[E']$. Um

representante ξ da classe $[E] + [E']$ é obtido em duas etapas, fazendo um push-out seguido de um pull-back como indica o seguinte diagrama:

$$\begin{array}{ccccc}
 A \oplus A & \xrightarrow{\quad} & E \oplus E' & \longrightarrow & G \oplus G' \\
 \nabla \downarrow & \text{push-out} & \downarrow & & \parallel & \text{1a. etapa} \\
 A & \xrightarrow{\quad} & \nabla(E \oplus E') & \longrightarrow & G + G' \\
 \parallel & & \uparrow & \text{pull-back} & \uparrow \Delta & \text{2a. etapa} \\
 A & \xrightarrow{\quad} & (\nabla(E \oplus E'))_{\Delta} & \longrightarrow & G
 \end{array}$$

onde $\nabla(a, a') = a + a'$ e $\Delta(g) = g + g$

Com essa operação de adição, $E(G, A)$ é um grupo abeliano, chamado segundo grupo de cohomologia de G com coeficientes em A, denotado por $H^2(G, A)$.

Podemos colocar esse grupo num contexto mais amplo, que esboçamos a seguir.

§ 7 - COMPLEXOS, COHOMOLOGIA, Ext^n e H^n (Ver Rotman [18] e Babakhanian [1])

Um complexo A é uma sequência A_n , $n \in \mathbb{Z}$, de R-módulos e homomorfismos d_n

$$A : \dots \rightarrow A_n \xrightarrow{d_n} A_{n+1} \xrightarrow{d_{n+1}} A_{n+2} \rightarrow \dots$$

tais que $d_{n+1} d_n = 0$.

Como $\text{im } d_n \subset \ker d_{n+1}$, podemos definir os grupos $H^n(A) = \ker d_{n+1} / \text{im } d_n$, para $n \in \mathbb{Z}$, dito o n-ésimo grupo de cohomologia do complexo.

Define-se um morfismo de complexos $f : A \rightarrow A'$ como sendo uma coleção de R-homomorfismos $f_n : A_n \rightarrow A'_n$ tal que o diagrama

$$\begin{array}{ccccccc} & & & d_n & & & \\ & & & \downarrow & & & \\ \dots & \rightarrow & A_n & \xrightarrow{\quad} & A_{n+1} & \rightarrow & \dots \\ & & \downarrow f_n & & \downarrow f_{n+1} & & \\ & & & d'_n & & & \\ \dots & \rightarrow & A'_n & \xrightarrow{\quad} & A'_{n+1} & \rightarrow & \dots \end{array}$$

é comutativo, para todo n .

Dados dois complexos A e A' , um morfismo $f : A \rightarrow A'$ induz, para todo n , um R-homomorfismo

$$f_n^* : H^n(A) \rightarrow H^n(A')$$

Uma sequência de complexos $A \rightarrow B \rightarrow C$ é dita exata se $A_n \rightarrow B_n \rightarrow C_n$ é exata, para todo n . Nesse caso obtêm-se a seguinte sequência longa exata de cohomologia

$$\dots \rightarrow H^n(A) \rightarrow H^n(B) \rightarrow H^n(C) \rightarrow H^{n+1}(A) \rightarrow \dots$$

Uma resolução projetiva $\{P_n\}$ de um R-módulo A é uma sequência exata $\dots \rightarrow P_n \xrightarrow{d_n} P_{n-1} \rightarrow \dots \rightarrow P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \rightarrow 0$ onde cada P_i é projetivo. Como todo R-módulo é imagem de um R-módulo livre (e portanto projetivo), todo R-módulo tem uma resolução projetiva.

Sejam A e C R-módulos e $\{P_n\}$ uma resolução projetiva de A. No complexo

$$0 \rightarrow \text{Hom}_R(P_0, C) \xrightarrow{d'_0} \text{Hom}_R(P_1, C) \xrightarrow{d'_1} \dots$$

podemos considerar o n-ésimo grupo de cohomologia $\ker d'_{n+1} / \text{im } d'_n$ denotado $\text{Ext}_R^n(A, C)$. Prova-se que esses grupos não dependem da particular resolução projetiva de A.

Dã-se uma interpretação de $\text{Ext}_R^n(A, C)$, $n = 1, 2, \dots$, por meio de n-extensões exatas de C por A:

$$0 \rightarrow C \rightarrow E_n \rightarrow \dots \rightarrow E_1 \rightarrow A \rightarrow 0$$

(Vide Hilton-Stammbach, [14], pags. 91 e 148, ou Rotman [18], para o caso $n = 1$).

De uma sequência exata de R-módulos $A \rightarrow B \rightarrow C$ podemos construir, tomando resoluções projetivas de A, B e C, uma sequência exata de complexos $\hat{A} \rightarrow \hat{B} \rightarrow \hat{C}$.

Uma sequência exata de complexos $A \rightarrow B \rightarrow C$, induz as sequências exatas

$$\dots \rightarrow \text{Ext}^n(C, D) \rightarrow \text{Ext}^n(B, D) \rightarrow \text{Ext}^n(A, D) \rightarrow \text{Ext}^{n+1}(C, D) \rightarrow \dots$$

e

$$\dots \rightarrow \text{Ext}^n(D, A) \rightarrow \text{Ext}^n(D, B) \rightarrow \text{Ext}^n(D, C) \rightarrow \text{Ext}^{n+1}(D, A) \rightarrow \dots,$$

para qualquer complexo D.

No caso particular em que, dados um grupo G, um G-módulo A e tomamos uma resolução projetiva $\{P_n\}$ de $\mathbb{Z}$ considerado como G-módulo trivial, no complexo

$$0 \rightarrow \text{Hom}_{\mathbb{Z}G}(P_0, A) \rightarrow \text{Hom}_{\mathbb{Z}G}(P_1, A) \rightarrow \dots$$

os grupos $\text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, A)$ são denotados por $H^n(G, A)$ e chamados n-ésimo grupo de cohomologia de G com coeficientes em A.

Prova-se que se G é um grupo finito, então a ordem de todo elemento de $H^n(G, A)$ divide a ordem de G, $\forall n \geq 1$.

§ 8 - O HOMOMORFISMO INFLAÇÃO (Ver Babakhanian [1])

Sejam A um G-módulo e $N \twoheadrightarrow G \twoheadrightarrow Q$ uma sequência exata de grupos. Consideremos o subgrupo A^N dos elementos de A invariantes pela ação de N; ele admite uma estrutura de Q-módulo. Seja $A^N \hookrightarrow A$ a inclusão de A^N em A.

Dada uma extensão $A^N \twoheadrightarrow E \twoheadrightarrow Q$, que representa

um elemento $[E]$ de $H^2(Q, A^N)$, fazendo um pull-back seguido de um push-out como indica o diagrama

$$\begin{array}{ccccc}
 A & \twoheadrightarrow & E'' & \twoheadrightarrow & G \\
 \uparrow & & \uparrow & & \parallel \\
 \int \text{ push-out} & & & & \text{2a. etapa} \\
 A^N & \twoheadrightarrow & E' & \twoheadrightarrow & G \\
 \parallel & & \downarrow \text{ pull-back} & & \downarrow \\
 & & & & \text{1a. etapa} \\
 A^N & \twoheadrightarrow & E & \twoheadrightarrow & Q
 \end{array}$$

obtemos uma extensão $A \twoheadrightarrow E'' \twoheadrightarrow G$ que representa um elemento $[E'']$ de $H^2(G, A)$.

Demonstra-se que a aplicação

$$\text{inf} : H^2(Q, A^N) \longrightarrow H^2(G, A)$$

definida pela construção acima é um homomorfismo, dito homomorfismo inflação (nos segundos grupos de cohomologia).

Observação 8.1 - Nos interessa em particular, o caso em que A é um G -módulo trivial livre de torção e $Q = G/G'$. Nesse caso, mostramos a seguir, o homomorfismo inflação é injetor.

Seja $\hat{E}_i$ obtido por inflação de E_i , $i = 1, 2$ e suponhamos $\hat{E}_1 \cong \hat{E}_2$. Como o subgrupo derivado E_1' de E_1 está contido no núcleo do homomorfismo transfer e sendo A livre de torção $A \cap E_1' = \{1\}$ e, em consequência $p^{-1}(G)$ tem a forma

$\hat{E}'_i \times A$ e da comutatividade do diagrama

$$\begin{array}{ccccc}
 A & \xrightarrow{\quad} & \hat{E}'_i \times A & \longrightarrow & G' \\
 \parallel & & \downarrow & & \downarrow \\
 A & \xrightarrow{\quad} & \hat{E}_i & \xrightarrow[p]{} & G \\
 \parallel & & \downarrow & & \downarrow \\
 A & \xrightarrow{\quad} & E_i & \longrightarrow & G/G'
 \end{array} \quad (i = 1, 2)$$

$\inf([E_i]) = [\hat{E}_i]$
 $\uparrow$
 $[E_i]$

tiramos que $E_1 \cong \hat{E}_1/\hat{E}'_1 \times A \cong \hat{E}_2/\hat{E}'_2 \times A \cong E_2$.

CAPÍTULO I

SISTEMAS DE CLIFFORD

§ 9 - A TEORIA DE CLIFFORD

A teoria de Clifford relaciona as representações irredutíveis de dimensão finita, sobre um corpo $\mathbb{F}$ algebricamente fechado, de um grupo H com as de um subgrupo normal N de H . Equivalentemente, relaciona os ideais bilaterais maximais de codimensão finita de $\mathbb{F}H$ com os de $\mathbb{F}N$. Na axiomatização dessa teoria são usados, em vez de H e N , as álgebras de grupos $A = \mathbb{F}H$ e $A_1 = \mathbb{F}N$. A relação entre um elemento $g \in G = H/N$ e a álgebra A é dada pelo "sub-espço lateral" A_g gerado sobre $\mathbb{F}$ pelos elementos da classe lateral Ng . Claramente, A é soma dos seus sub-espços A_g , $g \in G$. Se $g, h \in G$, então o produto $A_g A_h$ é A_{gh} . Finalmente, A_1 contém a identidade 1 de G e A . Essas três propriedades constituem os axiomas

da seguinte definição.

Definição 9.1 - Um sistema de Clifford $A, \{A_g \mid g \in G\}$ sobre um corpo $\mathbb{F}$ (algebricamente fechado) é formado por uma álgebra associativa A sobre $\mathbb{F}$, um grupo G e uma família de $\mathbb{F}$ -subespaços A_g de A , indexada pelos elementos g de G , satisfazendo as seguintes condições:

$$a) A = \sum_{g \in G} A_g,$$

$$b) A_g A_h = \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in A_g, y_i \in A_h, n=1,2,\dots \right\} = A_{gh}, \forall g, h \in G,$$

c) a sub-álgebra A_1 tem uma identidade bilateral.

Um sistema de Clifford será dito G-graduado se for satisfeita a condição

$$d) A = \bigoplus_{g \in G} A_g.$$

Os axiomas anteriores estabelecem uma "representação" $g \longmapsto A_g$ de G por sub-espaços vetoriais A_g de A .

EXEMPLOS:

- 1 - Como indicamos na introdução do parágrafo, dados um grupo H e um subgrupo $N \triangleleft H$, tomando $A = \mathbb{F}H$ e A_g como sendo o $\mathbb{F}$ -subespaço gerado

por $\{x | x \in Ng\}$, obtemos um sistema de Clifford G-graduado onde $A_1 = \mathbb{F}N$.

2 - Dado um corpo $\mathbb{F}$ qualquer, tomando $G = \{1\}$ e $A = A_1 = \mathbb{F}$, obtemos um sistema de Clifford trivial $A, \{A_1\}$.

3 - Sejam G um grupo transitivo de permutações sobre $\{1, \dots, n\}$ e $\mathbb{F}$ um corpo. Sejam $V_1, \dots, V_n$ $\mathbb{F}$ -espaços vetoriais de dimensão finita não triviais. Identifiquemos cada V_i , $i = 1, 2, \dots, n$, com a sua imagem natural na soma direta $V = V_1 \oplus \dots \oplus V_n$.

Seja A a álgebra $\text{Hom}_{\mathbb{F}}(V, V)$. Para cada $i, j = 1, 2, \dots, n$, seja

$$A_{ij} = \{f \in A \mid f(V_k) = \{0\}, \text{ se } k \neq j \text{ e } f(V_j) \subset V_i\}$$

Verifica-se facilmente que $A = \bigoplus_{i,j=1}^n A_{ij}$ e que

$$A_{ij}A_{kl} = \begin{cases} \{0\}, & \text{se } j \neq k \\ A_{il}, & \text{se } j = k. \end{cases}$$

Para cada $g \in G$, definimos $A_g = \bigoplus_{i=1}^n A_{ig(i)}$. De

corre das propriedades destacadas acima e da

transitividade de G , que $A, \{A_g | g \in G\}$ é um sistema de Clifford sobre $\mathbb{F}$ que é G -graduado se, e somente se, G é um grupo transitivo de permutações regular.

4 - Seja A a álgebra das funções racionais sobre um corpo $\mathbb{F}$ algebricamente fechado. Dados $f, g \in \mathbb{F}[X]$, define-se $\text{grau}(\frac{f}{g}) = \text{grau}(f) - \text{grau}(g)$. Seja $A_m = \{ \frac{f}{g} \in A | \text{grau}(\frac{f}{g}) < m \} \cup \{0\}$, $m \in \mathbb{Z}$. Então $A, \{A_m | m \in \mathbb{Z}\}$ é um sistema de Clifford sobre $\mathbb{F}$.

5 - Seja D um anel de valorizações que contém o corpo $\mathbb{F}$, com $\mathbb{Z}$ como seu grupo de valores, tal que o ideal maximal M de D tem $\mathbb{F}$ -codimensão finita em D . Seja A o corpo de frações de D . Então, $A, \{M^n | n \in \mathbb{Z}\}$ é um sistema de Clifford sobre $\mathbb{F}$.

6 - Sejam $\mathbb{K}$ um corpo, H um grupo finito, N um subgrupo normal de H e $G = H/N$. Seja M um R_N -módulo à direita H -estável. Seja $C = \text{Hom}_{\mathbb{K}H}(M^H, M^H)$, onde $M^H = M \otimes_{\mathbb{K}N} H$, então, como no artigo de Ward [23], podemos escrever C na forma

$$C = \bigoplus_{g \in G} C_g,$$

onde cada somando C_g é um $\mathbb{K}$ -sub-espço de C e, para cada $g, h \in G$,

$$C_g C_h = C_{gh}$$

A sub-álgebra C_1 é isomorfa a $\text{Hom}_{\mathbb{K}N}(M, M)$ e, con-
quentemente, uma $\mathbb{K}$ -sub-álgebra de C e que con-
tém a identidade de C .

Na nossa terminologia, $C, \{C_g | g \in G\}$ é um siste-
ma de Clifford G -graduado.

- 7 - Outros exemplos interessantes são fornecidos ,
como veremos posteriormente, pela aplicação do
Corolário 12.5 e pela aplicação da Proposição 15.3.

A seguir damos algumas propriedades elementares de
um sistema de Clifford.

Proposição 9.2 - A identidade 1 de A_1 é a identidade bilater
ral de A .

Demonstração - Decorre diretamente do fato de que $A_1 A A_1 =$
 $= A_1 \left(\sum_{g \in G} A_g \right) A_1 = A. \square$

Proposição 9.3 - Dado $g \in G$, existem elementos $a_1, \dots, a_n,$
 $b_1, \dots, b_n$ em A , para algum natural n , satisfazendo

a) $a_1, \dots, a_n \in A_{g^{-1}},$

b) $b_1, \dots, b_n \in A_g,$

$$c) \quad \sum_{i=1}^n a_i b_i = 1$$

Para tais elementos temos:

$$d) \quad A_g = A_1 b_1 + \dots + A_n b_n;$$

$$e) \quad A_{g^{-1}} = a_1 A_1 + \dots + a_n A_1$$

Assim, cada $A_g, g \in G$, é finitamente gerado como A_1 -módulo à esquerda e à direita.

Demonstração - A primeira associação decorre da proposição anterior e da propriedade $A_{g^{-1}} A_g = A_1$. Por outro lado, se $y \in A_g$, então $y = \sum_{i=1}^n (y a_i) b_i \in A_1 b_1 + \dots + A_1 b_n$; donde decorre (d).
Prova-se (e) de maneira análoga. $\square$

Dado um sistema de Clifford A , $\{A_g; g \in G\}$ é fácil obter novos sistemas a partir dele; como mostram as seguintes proposições.

Proposição 9.4 - Se ψ é um epimorfismo da álgebra A sobre uma álgebra $\psi(A)$, então $\psi(A), \{\psi(A_g); g \in G\}$ um sistema de Clifford. $\square$

Dado um sub-conjunto S de G , definimos $A_S = \sum_{g \in S} A_g$. Temos, então, $A_S A_T = A_{ST}, \forall S, T \subset G$.

Proposição 9.5 - Se H é um subgrupo de G , então

$A_H, \{A_g; g \in H\}$ é um sistema de Clifford. $\square$

Proposição 9.6 - Se H é um subgrupo normal de G , então

$A, \{A_g; g \in G/H\}$ é um sistema de Clifford.

Demonstração - Decorre diretamente do computo

$$\sum_{g \in G/H} A_g = \sum_{g \in G/H} \sum_{t \in g} A_t = \sum_{t \in G} A_t = A \text{ e do fa-}$$

to de que $1 \in A_H$. $\square$

§10 - AÇÕES DE G

Definição 10.1 - Sejam B um anel e D um sub-anel de B , denotaremos por Mod (D,B) a família de todos os D - D sub-bimódulos em B e por C(D,U) o centralizador de D em U , para cada $U \in \text{Mod (D,B)}$, isto é,

$$C(D,U) = \{u \in U \mid ud = du, \quad \forall d \in D\}$$

Dado um sistema de Clifford $A, \{A_g \mid g \in G\}$ o grupo G age naturalmente sobre o conjunto Mod (A₁,A) e sobre a sub-álgebra C(A₁,A) de A . Sobre o primeiro, a ação é dada pela seguinte proposição.

Proposição 10.2 - Dados $U \in \text{Mod (A₁,A)}$ e $g \in G$, então $U^g = A_{g^{-1}} U A_g$

é uma ação de G sobre $\text{Mod}(A_1, A)$ que preserva inclusões, somas, intersecções e produtos de módulos.

Demonstração - Dados $U \in \text{Mod}(A_1, A)$ e $g \in G$, temos

$$A_1 U^g A_1 = A_1 A_{g^{-1}} U A_g A_1 = A_{g^{-1}} U A_g = U^g, \text{ assim}$$

$$U^g \in \text{Mod}(A_1, A). \text{ Também temos } U^1 = A_1 U A_1 = U \text{ e}$$

$$(U^g)^h = A_h A_{g^{-1}} U A_g A_h = U^{gh}.$$

Fixado $g \in G$, de $U \subset V$ decorre imediatamente que $U^g \subset V^g$, portanto a aplicação $U \mapsto U^g$ preserva inclusões, e em consequência, somas e intersecções em $\text{Mod}(A_1, A)$. Por outro lado, se $U, V \in \text{Mod}(A_1, A)$, então

$$U^g V^g = A_{g^{-1}} U A_g A_{g^{-1}} V A_g = A_{g^{-1}} U V A_g = (UV)^g,$$

portanto a ação dada preserva também produtos. $\square$

Proposição 10.3 - Se $U \in \text{Mod}(A_1, A)$ satisfaz $U^g \subset U$, $\forall g \in G$, então G fixa U . Nesse caso, $UA = AU$ é um ideal bilateral de A .

Demonstração - Como $U = (U^{g^{-1}})^g \subset U^g$, $\forall g \in G$, segue a tese. E como

$$U A_g = A_g A_{g^{-1}} U A_g = A_g U^g = A_g U, \quad \forall g \in G, \text{ temos}$$

$$UA = U\left(\sum_{g \in G} A_g\right) = \left(\sum_{g \in G} A_g\right) U = AU. \quad \square$$

Antes de definir a ação de G sobre $C(A_1, A)$, temos o seguinte Lema

Lema 10.4 - Fixados $g \in G$ e $y \in C(A_1, A)$, existe um único elemento $y^g \in A$ satisfazendo a relação

$$yw = wy^g, \quad \forall w \in A_g.$$

Demonstração - Pela Proposição 9.3, existem elementos $a_1, \dots, a_n \in A_{g^{-1}}$, $b_1, \dots, b_n \in A_g$ satisfazendo $\sum_{i=1}^n a_i b_i = 1$. Definimos $y^g = \sum_{i=1}^n a_i y b_i$. Se $w \in A_g$, então, o elemento $wa_i \in A_{g^{-1}} = A_1$, $i = 1, 2, \dots, n$, comuta com todo elemento y de $C(A_1, A)$, portanto

$$wy^g = \sum_{i=1}^n wa_i y b_i = \sum_{i=1}^n y wa_i b_i = y w 1 = y w, \text{ e a relação é satisfeita.}$$

Por outro lado, seja y^g um elemento que satisfaça a relação. Então tem-se $y b_i = b_i y^g$, $i = 1, 2, \dots, n$, portanto

$$\sum_{i=1}^n a_i y b_i = \sum_{i=1}^n a_i b_i y^g = 1 y^g = y^g$$

o que prova a unicidade. $\square$

Proposição 10.5 - A aplicação $(g, y) \mapsto y^g$ define uma ação de G por automorfismos da sub-álgebra $C(A_1, A)$.

Demonstração - Fixemos $g \in G$ e $y \in C(A_1, A)$. Dados $w \in A_g$ e $z \in A_1$, tem-se $wz \in A_g A_1 = A_g$, e pelo lema anterior,

$$w(zy^g) = (wz)y^g = y(wz) = (yw)z = (wy^g)z = w(y^g z).$$

Donde

$$A_g(zy^g - y^g z) = \{0\}, \quad \text{logo}$$

$$A_1(zy^g - y^g z) = A_{g^{-1}} A_g(zy^g - y^g z) = \{0\},$$

e como $1 \in A_1$, devemos ter $zy^g = y^g z$, $\forall z \in A_1$. Portanto,

$$y^g \in C(A_1, A).$$

Como $1 \in A_1$, tem-se $y = y1 = 1y^1 = y^1$, $\forall y \in C(A_1, A)$. Dados $g, h \in G$, $w \in A_g$ e $u \in A_h$, tem-se $y(wu) = w y^g u = (wu)(y^g)^h$. Como os produtos wu geram $A_g A_h = A_{gh}$, então $yv = v(y^g)^h$, $\forall v \in A_{gh}$, o que implica, pelo lema anterior, que $(y^g)^h = y^{gh}$. Portanto $(g, y) \mapsto y^g$ é uma ação de G sobre $C(A_1, A)$.

Da expressão $y^g = \sum a_i y b_i$ decorre que $y \mapsto y^g$ é aditiva e se $y, t \in C(A_1, A)$ então, pelo lema anterior,

$$(yt)w = ywt^g = w y^g t^g, \quad \forall w \in A_g,$$

mas

$$(yt)w = w(yt)^g, \quad \forall w \in A_g,$$

portanto $(yt)^g = y^g t^g$. Analogamente verifica-se que $(ky)^g = ky^g$, $\forall k \in F$.

Se $y^g = 0$, então $wy^g = yw = 0$, $\forall w \in A_g$, portanto $y = y.1 = \sum a_i (yb_i) = 0$. Finalmente, como $(y^{g^{-1}})^g = y$, temos que $y \mapsto y^g$ é um automorfismo da sub-álgebra $C(A_1, A)$. $\square$

As duas ações anteriores de G estão relacionadas entre si de duas maneiras, dadas pelas seguintes proposições

Proposição 10.6 - Dados $U \in \text{Mod}(A_1, A)$ e $g \in G$, tem-se

$$C(A_1, U)^g = C(A_1, U^g)$$

Demonstração - Dado $y \in C_1(A_1, U) = U \cap C_1(A_1, A)$, tem-se que $y^g \in A_{g^{-1}} \cup A_g = U^g$ e $y^g \in C(A_1, A)$, como foi visto na proposição anterior, portanto $y^g \in C(A_1, U^g)$, $\forall U \in \text{Mod}(A_1, A)$, $\forall g \in G$. $\square$

Proposição 10.7 - Seja S um subconjunto não vazio de $C(A_1, A)$. Então, $SA_1 = A_1 S \in \text{Mod}(A_1, A)$ e $(A_1 S)^g = A_1 S^g$, $\forall g \in G$.

Demonstração - A primeira asserção é imediata. A segunda decorre do fato de que $SA_g = A_g S^g$, $\forall g \in G$, portanto $(A_1 S)^g = A_{g^{-1}} A_1 S A_g = A_{g^{-1}} A_1 A_g S^g = A_1 S^g$. $\square$

Como cada $U \in \text{Mod}(A_1, A)$ é um F -subespaço de A , pode-

mos considerar a codimensão de U em qualquer $B \in \text{Mod}(A_1, A)$ que o contenha.

Definição 10.8 - Dizemos que uma aplicação ψ definida numa família M de $\mathbb{F}$ -espaços vetoriais sobre outra família $\psi(M)$ preserva a codimensão finita se dados $U, V \in M, U \subset V$, tais que a codimensão de U em V seja finita, tem-se que $\psi(U) \subset \psi(V)$ e $\psi(U)$ tem codimensão finita em $\psi(V)$.

Finalizamos o parágrafo com a seguinte proposição, que completa a proposição 10.2.

Proposição 10.9 - Dado $g \in G$, a aplicação $U \mapsto U^g$ preserva a codimensão finita de módulos em $\text{Mod}(A_1, A)$.

Demonstração - Dado $U \in \text{Mod}(A_1, A)$, pela proposição 9.3, existem elementos $a_1, \dots, a_n$ em A_{g-1} e $b_1, \dots, b_n$ em A_g tais que

$$1 = \sum_{i=1}^n a_i b_i. \text{ Assim,}$$

$$U^g = A_{g-1} U A_g = \left(\sum_{i=1}^n a_i A_1 \right) U \left(\sum_{j=1}^n A_1 b_j \right) = \sum_{i,j=1}^n a_i A_1 U A_1 b_j = \sum_{i,j=1}^n a_i U b_j$$

Se U tem codimensão finita em $V \in \text{Mod}(A_1, A)$, então $a_i U b_j$ tem codimensão finita em $a_i V b_j, \forall i, j = 1, 2, \dots, n$, portanto U^g tem codimensão finita em V^g . $\square$

Como todo ideal bilateral em A_1 é um elemento de $\text{Mod}(A_1, A)$ e como a aplicação $U \mapsto U^g$ preserva inclusões e a

codimensão finita, podemos concluir que a família dos ideais maximais em A_1 é um subconjunto G -invariante de $\text{Mod}(A_1, A)$.

Introduzimos a seguinte definição para deixar senta da a observação anterior, que será usada posteriormente.

Definição 10.10 - Dada uma álgebra B (com unidade) sobre um corpo $\mathbb{F}$, denotaremos por $\text{Max}(B)$ a família de todos os ideais bilaterais maximais de codimensão finita em B .

Temos, então,

Corolário 10.11 - A família $\text{Max}(A_1)$ é um sub-conjunto G -invariante de $\text{Mod}(A_1, A)$. $\square$

§11- IDEMPOTENTES DE A_1

Usando a técnica de "retração" baseada num idempotente podem ser obtidos novos sistemas de Clifford e diversas correspondências entre famílias de módulos.

Consideremos, inicialmente, um idempotente e de A_1 tal que $A_1 e A_1 = A_1$

Nesse caso, eA_1e é um sub-anel de eAe e temos a seguinte proposição.

Proposição 11.1 - Seja $e \in A_1$ um idempotente tal que $A_1 e A_1 = A$.

Então, a aplicação $U \mapsto eUe = U \cap eAe$ estabelece uma bijeção entre $\text{Mod}(A_1, A)$ e $\text{Mod}(eA_1e, eAe)$. A aplicação inversa associa ao elemento $B \in \text{Mod}(eA_1e, eAe)$ o elemento A_1BA_1 . Essas aplicações preservam inclusões, intersecções, somas e produtos de módulos.

Demonstração - Dado $U \in \text{Mod}(A_1, A)$, como $eA_1e = A_1$, tem-se que $eUe \in \text{Mod}(eA_1e, eAe)$. Como $1 \in A$, temos $U = A_1UA_1$ e, portanto, $A_1(eUe)A_1 = (A_1eA_1)U(A_1eA_1) = A_1UA_1 = U$.

Dado $B \in \text{Mod}(eA_1e, eAe)$, temos $A_1BA_1 \in \text{Mod}(A_1, A)$, e como o elemento $e \in eA_1e$ é a identidade de eAe , temos $eA_1BA_1e = eA_1eBeA_1e = B$. Portanto, as duas aplicações definidas são uma a inversa da outra.

É fácil ver que essas aplicações preservam inclusões e, em consequência, também preservam intersecções e somas. Além disso, se $U, V \in \text{Mod}(A_1, A)$, então $e(UV)e = eUA_1Ve = eUA_1eA_1Ve = (eUe)(eVe)$, e, assim, preservam também produtos. $\square$

Decorrem, imediatamente, os seguintes corolários.

Corolário 11.2 - Seja e, A_1 um idempotente tal que $eA_1e = A_1$. Então, $eAe, \{eA_g e \mid g \in G\}$ é um sistema de Clifford. $\square$

Corolário 11.3 - As aplicações definidas na proposição anterior preservam as ações de G sobre $\text{Mod}(A_1, A)$ e $\text{Mod}(eA_1e, eAe)$.

Com efeito, tem-se $(eUe)^g = (eA_{g^{-1}}e) eUe (eA_g e) =$
 $= eA_{g^{-1}}A_1eA_1UA_1eA_1A_g e = eA_{g^{-1}}UA_g e, \quad \forall U \in \text{Mod}(A_1, A). \quad \square$

Proposição 11.4 - A ação de G sobre $C(A_1, A)$ deixa invariante o conjunto dos idempotentes centrais de A_1 .

Demonstração - Como $A_1^g = A_{g^{-1}}A_1A_g = A_1$, vemos que A_1 é um elemento G -invariante de $\text{Mod}(A_1, A)$ e de $C(A_1, A_1)^g = C(A_1, A_1^g) = C(A_1, A_1)$ concluímos que $C(A_1, A_1)$ é G -invariante e como G age por automorfismos sobre $C(A_1, A)$, tem-se que $e^g e^g = (ee)^g = e^g$, para todo idempotente $e \in C(A_1, A_1)$, $\forall g \in G$. $\square$

Estamos interessados em idempotentes $\underline{e}$ que satisfaçam a condição:

11.5 - $\underline{e}$ é um idempotente central de A_1 , tal que se $g \in G$, então $e^g = e$ ou $e^g e = ee^g = 0$.

Como G age por automorfismo sobre $C(A_1, A)$, o conjunto

$$G_e = \{g \in G \mid e^g = e\}$$

é um subgrupo de G , conhecido como estabilizador de $\underline{e}$ em G , e temos

Proposição 11.6 - Seja $\underline{e}$ um idempotente que satisfaz a con

dição 11.5. Então, tem-se que

$$eAe, \{eA_g = A_g e \mid g \in G_e\}$$

é um sistema de Clifford.

Demonstração - Como $ew = we^g$, $\forall g \in G$, segue-se que $eA_g = A_g e$, $\forall g \in G_e$. Dado $g \in G - G_e$, tem-se $eA_g e = A_g e^g e = \{0\}$, portanto

$$eAe = \sum_{g \in G} eA_g e = \sum_{g \in G} A_g e^g e = \sum_{g \in G_e} A_g e, \text{ e se}$$

$g, h \in G_e$, então $A_g eA_h e = A_g A_h e^h e = A_{gh} e$. Finalmente, $\underline{e}$ é a identidade bilateral de $eA_1 = A_1 e$. $\square$

Queremos estudar o caso em que vale $AeA = A$. Temos a seguinte proposição.

Proposição 11.7- Seja $\underline{e}$ um idempotente satisfazendo a condição 11.5. Então, $eAe = A$ se, e somente se, as seguintes condições estiverem satisfeitas:

a) a G -órbita E de $\underline{e}$ é finita,

b) $1 = \sum_{f \in E} f$.

Demonstração - Suponhamos que $AeA = A$. Se $e = 0$, então $A = \{0\}$ e $1 = 0$, portanto valem a) e b).

Assumamos que $e \neq 0$. Temos

$$A = AeA = \sum_{g,h \in G} A_g e A_h$$

e existe um subconjunto finito $T \subset G$ tal que

$$1 \in \sum_{g,h \in T} A_g e A_h$$

Seja $F = \{e^g \mid g \in T\}$, então dois idempotentes de F são iguais ou ortogonais e o elemento $a = \sum_{f \in F} f$ é um idempotente e temos $Aa = \sum_{f \in F} Af$. Assim,

$$1 \in \sum_{g,h \in T} A_g e A_h = \sum_{g,h \in T} A_g A_h e^h \quad \sum_{f \in F} Af = Aa$$

Portanto $1 = 1a = a$. Se $e^g \in E-F$, para algum $g \in G$, então, por 11.5, $0 = e^g a = e^g 1 = e^g$, logo $e = 0$, contra o suposto. Assim, $E-F$ é vazio, isto é, a G -órbita E de e é o conjunto finito F . Além disso, $1 = a = \sum_{f \in F} f = \sum_{f \in E} f$.

Reciprocamente, suponhamos que vale a) e b). Então, como vimos na demonstração do Lema 10.4,

$$e^g = \sum_{i=1}^n a_i e b_i \in A_{g^{-1}} e A_g \subset AeA, \quad \forall g \in G$$

portanto $1 = \sum_{f \in E} f \in AeA$, e temos que $AeA = A$. $\square$

Corolário 11.8 - Se as condições 11.5 e a) e b) da proposição anterior estiverem satisfeitas, a correspondência $L \mapsto eLe = L \cap eAe$ estabelece uma bijeção entre o conjunto $\text{Mod}(A, A)$ dos ideais bilaterais de A e $\text{Mod}(eAe, eAe)$. A aplicação inversa associa ao elemento $H \in \text{Mod}(eAe, eAe)$ o elemento AHA . Essas aplicações preservam inclusões, intersecções, somas e produtos de ideais.

Demonstração - Pela proposição anterior o elemento e satisfaz a condição $A_1 e A_1 = A_1$ relativamente ao sistema de Clifford trivial $A, \{A_g \mid g \in \{1\}\}$. Portanto, pela proposição 11.1, temos a tese. $\square$

Corolário 11.9 - Com as mesmas hipóteses do corolário anterior, as aplicações

$$L \mapsto eLe \quad \text{e} \quad H \mapsto AHA$$

preservam a codimensão finita de módulos e estabelecem uma bijeção entre $\text{Max}(\Lambda)$ e $\text{Max}(eAe)$.

Demonstração - Pelo corolário anterior, os ideais máxi-
mais de A se correspondem com os maximais de eAe . Por ou-
tro lado, é claro que se $U \in \text{Mod}(A_1, A)$ tem codimensão fini-
ta em $V \in \text{Mod}(A_1, A)$, então eUe tem codimensão finita em eVe .

Reciprocamente, pela Prop. 9.3, existem elementos
 $c_1, \dots, c_n, d_1, \dots, d_n$ em A_1 tais que $1 = \sum_{i=1}^n c_i e d_i$, e en-
tão dado $u \in U \in \text{Mod}(A_1, A)$, tem-se que

$$u = 1u1 = \sum_{i,j=1}^n c_i e d_i u c_j e d_j \in \sum_{i,j=1}^n c_i e U e d_j$$

e, em consequência, $U = \sum_{i,j=1}^n c_i e U e d_j$. Assim,

se $U, V \in \text{Mod}(A_1, A)$ e eUe tem codimensão finita em eVe , en-
tão $c_i e U e d_j$ tem codimensão finita em $c_i e V e d_j$, $\forall i, j=1, 2, \dots, n$,
portanto U tem codimensão finita em V . $\square$

§12- SUB-ÁLGEBRAS CENTRAIS SIMPLES DE A

Seja $A, \{A_g | g \in G\}$ um sistema de Clifford. Estamos
interessados em sub-álgebras D satisfazendo as seguintes con-
dições:

- (12.1) a) D é uma sub-álgebra de A_1 ,
b) D é uma álgebra central simples de dimensão fi

nita sobre $\mathbb{F}$,

c) D contém a identidade 1 de A .

Para tal sub-álgebra temos o conhecido

Lema 12.2 - Se $U \in \text{Mod}(D, A)$ então a aplicação linear canônica que manda $c \otimes d$ em $cd = dc$, $c \in C(D, U)$, $d \in D$, é um isomorfismo de $C(D, U) \otimes_{\mathbb{F}} D$ sobre U , e, em consequência, $U = C(D, U)D$.

Demonstração - Seja D^* a álgebra oposta de D , com a mesma adição de D e o produto $d^*d' = dd'$. Consideremos U como um $D \otimes_{\mathbb{F}} D^*$ - módulo com a multiplicação por escalares definida por $(d \otimes d')a = dad^*$, $d \in D$, $a \in U$, $d^* \in D^*$. Então $\text{Mod}(D, A)$ é o conjunto dos $D \otimes_{\mathbb{F}} D^*$ - submódulos de A .

Pela Proposição 1.15, as condições 12.1 acarretam que $D \otimes_{\mathbb{F}} D^*$ é uma álgebra central simples de dimensão finita sobre $\mathbb{F}$, em consequência U é um $D \otimes_{\mathbb{F}} D^*$ - módulo semi-simples, portanto $U = \bigoplus_{\alpha \in I} B_{\alpha}$, onde cada B_{α} é isomorfo ao $D \otimes_{\mathbb{F}} D^*$ - módulo irredutível D . Como $C(D, U) = \bigoplus_{\alpha \in I} C(D, B_{\alpha})$, pela distributividade do produto tensorial em relação à soma direta, o lema vale para U se for verdadeiro para cada B_{α} , isto é, se for verdadeiro para D . Mas $C(D, D) = \mathbb{F}$, pois D é central e o isomorfismo $\mathbb{F} \otimes_{\mathbb{F}} D \rightarrow D$ é dado precisamente pela aplicação $f \otimes d \rightarrow fd$. Assim, o lema vale para D , portan

to vale no caso geral. $\square$

Corolário 12.3 - Se $U \in \text{Mod}(A_1, A)$, então

$$C(A_1, U) = C(C(D, A_1), C(D, U))$$

Demonstração - Como $A_1 \in \text{Mod}(D, A)$, pelo lema anterior $A_1 = C(D, A_1)D$, e a igualdade $C(C(D, A_1)D, U) = C(C(D, A_1), C(D, U))$ é imediata. $\square$

Proposição 12.4 - A aplicação $U \mapsto C(D, U)$ estabelece uma bijeção entre $\text{Mod}(D, A)$ e o conjunto de todos os $\mathbb{F}$ -sub-espços de $C(D, A)$. A aplicação inversa associa um $\mathbb{F}$ -sub-espço $B \subset C(D, A)$ com $BD = DB$. Estas aplicações preservam inclusões, intersecções, somas, produtos e codimensão finita de módulos.

Demonstração - Se $U \in \text{Mod}(D, A)$, então $C(D, U)$ é um $\mathbb{F}$ -sub-espço de $C(D, A)$ e, pelo lema anterior, $U = C(D, U)D$. Se B é um $\mathbb{F}$ -sub-espço de $C(D, A)$, então $BD = DB \text{ Mod}(D, A)$, portanto $C(D, BD)$ é um $\mathbb{F}$ -sub-espço de $C(D, A)$. É claro que $B \subset C(D, BD)$, e que a imagem do sub-espço $B \otimes_{\mathbb{F}} D$ pelo isomorfismo $C(D, BD) \otimes_{\mathbb{F}} D \rightarrow BD$ é BD e da exatidão da sequência $B \otimes_{\mathbb{F}} D \xrightarrow{i \times \text{id}} C(D, BD) \otimes_{\mathbb{F}} D \twoheadrightarrow (C(D, BD)/B) \otimes_{\mathbb{F}} D$ decorre que $0 = (C(D, BD)/B) \otimes_{\mathbb{F}} D$, donde $C(D, BD)/B = 0$, e

portanto $B = C(D, BD)$.

Assim, as duas aplicações são inversas uma da outra e é fácil ver que preservam inclusões, intersecções e somas. Se B e E são F -sub-espacos de $C(D, A)$, então $(BE)D = BED^2 = (BD)(ED)$ e portanto, o produto de módulos também é preservado. Finalmente, é fácil ver que a aplicação $U \mapsto C(D, U) = U \cap C(D, A)$ preserva a codimensão finita de módulos da mesma maneira que, pelo fato de ser D de dimensão finita, a aplicação $B \mapsto BD$. $\square$

Corolário 12.5 - Se $A, \{A_g | g \in G\}$ é um sistema de Clifford (resp., G -graduado), então

$$C(D, A), \{C(D, A_g) | g \in G\}$$

é um sistema de Clifford (resp., G -graduado).

Demonstração - É claro que $C(D, A)$ é uma F -sub-álgebra de A . Como $A_g \in \text{Mod}(D, A)$, $\forall g \in G$, então $C(D, A_g)$ é um F -sub-espaco de $C(D, A)$ e as condições a) e b) da definição de sistema de Clifford decorrem do fato de que as aplicações definidas na proposição anterior preservam somas, produtos e intersecções e como 1 é a identidade bilateral de $C(D, A_1)$, o corolário está provado. $\square$

Corolário 12.6 - A aplicação $U \mapsto C(D, U)$ estabelece uma bije

ção entre $\text{Mod}(A_1, A)$ e $\text{Mod}(C(D, A_1), C(D, A))$. A inversa manda B em $BD = BA_1 = A_1B$. Essas aplicações preservam inclusões, intersecções, somas, produtos, codimensão finita e ações de G .

Demonstração - Dado $B \in (C(D, A_1), C(D, A))$, tem-se

$BA_1 = BC(D, A_1)D = BD$, pelo lema 12.2. Analogamente, $A_1B = DB = BD$. O resto do corolário segue da proposição anterior, do fato de que D é uma sub-álgebra de A_1 e da Proposição 10.2. $\square$

§ 13 - A_1 -CONSTITUINTES

A teoria de Clifford desenvolvida em [2] começa com demonstração de que a restrição a um subgrupo normal N , de um grupo H de uma representação irredutível de H , de dimensão finita sobre um corpo F , é completamente redutível e que suas distintas constituintes irredutíveis formam uma H -órbita de F -representações irredutíveis de N . Provaremos o resultado correspondente para sistemas de Clifford.

Proposição 13.1 - $A, \{A_g | g \in G\}$ um sistema de Clifford e seja M um elemento de $\text{Max}(A)$, o conjunto dos ideais bilaterais maximais de codimensão finita em A . Então, $A_1/(A_1 \cap M)$ é uma álgebra semi-simples de dimensão finita sobre F .

Demonstração - Usando a Proposição 1.4, temos que $\bar{A} = A/M$, $\{(A_g + M)/M ; g \in G\}$ é um sistema de Clifford e sendo $M \in \text{Max}(A)$, A/M é simples e de dimensão finita sobre $\mathbb{F}$. Como

$$\bar{A}_1 = A_1 / (A_1 \cap M) \simeq (A_1 + M) / M = A/M$$

temos que $\bar{A}_1$ é de dimensão finita sobre $\mathbb{F}$ e, assim, o seu radical R_1 é nilpotente, isto é, $R_1^n = \{0\}$, para algum inteiro positivo n . Dado $g \in G$, $R_1^g \subset \bar{A}_1^g = \bar{A}_1$ é um ideal de $\bar{A}_1$ tal que $(R_1^g)^n = (R_1^n)^g = \{0\}$, portanto é um ideal nilpotente de $\bar{A}_1$ e temos $R^g \subset R_1$, $\forall g \in G$. Disto decorre, usando a Proposição 10.3 que $R_1 \bar{A} = \bar{A} R_1$ é um ideal bilateral de $\bar{A}$, assim $(R_1 A)^n = R_1 \bar{A}^n = \{0\}$ e como $\bar{A}$ é simples concluímos que $R_1 \bar{A} = \{0\}$. Logo $R_1 = \{0\}$ e $\bar{A}_1$ é semi-simples. $\square$

Definição 13.3 - Dado um ideal $M \in \text{Max}(A)$, chamaremos de A_1 -constituente de M a todo ideal $N \in \text{Max}(A_1)$ tal que $M \cap A_1 \subset N$.

Estabeleceremos agora o resultado procurado na introdução do parágrafo.

Proposição 13.4 - Os A_1 -constituíntes de um ideal $M \in \text{Max}(A)$ formam uma G -órbita finita $N_1, \dots, N_t$ em $\text{Max}(A_1)$ satisfazendo $N_1 \cap \dots \cap N_t = M \cap A_1$.

Demonstração - Pela proposição anterior, $A_1 / (A_1 \cap M)$ é uma álgebra semi-simples de dimensão finita, portanto M tem um número finito de A_1 -constituíntes $N_1, \dots, N_t$ e que verifi-

com $N_1 \cap \dots \cap N_t = A_1 \cap M$. Como M é um ideal de A , $M^g = A^{-1}_g M A_g \subset M$, $\forall g \in G$, portanto M é G -invariante, pela Proposição 10.3.

Também A_1 , $A_1 \cap M$ e $\text{Max}(A_1)$ são G -invariantes, portanto o conjunto $\{N_1, \dots, N_t\}$ é G -invariante.

Suponhamos agora que $\{N_1, \dots, N_t\}$ não seja uma G -órbita. Então esse conjunto contém um subconjunto próprio G -invariante, digamos $\{N_1, \dots, N_s\}$, com $1 \leq s \leq t-1$. Os ideais $N_1 \cap \dots \cap N_s$ e $N_{s+1} \cap \dots \cap N_t$ são ambos G -invariantes, portanto $A(N_1 \cap \dots \cap N_s)$ e $(N_{s+1} \cap \dots \cap N_t)A$ são, pela Proposição 10.3, ideais bilaterais de A , mas

$$[A(N_1 \cap \dots \cap N_s)] [(N_{s+1} \cap \dots \cap N_t)A] \subset A(N_1 \cap \dots \cap N_t)A = A(M \cap A_1)A \subset M$$

e como M é um ideal maximal de A , M contém um dos ideais $A(N_1 \cap \dots \cap N_s)$ ou $(N_{s+1} \cap \dots \cap N_t)A$, e portanto $A_1 \cap M$ contém $N_1 \cap \dots \cap N_s$ ou $N_{s+1} \cap \dots \cap N_t$, e em consequência $A_1 \cap M$ coincide com um desses dois ideais, o que contradiz, pela semi-simplicidade da álgebra $A_1/(A_1 \cap M)$, a irredundância das t A_1 -constituintes. Assim, $\{N_1, \dots, N_t\}$ é uma G -órbita. $\square$

Definição 13.4 - Dado $N \in \text{Max}(A_1)$, definimos $\text{Max}(A|N)$ como sendo o conjunto de todos os $M \in \text{Max}(A)$ que tem N como A_1 -constituinte. Chamaremos de $\underline{B}(N)$ o ideal bilateral $A(\bigcap_{g \in G} N^g) =$

$= (\bigcap_{g \in G} N^g)A$ de A e denotaremos por $\text{Max}^*(A_1)$ o conjunto de todos os $N \in \text{Max}(A_1)$ tais que $B(N) \neq A$ e $\text{Orb}(N)$, a G -órbita de N em $\text{Max}(A_1)$, é finita.

Temos a seguinte proposição.

Proposição 13.5 - Se $N \in \text{Max}(A_1) - \text{Max}^*(A_1)$, então $\text{Max}(A|N)$ é vazio. Se $N \in \text{Max}^*(A_1)$, então $B(N) \cap A_1 = \bigcap_{g \in G} N^g \subset N \subsetneq A_1$; nessas condições, $\text{Max}(A|N)$ consiste dos $M \in \text{Max}(A)$ tais que $M \supset B(N)$.

Demonstração - Sejam $N \in \text{Max}(A_1)$ e $M \in \text{Max}(A|N)$, pela proposição anterior a G -órbita de N em $\text{Max}(A_1)$ é finita e temos $B(N) = A(M \cap A_1) \subsetneq M \subsetneq A$, portanto $N \in \text{Max}^*(A_1)$, o que prova a primeira asserção.

Assumamos agora que $N \in \text{Max}^*(A_1)$. Como $\text{Orb}(N)$ é finita todo ideal bilateral J de A_1 que contém $\bigcap_{g \in G} N^g$ é da forma $\bigcap_{L \in S} L$, com $S \subset \text{Orb}(N)$. Além disto $J^g = \bigcap_{L \in Sg} L$, $\forall g \in G$, e concluímos que se $N \in \text{Max}^*(A_1)$, então os únicos ideais bilaterais G -invariantes de A_1 que contém $\bigcap_{g \in G} N^g$ são ele próprio e A_1 .

Como $B(N)$ é um ideal bilateral G -invariante de A que não contém o 1, temos que $B(N) \cap A_1$ é um ideal bilateral de A_1 , distinto de A_1 , que contém $\bigcap_{g \in G} N^g$, portanto coincide com ele.

Finalmente, se $M \in \text{Max}(A|N)$, vimos acima que $B(N) \subset M$. Reciprocamente, se $M \in \text{Max}(A)$ e $B(N) \subset M$, então $\bigcap_{g \in G} N^g = B(N) \cap A_1 \subset M \cap A_1 \neq A_1$, pois $1 \notin M$, e como M é G -invariante, $M \cap A_1 = \bigcap_{g \in G} N^g \subset N$, portanto $M \in \text{Max}(A|N)$. $\square$

§14 - A CORRESPONDÊNCIA DE CLIFFORD

Sejam $A, \{A_g | g \in G\}$ um sistema de Clifford sobre um corpo F algebricamente fechado e N um ideal em $\text{Max}^*(A_1)$. Usaremos barras para denotar as imagens de objetos na álgebra quociente $\bar{A} = A / B(N)$ pelo homomorfismo canônico. Assim, temos um isomorfismo natural entre $A_1 / B(N) \cap A_1$ e $\bar{A}_1$ das proposições 9.4, e 13.5 decorre que

$\bar{A}, \{\bar{A}_g | g \in G\}$ é um sistema de Clifford sobre F ;

(14.1) $\bar{A}_1$ é uma álgebra semi-simples de dimensão finita sobre F , e

$L \mapsto \bar{L}$ estabelece uma bijeção, G -invariante, entre $\text{Orb}(N)$ e $\text{Max}(\bar{A}_1)$.

Em consequência, existe uma bijeção $L \mapsto e(L)$ entre $\text{Orb}(N)$ e o conjunto E dos idempotentes centrais primitivos de $\bar{A}_1$ tal que $\bar{L} = (\bar{1} - e(L)) \bar{A}_1$, $\forall L \in \text{Orb}(N)$. Essa aplicação é G -invariante por 10.7. Em particular, $G_{e(N)}$ é o normalizador $N_G(N)$ de N em G .

Temos o seguinte lema.

Lema 14.2 - O idempotente $e = e(N)$ satisfaz as condições 11.5 no sistema $\bar{A}, \{\bar{A}_g | g \in G\}$, isto é, $\underline{e}$ é um idempotente central de $\bar{A}_1$, e se $g \in G$, então $e^g = e$ ou $e^g e = e e^g = 0$. Além disso, a G -órbita E de $\underline{e}$ é finita e $\bar{l} = \sum_{f \in E} f$.

Demonstração - A G -órbita de $\underline{e}$ é o conjunto E dos idempotentes centrais primitivos de $\bar{A}_1$, portanto $\underline{e}$ satisfaz as condições 11.5. Como $\bar{A}_1$ é uma álgebra semi-simples de dimensão finita sobre $\mathbb{F}$, temos que E é finito e que $\bar{l} = \sum_{f \in E} f$. $\square$

Definição 14.3 - Seja $e = e(N)$. Definimos $A < N > = C(e\bar{A}_1, e\bar{A}e)$, e $A < N >_g = C(e\bar{A}_1, e\bar{A}_g)$, $\forall g \in G_e$.

Temos então, a seguinte proposição.

Proposição 14.4 - $A < N >, \{A < N >_g; g \in G_e\}$ é um sistema de Clifford sobre $\mathbb{F}$ no qual $A < N >_1 = \mathbb{F}e$ é unidimensional.

Demonstração - Pelo lema anterior, $\underline{e}$ satisfaz 11.5, e pela Proposição 11.6, temos que $A < N >, \{A < N >_g; g \in G_e\}$ é um sistema de Clifford sobre $\mathbb{F}$.

Por outro lado, como $\underline{e}$ é um idempotente central primitivo da álgebra semi-simples de dimensão finita $\bar{A}_1$, temos que $e\bar{A}_1$ é uma álgebra simples de dimensão finita so-

bre o corpo $\mathbb{F}$ algebricamente fechado, logo $e\bar{A}_1$ é central. Assim, $D = e\bar{A}_1$ é uma sub-álgebra que satisfaz as condições 12.1 em relação ao sistema $eAe, \{eA_g; g \in G_e\}$ e portanto, por 12.5, temos a tese. $\square$

Definição 14.5 - Dado $M \in M(A|N)$, (veja Definição .4), definimos $M \langle N \rangle = A \langle N \rangle \bar{M} = C(e\bar{A}_1, e\bar{M}e)$.

A correspondência básica de Clifford é dada pela seguinte proposição.

Proposição 14.6 - A aplicação $M \mapsto M \langle N \rangle$ estabelece uma bijeção entre $\text{Max}(A|N)$ e $\text{Max}(A \langle N \rangle)$. A aplicação inversa associa ao elemento $L \in \text{Max}(A \langle N \rangle)$ a imagem inversa de $\bar{A} L \bar{A} \in \text{Max}(\bar{A})$ em A .

Demonstração - A tese decorre das considerações que faremos sobre cada uma das aplicações seguintes:

$\text{Max}(A|N) \rightarrow \text{Max}(\bar{A}) \rightarrow \text{Max}(e\bar{A}e) \rightarrow \text{Max}(A \langle N \rangle)$, dadas por

$$M \mapsto \bar{M} \mapsto \bar{M} \cap e\bar{A}e \mapsto \bar{M} \cap e\bar{A}e \cap A \langle N \rangle = M \langle N \rangle,$$

e da descrição de suas inversas.

A primeira delas estabelece uma bijeção entre $\text{Max}(A|N)$ e $\text{Max}(\bar{A})$, pela Proposição 13.5 onde $\bar{A} = A/B(N)$. A sua inversa associa a $L \in \text{Max}(\bar{A})$ a sua imagem inversa, pela

projeção canônica, em A .

Na segunda, pelo Lema 14.2, $\underline{e}$ é um idempotente de $\bar{A}$ que satisfaz as condições 11.5 e, usando o corolário

11.9, obtemos uma correspondência bijetora entre $\text{Max}(\bar{A})$ e $\text{Max}(e\bar{A}e)$, dada por $\bar{M} \rightarrow \bar{M} \cap e\bar{A}e = e\bar{M}e$, cuja inversa manda $L \in \text{Max}(e\bar{A}e)$ em $\bar{A} \cap L \bar{A}$

Como vimos na Proposição 14.4, a sub-álgebra $D = e\bar{A}_1$ satisfaz as condições 12.1 em relação ao sistema $e\bar{A}e$, $\{e\bar{A}_1; g \in G_e\}$. Do corolário 12.6, concluimos que a aplicação

$$e\bar{M}e \rightarrow C(e\bar{A}_1, e\bar{M}e) = e\bar{M}e \cap A < N >,$$

estabelece uma bijeção entre $\text{Max}(e\bar{A}e)$ e $\text{Max}(A < N >)$, cuja inversa manda $L \in \text{Max}(A < N >)$ em

$$(e\bar{A}_1)L = (e\bar{A}_1)L(e\bar{A}_1) = [(e\bar{A}_1)A < N > (e\bar{A}_1)]L[A < N > (e\bar{A}_1)] = (e\bar{A}e)L(e\bar{A}e). \quad \square$$

§ 15 - A_1 UNIDIMENSIONAIS

Seja $A, \{A_g | g \in G\}$ um sistema de Clifford G -graduado sobre um corpo F tal que A_1 é de dimensão 1 sobre F . Então tem-se:

Lema 15.1 - Cada $A_g, g \in G$, é de dimensão 1 sobre F .

Demonstração - Como $A_{g^{-1}} A_g = A_1 \neq 0$, existem elementos

$c \in A_{g^{-1}}$ e $d \in A_g$ tais que $cd \neq 0$. Sendo $\dim_{\mathbb{F}} A_1 = 1$, existe $f \in \mathbb{F}$ tal que $fcd = 1$. Tomando $n = 1$, $a_1 = fc$ e $b = d$ eles satisfazem a Proposição 9.3 pois:

a) se $y \in A_g$, então $y f c \in A_g A_{g^{-1}} = A_1$, logo

$$y = y.1 = y(f c d) = (y f c) d \in A_1 d, \text{ e}$$

b) $A_1 A_g = A_g$, logo $A_1 d \subset A_g$. $\square$

Identificamos $\mathbb{F}$ com A_1 pelo isomorfismo $f \in \mathbb{F} \mapsto f.1$, e $A_1 - \{0\}$ com o grupo multiplicativo $F = \mathbb{F} - \{0\}$ de $\mathbb{F}$.

Seja $G^* = \bigcup_{g \in G} (A_g - \{0\})$. Como $A = \bigoplus_{g \in G} A_g$, a reunião que define G^* é disjunta, e assim existe uma única função $\text{pr} : G^* \rightarrow G$ tal que $\text{pr}^{-1}(g) = A_g - \{0\}$, $\forall g \in G$.

O conjunto G^* e a função pr satisfazem a seguinte proposição:

Proposição 15.2 - G^* é um subgrupo do grupo das unidades da álgebra A e a função pr é um epimorfismo cujo núcleo é o subgrupo central F de G^* .

Demonstração - Pelo lema anterior, $A_g \neq \{0\}$, $\forall g \in G$, e assim pr manda G^* sobre G .

Suponhamos que $g, h \in G$, $a \in A_g - \{0\}$ e $b \in A_h - \{0\}$.

Pelo mesmo lema, $A_g = \mathbb{F}a$ e $A_h = \mathbb{F}b$,

logo $A_{gh} = \mathbb{F}ab$, e como $A_{gh} \neq \{0\}$, $ab \in A_{ab} - \{0\}$, portanto G^* é um subconjunto de A fechado em relação à multiplicação e pr é um epimorfismo do semigrupo G^* sobre G .

O núcleo de pr é o subgrupo F de G^* e como $\text{pr}(G^*) = G$ é um grupo e F contém a identidade 1 de G^* , isto implica que G^* é um grupo, pois se $m \in G^*$, existe $g \in G$ tal que $m \in A_g - \{0\}$ e como $A_g A_{g^{-1}} = A_1$, existem $u \in A_g$ e $v \in A_{g^{-1}}$ tais que $uv = 1$, portanto $A_g = \mathbb{F}u$ e $A_{g^{-1}} = \mathbb{F}v$, logo $m = fu$, com $f \in F$, donde $m(f^{-1}v) = (fu)(f^{-1}v) = uv = 1$, com $f^{-1}v \in A_{g^{-1}} - \{0\} \subset G^*$, em consequência G^* é um grupo contido no grupo das unidades de A .

Finalmente, F é central em G^* pois A é uma álgebra sobre F . $\square$

Seja $\mathbb{F}$ um corpo e F o seu grupo multiplicativo. Suponhamos, agora, que temos uma extensão arbitrária de F por um grupo G , $F \twoheadrightarrow G^* \xrightarrow{\text{pr}} G$. Queremos construir um sistema de Clifford G -graduado $\mathbb{F}[G^*]$, $\{\mathbb{F}[G^*]_g; g \in G\}$ sobre $\mathbb{F}$, tal que $\mathbb{F}[G^*]_1$ seja unidimensional e do qual a extensão G^* possa ser recuperada da maneira exposta no comentário anterior à Proposição 12.2.

Podemos assumir que o elemento 0 de $\mathbb{F}$ não está em G^* e definimos

$$\mathbb{F}[G^*]_g = \text{pr}^{-1}(g) \cup \{0\}, \quad \forall g \in G.$$

Denotemos, provisoriamente, o produto em $\mathbb{F}[G^*]_g$

por $y.z$ para distingui-lo do produto yz quando $y, z \in G^*$.
Produtos e somas de elementos homogêneos são definidos por

$$\begin{aligned} 0.0 &= y.0 = 0.z = 0 \\ y.z &= yz, \text{ para } y \in \text{pr}^{-1}(g), z \in \text{pr}^{-1}(h), \quad g, h \in G, \\ y+fy &= (1+f)y, \text{ para } f \in \mathbb{F}, y \in \text{pr}^{-1}(g), g \in G, \text{ onde} \\ &1+f \text{ é tomado em } \mathbb{F}[G^*]_1 = \mathbb{F}. \end{aligned}$$

Verifica-se que as operações assim definidas coincidem com as do corpo $\mathbb{F}$ sobre o conjunto $\text{pr}^{-1}(1) \cup \{0\} = F \cup \{0\}$. Além do mais, elas tornam cada $\mathbb{F}[G^*]_g$ um $\mathbb{F}$ -espaço vetorial de dimensão 1.

Dados $y, z \in \text{pr}^{-1}(g)$, então $\text{pr}(zy^{-1}) = 1$, em consequência existe $w \in F \setminus G^*$ tal que $z = wy$, logo todos os elementos de $\text{pr}^{-1}(g)$ são gerados por y , como $\mathbb{F}$ -espaço vetorial. Por isto, só são definidas somas do tipo $y+fy = (1+f)y$, e $\mathbb{F}[G^*]_g$ é fechado, portanto, em relação a esta adição e é fácil ver que também é fechado em relação à multiplicação por elementos de $\mathbb{F}$. Vale também $fy+f'y = (f+f').y$ o que decorre do fato de que se $fy, f'y \in \text{pr}^{-1}(g)$, então $f = wf'$, para algum $w \in F$, portanto $fy+f'y = wf'y+f'y = (w+1).f'y = [(w+1)f']y = (f+f').y$.

Finalmente, a multiplicação é uma aplicação $\mathbb{F}$ -bilinear

$$\mathbb{F}[G^*]_g \times \mathbb{F}[G^*]_h \rightarrow \mathbb{F}[G^*]_{gh}, \quad \forall g, h \in G,$$

que é associativa de $\mathbb{F}[G^*]_g \times \mathbb{F}[G^*]_h \rightarrow \mathbb{F}[G^*]_i$ em $\mathbb{F}[G^*]_{ghi}$, $\forall g, h, i \in G$.

Definimos $\mathbb{F}[G^*]$ como sendo a soma direta externa de espaços vetoriais $\mathbb{F}[G^*] = \bigoplus_{g \in G} \mathbb{F}[G^*]_g$, e identificamos cada $\mathbb{F}[G^*]_g$ com a sua imagem canônica em $\mathbb{F}[G^*]$. Estendemos a multiplicação a $\mathbb{F}[G^*]$ por bilinearidade. Fica assim demonstrado o seguinte teorema:

Teorema 15.3 - Sejam $\mathbb{F}$ um corpo, F o seu grupo multiplicativo e $F \xrightarrow{\text{pr}} G^* \rightarrow G$ uma extensão central de F por um grupo G . Então, $\mathbb{F}[G^*], \{\mathbb{F}[G^*]_g; g \in G\}$ é um sistema de Clifford G -graduado sobre $\mathbb{F}$, tal que $\mathbb{F}[G^*]_1$ é unidimensional e na qual $G^* = \bigcup_{g \in G} \mathbb{F}[G^*]_g - \{0\}$ e $\text{pr}^{-1}(g) = \mathbb{F}[G^*]_g - \{0\}$. Reciprocamente, se $A, \{A_g; g \in G\}$ é um sistema de Clifford sobre $\mathbb{F}$, tal que A_1 é unidimensional e G^* é a extensão central de F por G construída pelo método indicado no início do parágrafo, então $A, \{A_g; g \in G\}$ é idêntico a $\mathbb{F}[G^*], \{\mathbb{F}[G^*]_g; g \in G\}$, identificando a soma direta interna de A com a soma direta externa que define $\mathbb{F}[G^*]$.

Assim, sistemas de Clifford G -graduados sobre $\mathbb{F}$ com A_1 unidimensional e extensões centrais de F por G são equivalentes.

Suponha, agora, que λ é um caráter linear de $\mathbb{F}[G^*]$, isto é, um homomorfismo (de álgebras) $\lambda: \mathbb{F}[G^*] \rightarrow \mathbb{F}$ cuja res-

trição a $\mathbb{F} = \mathbb{F}e$, com $e = e(\lambda)$, $\tilde{e} = \text{id}_{\mathbb{F}}$, então

$$\mathbb{F}[G^*] \cong \mathbb{F} \times \ker \lambda.$$

Assim, $\ker \lambda$ determina λ como a projeção sobre o fator $\mathbb{F}$ nesse produto direto e a aplicação

$$\lambda \longleftrightarrow \ker \lambda$$

é uma correspondência bijetora entre caracteres lineares de $\mathbb{F}[G^*]$ e subgrupos $\ker \lambda$ complementares a $\mathbb{F}$ em G^* . Temos, assim, o seguinte corolário.

Corolário 15.4 - A extensão $\mathbb{F} \twoheadrightarrow G^* \twoheadrightarrow G$ é cindida se, e somente se, existe um caráter linear λ definido sobre $\mathbb{F}[G^*]$ tal que $\mathbb{F}[G^*] \cong \mathbb{F} \times \ker \lambda$. $\square$

O Teorema 15.3 nos permite introduzir a seguinte definição, que usaremos no Capítulo II.

Definição 15.5 - Sejam $\mathbb{F} \twoheadrightarrow G_1^* \twoheadrightarrow G$ e $\mathbb{F} \twoheadrightarrow G_2^* \twoheadrightarrow G$, duas extensões centrais de $\mathbb{F}$ por G . O produto central $G_1^* \vee G_2^*$ com $\mathbb{F}$ amalgamado é a extensão central de $\mathbb{F}$ por $G \times G$ determinada pelas condições:

$$\mathbb{F}[G_1^* \vee G_2^*] = \mathbb{F}[G_1^*] \otimes_{\mathbb{F}} \mathbb{F}[G_2^*], \quad e$$

$$\mathbb{F}[G_1^* \vee G_2^*]_{g \times h} = \mathbb{F}[G_1^*]_g \otimes_{\mathbb{F}} \mathbb{F}[G_2^*]_h, \quad \forall g, h \in G.$$

CAPÍTULO II

CARACTERES E EXTENSÕES DE CLIFFORD

§ 16 - EXTENSÃO DE CLIFFORD CORRESPONDENTE A UM CARÁTER.

Sejam H e G grupos finitos, $\eta: H \rightarrow G$ um epimorfismo, $N = \ker \eta$, χ um $\mathbb{C}$ -caráter complexo irredutível H -invariante de N e $\mathbb{K}$ um subcorpo de $\mathbb{C}$ que contém todos os valores $\chi(h)$, $h \in N$.

Seja $e = e(\chi) = \frac{\chi(1)}{|N|} \sum_{g \in N} \chi(g^{-1})g$ o idempotente cen-

tral primitivo da álgebra de grupo $\mathbb{K}N$ correspondente ao caráter χ . Sendo e central temos $e\mathbb{K}N = \mathbb{K}Ne$ e por ser e primitivo $e\mathbb{K}N$ é uma álgebra simples somando direto de $\mathbb{K}N$:

$$\mathbb{K}N = \mathbb{K}Ne \oplus \mathbb{K}N(1-e).$$

Como $\mathbb{K} \supset \{\chi(h) \mid h \in N\}$, pelo Lema 2.6 ,

temos que $e\mathbb{K}N$ é uma álgebra central simples.

O idempotente e é também central em $\mathbb{K}H$ pois χ é H -invariante. Basta observar que

$$\begin{aligned} \sum_{g \in N} \chi(g^{-1})gh &= \sum_{g \in N} \chi(h^{-1}g^{-1}h)h(h^{-1}gh) = h \sum_{g \in N} \chi(h^{-1}g^{-1}h)h^{-1}gh \\ &= h \sum_{g \in N} \chi(g^{-1})g, \quad \forall h \in H, \text{ donde decorre que } eh = he, \quad \forall h \in H. \end{aligned}$$

Sendo e central em $\mathbb{K}H$, $e\mathbb{K}H = \mathbb{K}He$ é um somando direto (como álgebra) de $\mathbb{K}H$:

$$\mathbb{K}H = \mathbb{K}He \oplus \mathbb{K}H(1-e).$$

A extensão de Clifford $H\langle\chi\rangle$ de K por G ,

$$K \rightarrow H\langle\chi\rangle \xrightarrow{\text{pr}} G$$

será obtida pela aplicação do Teorema 15.3, dando a sua álgebra de grupo "twisted" $A = \mathbb{K}[H\langle\chi\rangle]$ sobre $\mathbb{K}$ (vide a observação 4.3), junto com a G -graduação dessa álgebra formada pelos sub-espacos unidimensionais $\mathbb{K}[H\langle\chi\rangle]_g$ cujos elementos não nulos formam a imagem inversa em $H\langle\chi\rangle$ dos elementos g de G .

Como vimos no exemplo 1, da pagina 19, tomando $A = \mathbb{K}H$, $N = \ker \eta$ e A_g como sendo o $\mathbb{K}$ -espaço vetorial gerado por $\{x \mid x \in Ng\}$, $g \in H$, obtemos um sistema de Clifford $A, \{A_g \mid g \in G\}$.

Como o idempotente $e = e(\chi)$ verifica a condição 11.5, temos pela Proposição 12.6, que, com $G_e = G$,

$$e\mathbb{K}H, \{(e\mathbb{K}H)_g \mid g \in G_e\}$$

é um sistema de Clifford, e aplicando o Corolário 12.5 para

$D=eKN$, temos que

$$C(eKN, eKH), \{C(eKN, (eKH)_g) \mid g \in G\}$$

é um sistema de Clifford G -gradação no qual

$A_1=C(eKN, (eKH)_1)=C(eKN, eKN)$ é $\mathbb{K}$ -unidimensional por ser eKN uma álgebra central.

Pelo teorema 15.3, podemos tomar $\mathbb{K}[\langle \chi \rangle]$ como sendo $C(eKN, eKH)$. Decorre do Lema 12.2, tomando $U=eKH$ e $D=eKN$, que

$$eKH=eKN \otimes_{\mathbb{K}} \mathbb{K}[\langle \chi \rangle].$$

Na G -gradação de $\mathbb{K}H$, a g -ésima componente $(\mathbb{K}H)_g$, $g \in G$, é o $\mathbb{K}$ -sub-espço que tem como base os elementos de $\eta^{-1}(g)$. Como $eKN=(\mathbb{K}H)_1$, a sub-álgebra eKH herda a G -gradação de $\mathbb{K}H$ e a g -ésima componente $(eKH)_g$ é o produto $e(\mathbb{K}H)_g=(\mathbb{K}H)_g e$ em $\mathbb{K}H$. O seu centralizador $C(eKN, eKH)=\mathbb{K}[\langle \chi \rangle]$ herda essa G -gradação, na qual se verifica que

$$\mathbb{K}[\langle \chi \rangle]_g=C(eKN, (eKH)_g), \quad \forall g \in G.$$

Denotaremos por $\alpha=\alpha(\chi, \mathbb{K})$ o elemento de $H^2(G, \mathbb{K})$ determinado pela extensão de Clifford

$$K \longrightarrow H\langle \chi \rangle \longrightarrow G.$$

A proposição seguinte fornece um critério simples para a trivialidade de α .

Proposição 16.1 - O elemento α é trivial se, e somente se, χ

pode ser estendido a um caráter complexo irredutível χ de H tal que $\chi(h) \in K$, $\forall h \in H$.

Demonstração - Sabemos que α é trivial se e somente se $H \langle \chi \rangle$ é uma extensão cindida de K por G , isto é, $H \langle \chi \rangle$ é o produto direto (a ação de G é trivial) de K por G . Tendo em vista o Corolário 15.4, isto ocorre se, e somente se, a álgebra de grupo "twisted" $K[H \langle \chi \rangle]$ possui um caráter linear λ com $H \langle \chi \rangle \cong K \rtimes \ker \lambda$ e como $eKH = eKN \otimes_K K[H \langle \chi \rangle]$ e eKN é central simples, tal λ existe se, e somente se, existe um epimorfismo Λ da álgebra eKH sobre eKN que restrito à última é a identidade e λ é a restrição de Λ a $K[H \langle \chi \rangle]$:

$$eKH = eKN \otimes_K K[H \langle \chi \rangle] \xrightarrow{\Lambda = \text{id}_{eKN} \otimes \lambda} eKN.$$

Como eKH é um somando direto de KH , tais epimorfismos Λ são precisamente as restrições a eKH dos epimorfismos (de álgebras)

$$\psi: KH \longrightarrow eKN$$

tais que $\psi|_{eKN} = \text{id}_{eKN}$. Mas esses epimorfismos ψ não são mais do que as extensões do epimorfismo canônico $KN \longrightarrow eKN$ a representações de KH na álgebra eKN e, portanto, estão em correspondência bijetora, pelo teorema 15.3, com os caracteres complexos irredutíveis χ de H , com valores em K , que restritos a N coincidem com χ .

Suponha, agora, que $\mathbb{L}$ é um subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$, portanto contém todos os valores de χ e podemos construir a extensão de Clifford $H\langle\chi, \mathbb{L}\rangle$ de L por G , usando $\mathbb{L}$ em lugar de $\mathbb{K}$; o idempotente e da $\mathbb{K}$ -subálgebra $\mathbb{K}N$ de $\mathbb{L}N$ é também o idempotente central primitivo de $\mathbb{L}N$ correspondente a χ . Como $\mathbb{L}N = \mathbb{K}N \otimes_{\mathbb{K}} \mathbb{L}$ segue-se que

$$\begin{aligned} \mathbb{L}[H\langle\chi, \mathbb{L}\rangle] &= C(e\mathbb{L}N, e\mathbb{L}H) = C(e\mathbb{K}N \otimes_{\mathbb{K}} \mathbb{L}, e\mathbb{K}H \otimes_{\mathbb{K}} \mathbb{L}) = C(e\mathbb{K}N, e\mathbb{K}H) \otimes_{\mathbb{K}} \mathbb{L} = \\ &= \mathbb{K}[H\langle\chi\rangle] \otimes_{\mathbb{K}} e\mathbb{L} \text{ e, analogamente,} \end{aligned}$$

$$\mathbb{L}[H\langle\chi, \mathbb{L}\rangle]_g = \mathbb{K}[H\langle\chi\rangle]_g \mathbb{L} \tilde{=} \mathbb{K}[H\langle\chi\rangle]_g \otimes_{\mathbb{K}} e\mathbb{L}, \quad \forall g \in G. \quad \square$$

Concluimos que a extensão $L \rightarrow H\langle\chi, L\rangle \rightarrow G$ é obtida da extensão $K \rightarrow H\langle\chi\rangle \rightarrow G$ via a inclusão $K \hookrightarrow L$. Temos assim o seguinte

Corolário 16.2 - O elemento $\alpha(\chi, \mathbb{L})$ correspondente à extensão $L \rightarrow H\langle\chi, L\rangle \rightarrow G$ é a imagem de $\alpha = \alpha(\chi, \mathbb{K})$ pelo homomorfismo

$$H^2(G, K) \longrightarrow H^2(G, L)$$

induzido pela inclusão $K \hookrightarrow L$. $\square$

§ 17 - EXTENSÕES CENTRAIS

As extensões centrais $A \xrightarrow{i} E \xrightarrow{p} G, A \subset Z(E)$, de um grupo abeliano A por um grupo finito G tem uma forma particularmente simples quando A é livre de torção, pois nesse caso o homomorfismo transfer $T: E \rightarrow A$ satisfaz $T(a) = a^{|G|}$, $\forall a \in A$, por ser A central, como foi visto no parágrafo 5, e o subgrupo derivado E' de E está contido em $\ker T$ e, por ser A livre de torção, $A \cap \ker T = \{1\}$ e, em consequência, $A \cap E' = \{1\}$. Segue-se, então, que $p^{-1}(G')$ tem a forma $E' \times A$ e, portanto, o seguinte diagrama, com linhas exatas, é comutativo:

$$\begin{array}{ccccc} A & \rightarrow & E & \rightarrow & G \\ || & & \downarrow & & \downarrow \\ A & \rightarrow & E/E' & \rightarrow & G/G' \end{array}$$

isto é, a sequência superior é obtida por inflação da inferior. Como as classes de equivalência das extensões abelianas de A por G/G' constituem o grupo $\text{Ext}_Z^1(G/G', A)$, e lembrando que, como vimos no parágrafo 8, no caso que estudamos o homomorfismo inflação é injetor, temos, assim, demonstrado a seguinte proposição:

Proposição 17.1 - Sejam A um grupo abeliano livre de torção, G um grupo finito e G' o subgrupo derivado de G. Então a composição dos seguintes monomorfismos

$$\text{Ext}_{\mathbb{Z}}^1(G/G', A) \xrightarrow{\sim} H^2(G/G', A) \xrightarrow{\inf} H^2(G, A)$$

é um isomorfismo. $\square$

Incidentalmente, usando o fato de que a primeira das setas é um isomorfismo, tiramos uma consequência que é típica das aplicações dos métodos da álgebra homológica à teoria dos grupos.

Cordário 17.2 - Seja E um grupo. Se E contém um subgrupo A livre de torção tal que $A \subset Z(E)$ e E/A é abeliano finito, então E é abeliano.

Com efeito, basta considerar a sequência

$$A \rightarrow E \rightarrow E/A = G, \quad G' = \{1\}$$

que é uma extensão central e, pela proposição anterior, abeliana, logo E é abeliano. $\square$

As extensões abelianas $A \rightarrow B \twoheadrightarrow G/G'$ de um grupo abeliano A qualquer por G/G' são relativamente fáceis de descrever. Escolhemos elementos $x_1, \dots, x_t$, $t \geq 0$, em G/G' , de ordens potências de primos $r_1, \dots, r_t$, respectivamente, tais que

$$G/G' = \langle x_1 \rangle \times \dots \times \langle x_t \rangle$$

Se $\tilde{x}_i \in j^{-1}(x_i)$, então $\tilde{x}_i^{r_i} \in A$ e este elemento é determinado, a menos de multiplicação por elementos de $A^{r_i} = \{a^{r_i} \mid a \in A\}$, pela classe de equivalência $\gamma \in \text{Ext}_{\mathbb{Z}}^1(G/G', A)$

da extensão B.

A aplicação

$\gamma \in \text{Ext}_Z^1(G/G', A) \mapsto y_1 \times \dots \times y_t \in A/A^{n_1} \times \dots \times A/A^{r_t}$, onde $y_i = \{\tilde{x}_i^{r_i} \in A/A^{r_i} \mid \tilde{x}_i \in B, j(\tilde{x}_i) = x_i\}$, $1 \leq i \leq t$, estabelece um isomorfismo que nos dá a descrição procurada. Compara-se com Rotman [18], teoremas 7.10 e 7.17.

Antes de demonstrar a proposição que encerra o capítulo, precisamos de um lema auxiliar.

Lema 17.3 - Sejam F um grupo abeliano sem torção e p um número primo. Então, para todo $n \in \mathbb{N}$, $F/p^n F$ é um $\mathbb{Z}/p^n \mathbb{Z}$ - módulo livre.

Demonstração - Faremos a demonstração por indução sobre n. É claro ver que vale para $n=0,1$. Dado $n \geq 2$, seja $\{x_i\}_{i \in I}$ uma base de $F/p^{n-1}F$ sobre $\mathbb{Z}/p^{n-1}\mathbb{Z}$. Vamos mostrar que $\{x_i\}_{i \in I}$ é uma base de $F/p^n F$ sobre $\mathbb{Z}/p^n \mathbb{Z}$.

Primeiramente, vejamos que $\{p^{n-1}x_i\}_{i \in I}$ é uma base de $p^{n-1}F/p^n F$ sobre $\mathbb{Z}/p\mathbb{Z}$.

Se $\sum_{i=1}^m \alpha_i p^{n-1} x_i = 0$, com $\alpha_i \in \mathbb{Z}$, então $\sum_i \alpha_i p^{n-2} x_i \in p^{n-1}F$, logo $\alpha_i p^{n-2} \in p^{n-1}\mathbb{Z}$ e, em consequência, $\alpha_i \in p\mathbb{Z}$, $i=1,2,\dots,m$, o que mostra que $\{p^{n-1}x_i\}_{i \in I}$ é $\mathbb{Z}/p\mathbb{Z}$ - livre.

Além disso, se $z \in p^{n-1}F$, existe $z' \in F$ tal que $z = p^{n-1}z'$, e como $z' = \sum_i \alpha_i x_i + \delta$, com $\delta \in p^{n-1}F$, tem-se que $z = p^{n-1}z' = \sum_i \alpha_i p^{n-1}x_i + \delta'$, com $\delta' \in p^n F$, o que mostra que $\{p^{n-1}x_i\}_{i \in I}$ gera $p^{n-1}F/p^n F$.

Mostremos, agora, que $\{x_i\}_{i \in I}$ é uma base de $F/p^n Z$ sobre $Z/p^n Z$.

Se $\sum_i \alpha_i x_i \in p^n F \subset p^{n-1}F$, então $\alpha_i \in p^{n-1}Z$, logo $\alpha_i = \beta_i p^{n-1}$ com $\beta_i \in Z$, portanto $\sum \beta_i p^{n-1}x_i \in p^n F$ e, em consequência, $\beta_i \in p^n Z \subset pZ$, donde $\alpha_i \in p^n Z$, o que prova que a família $\{x_i\}_{i \in I}$ é $Z/p^n Z$ - livre.

Por outro lado, dado $x \in F$, sejam $\alpha_i \in Z$, $i=1,2,\dots,t$ tais que $x = \sum_i \alpha_i x_i + \delta$, com $\delta \in p^{n-1}F$ e sejam $\beta_i \in Z$, $i=1,\dots,t$, tais que $\delta = \sum_i \beta_i p^{n-1}x_i + \delta' \in p^n F$, em consequência, $x = \sum_i (\alpha_i + \beta_i p^{n-1})x_i + \delta'$, o que termina a demonstração. $\square$

Dado um grupo abeliano A , denotamos por $\text{tor}(A)$ o subgrupo de torção de A e por $F(A)$ o grupo quociente $A/\text{tor}(A)$. Temos a seguinte proposição:

Proposição 17.4 - Sejam G um grupo finito e A um grupo abeliano. Então a sequência exata curta $1 \rightarrow \text{tor}(A) \xrightarrow{i} A \xrightarrow{j} F(A) \rightarrow 1$ induz a seguinte sequência exata cindida de cohomologia de grupos

$$1 \rightarrow H^2(G, \text{tor}(A)) \xrightarrow{i^*} H^2(G, A) \xrightarrow{j^*} H^2(G, F(A)) \rightarrow 1.$$

Demonstração - A sequência $1 \rightarrow \text{tor}(A) \xrightarrow{i} A \xrightarrow{j} F(A) \rightarrow 1$, induz a sequência exata longa de cohomologia

$$\dots \rightarrow H^1(G, F(A)) \rightarrow H^2(G, \text{tor}(A)) \xrightarrow{i^*} H^2(G, A) \xrightarrow{j^*} H^2(G, F(A)) \rightarrow \dots,$$

como foi indicado no parágrafo 7.

Como $H^1(G, F(A)) \cong \text{Hom}(G, F(A))$, pois a ação de G sobre $F(A)$ é trivial, sendo G finito e $F(A)$ sem torção, temos que $H^1(G, F(A)) = \{1\}$.

Assim, basta construir um homomorfismo $\psi: H^2(G, F(A)) \rightarrow H^2(G, A)$ tal que $j^* \circ \psi = \text{id}$. Tendo em vista a Prop. (10.1) e a inclusão natural $\text{Ext}_Z^1(G/G', A) \hookrightarrow H^2(G/G', A)$, é suficiente construir um homomorfismo que cinda a sequência

$$1 \rightarrow \text{Ext}_Z^1(G/G', \text{tor}(A)) \rightarrow \text{Ext}_Z^1(G/G', A) \rightarrow \text{Ext}_Z^1(G/G', F(A)) \rightarrow 1,$$

mas, pela descrição que fizemos de Ext_Z^1 , necessitamos apenas de um homomorfismo que cinda a sequência

$$1 \rightarrow \text{tor}(A) / \text{tor}(A)^{r_i} \rightarrow A / A^{r_i} \rightarrow F(A) / F(A)^{r_i} \rightarrow 1,$$

para cada $i=1, \dots, t$.

Como $\text{tor}(A) \cap A^{r_i} = \text{tor}(A)^{r_i}$, a sequência anterior é uma sequência exata de módulos sobre $Z/r_i Z$ e para mostrar que é cindida basta lembrar que, pelo lema anterior,

$F(A)/F(A)^{r_i}$ é um $Z/r_i Z$ - módulo livre e, portanto, projetivo. $\square$

Como $H^2(G, F(A)) \cong \text{Ext}_Z^1(G/G', F(A))$, temos a seguinte consequência imediata:

Corolário 17.5 - O homomorfismo ψ , da proposição anterior, associa

$$\beta \in H^2(G, F(A)) \mapsto \psi(\beta) \in H^2(G, A),$$

onde $\psi(\beta)$ corresponde a uma extensão $1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$ obtida por inflação de uma extensão abeliana $1 \rightarrow A \rightarrow B \rightarrow G/G' \rightarrow 1$. $\square$

§ 18 - MODIFICAÇÕES DE H

Sejam $\mathbb{K}$ um subcorpo dos complexos; K o seu grupo multiplicativo, G um grupo finito, $K \rightarrow E \rightarrow G$ uma extensão central e $\gamma \in H^2(G, K)$ o seu elemento correspondente. Se $\gamma \in i^* H^2(G, \text{tor}(K))$, então existe um subgrupo E_1 de E que torna o diagrama

$$\begin{array}{ccccc} \text{tor}(K) & \hookrightarrow & E_1 & \xrightarrow{p} & G \\ i \downarrow & & \downarrow & & \parallel \\ K & \rightarrow & E & \rightarrow & G \end{array}$$

comutativo e tal que $E_1 \cap K = \text{tor}(K)$. Para cada $g \in G$, escolhemos $g^* \in p^{-1}(g)$, então, para o subgrupo E_0 gerado pelos g^* , temos que $p|_{E_0} : E_0 \rightarrow G$ é sobrejetora, $\ker(p|_{E_0}) = E_0 \cap \text{tor}(K) \triangleleft E_0$ e, em

consequência, $E_0 / (E_0 \cap \text{tor}(K)) \cong G$. Sendo E_0 finitamente gerado, $K_0 = E_0 \cap \text{tor}(K)$ também o é e como cada elemento de K_0 é de ordem finita, tem-se que K_0 é um grupo abeliano finito gerado por elementos da forma

$$g * h * [(gh)^*]^{-1}; \quad g, h \in G.$$

Em consequência, E_0 é um grupo finito e temos assim demonstrado a seguinte proposição.

Proposição 18.1 - Dado $\gamma \in i^* H^2(G, \text{tor}(K))$, existe um grupo finito E_0 que é uma extensão central de um subgrupo finito K_0 , de K , por G tal que γ é a imagem do elemento $\gamma_0 \in H^2(G, K_0)$ correspondente a E_0 . $\square$

A imagem de γ_0 , é claramente, dada pela aplicação $i^*: H^2(G, K) \rightarrow H^2(G, K)$ induzida pela inclusão $i: K_0 \hookrightarrow K$. Evidentemente, i é também um caráter linear complexo de K_0 e como tal é E_0 -invariante pois K_0 é central em E_0 . Assim, da mesma maneira como foi feito no §16, podemos construir a extensão de Clifford $K \twoheadrightarrow E_0 \langle i \rangle \twoheadrightarrow G$, e sendo $e(i)$ o idempotente central primitivo da álgebra $\mathbb{K}K_0$ correspondente ao caráter i temos que $e(i)\mathbb{K}K_0$ é uma sub-álgebra unidimensional de $\mathbb{K}K_0$ e $\mathbb{K}[E_0 \langle i \rangle] = e(i)\mathbb{K}E_0$; $\mathbb{K}[E_0 \langle i \rangle]_g = e(i)(\mathbb{K}E_0)_g$, $\forall g \in G$.

Segue-se que a aplicação $x \in E_0 \mapsto e(i)x \in E_0 \langle i \rangle$ estabelece um homomorfismo de extensões

$$\begin{array}{ccccc} K_0 & \twoheadrightarrow & E_0 & \twoheadrightarrow & G \\ \downarrow 1 & & \downarrow & & \parallel \\ K & \rightarrow & E_0 \langle 1 \rangle & \twoheadrightarrow & G \end{array}$$

tal que restrita a K_0 verifica $k \in K_0 \mapsto e(1)k = e(1)1(k) \in e(1)K \cong K$.

Usando a notação $\alpha(1)$ para o elemento de $H^2(G, K)$ de terminado pela extensão $K \twoheadrightarrow E_0 \langle 1 \rangle \twoheadrightarrow G$, temos $\alpha(1) = 1^*(\gamma_0) = \gamma$.

Terminamos este parágrafo com a seguinte proposição.

Proposição 18.2 - Com as mesmas notações acima, dado $\gamma \in 1^*(H^2(G, \text{tor } K))$, existem um grupo finito H_0 , um epimorfismo $\eta_0: H_0 \rightarrow G$ e um caráter complexo irreduzível H_0 -invariante $\chi_0: \text{kern } \eta_0 \rightarrow K$ tais que $\alpha(\chi_0) = \gamma \alpha(\chi)$ em $H^2(G, K)$.

Demonstração - O produto direto $E_0 \times H$ é uma extensão central do seu subgrupo normal $K_0 \times N$ por $G \times G$ e temos $K(E_0 \times H) = K E_0 \otimes_K K H$, e esta igualdade nos permite concluir, usando o Teorema 15.3, que a extensão de Clifford $K \twoheadrightarrow (E_0 \times H) \langle 1 \times \chi \rangle \twoheadrightarrow G \times G$ correspondente ao caráter $1 \times \chi$ de $K_0 \times N$ é a extensão central

$$K \twoheadrightarrow E_0 \langle 1 \rangle \vee H \langle \chi \rangle \twoheadrightarrow G \times G,$$

onde $E_0 \langle 1 \rangle \vee H \langle \chi \rangle$ é o produto central de $E_0 \langle 1 \rangle$ e $H \langle \chi \rangle$ com K amalgamado (veja Def. 15.5).

Seja, agora, H_0 o pull-back do diagrama $E_0 \xrightarrow{H} G$, explicitamen

te, $H_0 = \{u \times v \in E_0 \times H; u \text{ e } v \text{ tem a mesma imagem em } G\}$, temos, assim, uma extensão $K_0 \times N \twoheadrightarrow H_0 \xrightarrow{\eta_0} G$, onde η_0 é a composição $H_0 \twoheadrightarrow H \xrightarrow{\eta} G$, da qual obtemos a extensão de Clifford

$$K \twoheadrightarrow H_0 \langle 1 \times \chi \rangle \twoheadrightarrow G.$$

Da definição de $\mathbb{K}[H_0 \langle 1 \times \chi \rangle]$ como

$C(e(1 \times \chi) \mathbb{K}(K_0 \times N), e(1 \times \chi) \mathbb{K}(H_0))$ e de $\mathbb{K}[(E_0 \times H) \langle 1 \times \chi \rangle]$ como $C(e(1 \times \chi) \mathbb{K}(K_0 \times N), e(1 \times \chi) \mathbb{K}(E_0 \times H))$ tiramos, imediatamente, a comutatividade do diagrama

$$\begin{array}{ccccc} K \twoheadrightarrow & H_0 \langle 1 \times \chi \rangle & \twoheadrightarrow & G \\ \parallel & \downarrow & & \downarrow \Delta \\ K \twoheadrightarrow & (E_0 \times H) \langle 1 \times \chi \rangle & \xrightarrow{\text{pr}} & G \times G, \end{array}$$

onde Δ é a inclusão $g \in G \mapsto g \times g \in G \times G$. Disto decorre que $H_0 \langle 1 \times \chi \rangle = \text{pr}^{-1}(\Delta G)$ e (veja a construção da soma de Baer de extensões) do diagrama comutativo

$$\begin{array}{ccccc} K \times K \twoheadrightarrow & E_0 \langle 1 \rangle \oplus H \langle \chi \rangle & \twoheadrightarrow & G \times G \\ \forall \downarrow \text{push out} & \downarrow & & \parallel \\ K \twoheadrightarrow & E_0 \langle 1 \rangle \oplus H \langle \chi \rangle & \xrightarrow{\text{pr}} & G \times G \\ \parallel & \uparrow \text{pull back} & & \uparrow \Delta \\ K \twoheadrightarrow & H_0 \langle 1 \times \chi \rangle & \twoheadrightarrow & G \end{array}$$

tiramos que $\alpha(1 \times \chi) = \alpha(1) \alpha(\chi) = \gamma \alpha(\chi)$ em $H^2(G, K)$. $\square$

§ 19 - EXTENSÕES CICLOTÔMICAS

Denotemos por $\mathbb{K}_n$, n inteiro positivo, a extensão ciclotômica obtida adjuntando a $\mathbb{K}$ todas as raízes n -ésimas

da unidade.

Lema 19.1 - Sejam H e G grupos finitos, $\eta: H \rightarrow G$ um epimorfismo, $N = \ker \eta$, χ um $\mathbb{C}$ -caráter complexo irreduzível H -invariante de N e $\mathbb{K}$ um subcorpo de $\mathbb{C}$ que contém todos os valores $\chi(h)$, $h \in N$. Seja $K \twoheadrightarrow H \langle \chi \rangle \twoheadrightarrow G$ uma extensão de Clifford obtida por inflação de uma extensão abeliana $K \twoheadrightarrow A \twoheadrightarrow G/G'$ e seja n o expoente de H . Então, a imagem de $\alpha \in H^2(G, \mathbb{K})$ em $H^2(G, \mathbb{K}_n)$ é o elemento 1.

Demonstração - Pelo Corolário 16.2, $\alpha \in H^2(G, \mathbb{K}) \mapsto \alpha(\chi, \mathbb{K}_n) \in H^2(G, \mathbb{K}_n)$, onde $\alpha(\chi, \mathbb{K}_n)$ é o elemento correspondente à extensão de Clifford $H \langle \chi, \mathbb{K}_n \rangle$. Analogamente, a imagem de α em $H^2(G, \mathbb{C}^*)$ é $\alpha(\chi, \mathbb{C})$ que corresponde à extensão de Clifford $H \langle \chi, \mathbb{C} \rangle$. Segue-se disto que $H \langle \chi, \mathbb{C} \rangle$ é obtida por inflação de uma extensão abeliana $\mathbb{C}^* \twoheadrightarrow B \twoheadrightarrow G/G'$, mas como $\mathbb{C}^*$ é um subgrupo divisível e ele é um $\mathbb{Z}$ -módulo injetivo, portanto a sequência anterior é cindida e, em consequência, $\alpha(\chi, \mathbb{C})$ é trivial. Pela Proposição 16.1, χ pode ser estendido a um caráter complexo irreduzível X de H tal que $X(h) \in \mathbb{K} \subset \mathbb{K}$, $\forall h \in H$, e, usando novamente a mesma proposição, temos que $\alpha(\chi, \mathbb{K}_n)$ é trivial. $\square$

Chamemos $\beta = \beta(\mathbb{K})$ a imagem de α em $H^2(G, F(\mathbb{K}))$. Dado um subcorpo $\mathbb{L}$ de $\mathbb{C}$ que contém $\mathbb{K}$, seja L o seu grupo multiplicativo. Temos a comutatividade do seguinte diagrama

$$\begin{array}{ccccc} \text{tor} K \twoheadrightarrow & K & \twoheadrightarrow & F(K) & \\ \downarrow & \downarrow & & \downarrow & \\ \text{tor} L \twoheadrightarrow & L & \twoheadrightarrow & F(L) & \end{array}$$

que, pelo Corolário 16.2 e a Proposição 17.4, induz a comutatividade e a correspondência de elementos no seguinte diagrama

$$\begin{array}{ccc} \alpha = \alpha(\chi, K) \in H^2(G, K) & \longmapsto & \beta = \beta(K) \in H^2(G, F(K)) \\ \downarrow & & \downarrow \\ \alpha(\chi, L) \in H^2(G, L) & \longrightarrow & \beta(L) \in H^2(G, F(L)) \end{array}$$

Teorema 19.2 - Existe um corpo K_n , $K \subset K_n \subset \mathbb{C}$, para algum inteiro positivo n , tal que a imagem $\beta(K_n)$ de β (e portanto de α) em $H^2(G, F(K_n))$ é trivial.

Demonstração - Com as notações do Corolário 17.5, o elemento $\gamma = [\psi j^*(\alpha)] \cdot \alpha^{-1}$ pertencente a $\ker j^* = \text{Im } i^*$, verifica $\gamma \alpha \in \text{Im } \psi$, portanto $\gamma \alpha$ é um elemento de $H^2(G, K)$ correspondente a uma extensão de K por G obtida por inflação de uma extensão abeliana de K por G/G' . Pela Proposição 18.2, existem um grupo finito H_0 , um epimorfismo $\eta_0: H_0 \rightarrow G$ e um caráter complexo irreduzível H_0 -invariante $\chi_0: \ker \eta_0 \rightarrow K$ tal que $\alpha(\chi_0) = \gamma \alpha$; em consequência, a extensão $H_0 \langle \chi_0 \rangle$ é obtida por inflação de uma extensão abeliana e, pelo Lema 19.1, a imagem $\beta(K_n)$ de $\gamma \alpha$ (e portanto de β) em $H^2(G, F(K_n))$ é trivial, sendo n o expoente de H_0 . $\square$

§ 20 - EXPOENTES

Tendo em vista o Teorema 19.2, é interessante o estudo do núcleo do homomorfismo $H^2(G, F(K)) \rightarrow H^2(G, F(L))$, para certas extensões L do corpo K . Pela Proposição 17.1, e pela descrição que fizemos precedendo o Lema 17.3, isto é equivalente a estudar os núcleos de homomorfismos $\phi = \phi_L: F(K)/F(K)^t \rightarrow F(L)/F(L)^t$, para alguns $t \in \mathbb{N}$, induzidos por $K \hookrightarrow L$. Esses núcleos são mais fáceis de descrever no caso em que L contém todas as raízes t^i -ésimas da unidade, para $i=1, 2, \dots$.

Lema 20.1 - Seja t um inteiro positivo e seja L uma extensão de K que contém uma raiz primitiva t^i -ésima da unidade, para todo $i \geq 1$. Seja $\bar{f}$ um elemento de ordem s em $F(K)/F(K)^t$. Então, $\phi(\bar{f})=1$ se, e somente se, existe $\ell \in L$ tal que:

$$(20.1a) \quad \ell^s = k \in K,$$

$$(20.1b) \quad k \text{ tem ordem } s, \text{ módulo } \text{tor}(K) \cdot K^s,$$

$$(20.1c) \quad \bar{f} \text{ é a imagem em } F(K)/F(K)^t, \text{ pela projeção canônica, de } \ell^{t=k^{t/s}}.$$

Demonstração - Começamos observando que $[F(K)/F(K)^t]^t = 1$, assim a fração t/s é um inteiro.

Se $\ell \in L$ satisfaz as tres condições acima, en-

$\phi(\bar{f})$ é a imagem em $F(L)/F(L)^t$ de ℓ^t , portanto $\phi(\bar{f})=1$.

Suponhamos agora que $\phi(\bar{f})=1$. Como $\bar{f}=f.F(K)^t$ tem ordem s , temos que $f^s=f_1^t$, para algum $f_1 \in F(K)$ e como $F(K)$ é livre de torção, temos $f=f_1^{t/s}$ e também que f_1 tem ordem s , módulo $F(K)^s$, portanto para todo elemento $k \in K$ tal que $k \in K \mapsto f_1 \in F(K)$ tem-se que $k \text{ tor}(K).F(K)^s = k \text{ tor}(K).K^s$ tem ordem s em $F(K)/F(K)^s$, logo para tais k vale (20.1b) e a verificação de (20.1c) segue das correspondências

$$k^{t/s} \in K \mapsto f_1^{t/s} = f \in F(K) \mapsto \bar{f} \in F(K)/F(K)^t \mapsto \phi(\bar{f}) = 1 \in F(L)/F(L)^t.$$

Assim, a imagem f_2 de k em $F(L)$ satisfaz $f_2^{t/s} \in F(L)^t$ e como $F(L)$ é livre de torção, isto implica que $f_2 \in F(L)^s$ e, em consequência, $k \in \text{tor}(L).L^s$. Como L contém todas as raízes t^i -ésimas da unidade, para $i=1, 2, \dots$, e s divide t , temos $\text{tor } L \supset (\text{tor } L)^s \supset (\text{tor } L)^t = \text{tor } L$, portanto $\text{tor } L = (\text{tor } L)^s \subset L^s$ e $k \in L^s$. Assim vale (20.1a) para algum $\ell \in L$. $\square$

A condição (20.1b) do lema anterior tem a seguinte útil consequência.

Lema 20.2 - Seja $k \in K$ um elemento que satisfaz a condição (20.1b) para algum inteiro positivo s , isto é, k tem ordem s módulo $\text{tor}(K).K^s$. Então, o polinômio $X^s - k$ é irredu

tível sobre $\mathbb{K}$.

Demonstração - As raízes de $X^s - k$ num corpo de decomposição $\mathbb{L}$ tem a forma $\zeta^i \ell$, $i=1,2,\dots,s$, onde ζ é uma raiz s -ésima primitiva da unidade e $\ell \in \mathbb{L}$. Portanto todo polinômio mônico $h(X)$, de grau r , que divide $X^s - k$ tem a forma

$$h(X) = \prod_{i \in I} (X - \zeta^i \ell), \text{ com } I \subset \{1,2,\dots,s\} \text{ e } r = \text{card} I.$$

Suponhamos que $h(X)$ tem coeficientes em $\mathbb{K}$. Temos, então, que $(-1)^r h(0) = \omega \ell^r \in \mathbb{K}$, onde $\omega = \prod_{i \in I} \zeta^i$ é uma raiz s -ésima da unidade. Sejam $q = \text{mdc}(r,s)$ e $a, b \in \mathbb{Z}$ tais que $q = ar + bs$. Como $\ell^s = k \in \mathbb{K}$, temos $\omega^a \ell^q = (\omega \ell^r)^a (\ell^s)^b \in \mathbb{K}$, donde $(\omega^a \ell^q)^{s/q} = \omega^{as/q} \ell^s = \omega^{as/q} k \in \mathbb{K}$, portanto a raiz da unidade $\omega^{as/q}$ está em $\mathbb{K}$, isto é, $\omega^{as/q} \in \text{tor}(K)$. Em consequência, $k \in \text{tor}(K) \cdot K^{s/q}$, logo $k^q \in \text{tor}(K) \cdot K^s$ e, por (20.1b), s divide q e portanto s divide $r = \text{card} I$, donde concluímos que $I = \{1,2,\dots,s\}$, a menos que $I = \emptyset$. Isto é, $h(X) = X^s - k$ ou $h(X) = 1$. $\square$

Usaremos a informação obtida sobre $\ker \phi$ para provar o seguinte teorema.

Teorema 20.3 - Seja $\mathbb{L}$ uma extensão abeliana do corpo $\mathbb{K}$ e seja s o expoente de $\ker \phi$. Então $\mathbb{K}$ contém uma raiz s -ésima primitiva da unidade.

Demonstração - Lembramos que uma extensão abeliana de $\mathbb{K}$ é uma extensão normal separável $\mathbb{L}$ de $\mathbb{K}$ tal que o grupo de Galois $\text{Gal}(\mathbb{L}/\mathbb{K})$ é abeliano. Adjuntando todas as raízes t^i -ésimas da unidade, $i=1,2,\dots$, a tal $\mathbb{L}$ obtemos uma extensão abeliana $\mathbb{M}$ de $\mathbb{K}$ e $\ker\phi_{\mathbb{L}}$ é um subgrupo de $\ker\phi_{\mathbb{M}}$. Assim, é suficiente provar o teorema para $\mathbb{M}$ em lugar de $\mathbb{L}$, isto é, podemos assumir que $\mathbb{L}$ contém todas as raízes t^i -ésimas da unidade, $i \geq 1$.

O grupo abeliano $\ker \phi$ contém um elemento $\bar{f}$ de ordem s , pois $s = \text{expoente de } \ker\phi$. Assim, aplicando o Lema 20.1, obtemos elementos $k \in \mathbb{K}$ e $\ell \in \mathbb{L}$ que satisfazem 20.1a - 20.1c. Pelo Lema 20.2, $X^s - k$ é o polinômio minimal de ℓ sobre $\mathbb{K}$, portanto $[\mathbb{K}(\ell):\mathbb{K}] = s$ e sendo $\mathbb{L}/\mathbb{K}$ abeliana também $\mathbb{K}(\ell)/\mathbb{K}$ o é. Em particular, $\mathbb{K}(\ell)$ contém todas as raízes $\zeta^i \ell$, $i=1,2,\dots,s$, de $X^s - k$, onde ζ é uma raiz s -ésima primitiva da unidade. Portanto $\zeta = \zeta \ell / \ell \in \mathbb{K}(\ell)$. Devemos mostrar que, de fato, $\zeta \in \mathbb{K}$.

Suponhamos, por absurdo, que $\zeta \notin \mathbb{K}$. Como $\zeta^s = 1 \in \mathbb{K}$, existe o menor divisor r de s tal que $\omega = \zeta^{s/r} \notin \mathbb{K}$, portanto r deve ser uma potência de um primo p e ω uma raiz r -ésima primitiva da unidade tal que $\omega^p \in \mathbb{K}$. Por (20.1b), k tem ordem r módulo $\text{tor}(\mathbb{K}) \cdot \mathbb{K}^r$, portanto o polinômio $X^r - k$ é irredutível sobre $\mathbb{K}$, pelo Lema 20.2. E,

como acima, concluímos que ω pertence ao corpo $\mathbb{K}(\ell^{s/r})$, gerado pela raiz $\ell^{s/r}$ do polinômio $X^r - k$.

Seja, agora, σ um elemento do grupo de Galois $\text{Gal}(\mathbb{K}(\ell^{s/r})/\mathbb{K})$ que fixa ω . Como $\sigma(\ell^{s/r})$ é uma raiz do polinômio $X^r - k$, temos que $\sigma(\ell^{s/r}) = \omega^i \ell^{s/r}$, para algum $i \in \{1, 2, \dots, r\}$. Como σ fixa ω , concluímos que a ordem de σ em $\text{Gal}(\mathbb{K}(\ell^{s/r})/\mathbb{K})$ coincide com a ordem de ω^i em $\text{tor}(L)$. Sabemos que $X^r - k$ é irredutível sobre $\mathbb{K}$ e, em consequência, $\text{Gal}(\mathbb{K}(\ell^{s/r})/\mathbb{K})$ tem ordem r e como σ não gera esse grupo, pois fixa o elemento $\omega \notin \mathbb{K}$, a ordem σ , e de ω^i , deve ser um divisor próprio da potência r de p e, portanto, divide r/p . Temos, então, que

$$\sigma(\ell^{s/p}) = \sigma^{r/p}(\ell^{s/r}) = \omega^{ir/p} \ell^{s/p} = \ell^{s/p}.$$

Portanto, todo $\sigma \in \text{Gal}(\mathbb{K}(\ell^{s/r})/\mathbb{K})$ que fixa ω fixa também $\ell^{s/p}$, isto é,

$$\mathbb{K}(\ell^{s/p}) \subset \mathbb{K}(\omega).$$

Da mesma maneira que provamos para $\ell^{s/r}$ anteriormente, por (20.1b) e o Lema 20.2, a extensão $\mathbb{K}(\ell^{s/p})$ tem grau p sobre $\mathbb{K}$ e como $\omega^p \in \mathbb{K}$, temos $\mathbb{K}(\ell^{s/p}) = \mathbb{K}(\omega)$. Assim, $\mathbb{K}(\omega)$ tem grau p sobre $\mathbb{K}$ e, portanto, ω não é uma raiz p -ésima da unidade e, sendo ω uma r -ésima primitiva da unidade e r uma potência de p , o subgrupo $\langle \omega^p \rangle$ de K contém uma raiz p -ésima primitiva ξ da unida-

de. Como a extensão cíclica $\mathbb{K}(\omega) = \mathbb{K}(\ell^{s/p})$, de grau p , pode ser gerada por ω ou por $\ell^{s/p}$, que são raízes p -ésimas de elementos de K , e como $\xi \in K$, temos que $\ell^{s/p} \in \omega^j K$, para algum $j \in \{1, 2, \dots, p-1\}$ e, então,

$$k = (\ell^{s/p})^p \in \omega^{pj} K^p \subset \text{tor}(K) \cdot K^p,$$

e, portanto, $k^{s/p} \in \text{tor}(K) \cdot K^s$, o que contradiz (20.1b), e o teorema está demonstrado. $\square$

O teorema anterior tem consequências imediatas sobre as ordens dos elementos $\alpha \in H^2(G, K)$ e $\beta \in H^2(G, F(K))$ do parágrafo anterior. Consideramos β primeiramente.

Teorema 20.3 - Seja r o expoente do grupo quociente G/G' e seja $r(K)$ a ordem do grupo das raízes r -ésimas da unidade em K . Tem-se, então, que $\beta^{r(K)} = 1$.

Demonstração - Pelo teorema 19.2 temos uma extensão ciclotômica, portanto abeliana, $\mathbb{L} = \mathbb{K}_n$ de $\mathbb{K}$ tal que β pertence ao núcleo da aplicação natural $S: H^2(G, F(K)) \rightarrow H^2(G, F(L))$. Como indicamos na introdução desse parágrafo, $\ker S$ é isomorfo ao produto direto dos núcleos das aplicações naturais

$$\phi_i: F(K)/F(K)^{r_i} \rightarrow F(L)/F(L)^{r_i}, \quad i=1, 2, \dots, u.$$

Assim, o expoente s de $\ker S$ é o mínimo múltiplo comum

dos expoentes s_i dos $\ker(\phi_i)$, $i=1,2,\dots,u$. Pelo teorema anterior, $\mathbb{K}$ contém uma raiz s_i -ésima primitiva da unidade, para cada $i=1,2,\dots,u$, e, portanto, contém uma raiz s -ésima primitiva ζ da unidade. Como s_i divide r_i , para $i=1,2,\dots,u$, então s divide o mínimo múltiplo comum dos r_i , que é r , pois $G/G' \cong F(K)/F(K)^{r_1} \times \dots \times F(K)/F(K)^{r_u}$ como vimos no § 17. Portanto, ζ é uma raiz r -ésima da unidade em $\mathbb{K}$ cuja ordem s divide $r(\mathbb{K})$ e como $\beta \in S$, temos a tese. $\square$

Para o elemento $\alpha \in H^2(G, \mathbb{K})$ temos o seguinte resultado.

Teorema 20.4 - Sejam m a ordem de G e $m(\mathbb{K})$ a ordem do grupo das raízes m -ésimas da unidade em $\mathbb{K}$. Temos, então, que $\alpha^{m(\mathbb{K})} = 1$.

Demonstração - Como $\text{tor}(K)$ é o produto direto fraco dos seus p -subgrupos de Sylow $\text{tor}(K)_p$, onde p percorre o conjunto dos números primos, mostremos inicialmente que

$$H^2(G, (\text{tor}K)_p)^{m(\mathbb{K})} = 1,$$

para todo primo p . Para tanto, observemos inicialmente que se $\text{tor}(K)_p^{m(\mathbb{K})} = 1$, a igualdade acima é imediata. Por outro lado, se $\text{tor}(K)_p^{m(\mathbb{K})} \neq 1$, para algum p , então existe um elemento de ordem p^{n+1} em $\text{tor}(K)_p$, onde p^n denota a

maior potência de p que divide $m(\mathbb{K})$. Em consequência, p^{n+1} não divide m e $m = p^n \cdot t$, com p e t primos entre si. Assim, sendo $H^2(G, \text{tor}(K)_p)$ um p -grupo, e lembrando que a ordem de todo elemento de $H^2(G, \text{tor}(K))$ divide a ordem de G , temos que

$$H^2(G, \text{tor}(K)_p)^{p^n} = H^2(G, \text{tor}(K)_p)^m = 1,$$

donde decorre $H^2(G, \text{tor}(K)_p)^{m(\mathbb{K})} = 1$, para todo primo p .

Finalmente, como o expoente r de G/G' divide a ordem m de G , $r(\mathbb{K})$ divide $m(\mathbb{K})$ e temos $\beta^{m(\mathbb{K})} = 1$ pelo teorema anterior, e usando o isomorfismo dado pela Prop 17.4, temos a tese. $\square$

Como uma consequência imediata temos o seguinte corolário.

Corolário 20.5 - Se $m(\mathbb{K}) = 1$, isto é, se 1 é a única raiz m -ésima da unidade em $\mathbb{K}$, então $\alpha = 1$ e χ pode ser estendido a um caráter complexo irreduzível X de H com valores em $\mathbb{K}$.

Demonstração - Basta usar o teorema anterior e aplicar diretamente a Proposição 16.1. $\square$

BIBLIOGRAFIA

- [1] BABAKHANIAN, A. - *Cohomological methods in group theory*.
Marcel Dekker, Inc., New York, (1972).
- [2] CLIFFORD, A. H. - *Representations induced in an invariant
subgroup*. Ann. of Math. 38, (1937), 533-550.
- [3] CONLON, S.B. - *Twisted group algebras and their repre-
sentations*. J. Austral. Math. Soc. 4 (1964), 152-
-173.
- [4] ————— - *Related components of representations*.
J. Algebra 8 (1968), 478-501.
- [5] CURTIS, C. W., REINER, I. - *Representation theory of
finite groups and associative algebras*. Intersci-
ence, New York (1962).
- [6] DORNHOFF, L. - *Group representation theory*. Marcel
Dekker, Inc., New York (1971).
- [7] DADE, E. C. - *Characters of solvable groups*. Univ. of
Illinois, (1967).

- [8] DADE, E. C. - *Compounding Clifford's theory*. Ann. of Math. 91 (1970), 236-290.
- [9] ———— *Isomorphisms of Clifford's extensions*. Ann. of Math. 91 (1970), 375-433.
- [10] ———— *Character values and Clifford extensions for finite groups*. Proc. London Math. Soc. 3,29, (1974), 216-236.
- [11] FELL, J. M. G. - *An extension of Mackey's method to algebraic bundles over finite groups*. Amer. J. Math. 41 (1969), 203-238.
- [12] FELZENSZWALB, B. - *Álgebras de dimensão finitas*. 129 Colóquio Brasileiro de Matemática, I.M.P.A. (1979).
- [13] GLAUBERMAN, G. - *Correspondences of characters for relatively prime operator groups*. Canad. J. Math. 20 (1968), 1465-1488.
- [14] HILTON, P. J. - STAMBACH, V. - *A course in homological algebra*. Springer-Verlag, Berlin (1971).
- [15] ISAACS, I. M. - *Invariant and extendable group characters*. Ill. J. Math. 14 (1970), 70-75.

- [16] ISAACS, I. M. - *Character theory of finite groups*.
Academic Press, New York, (1976).

- [17] MAIER, R., HO, C.-Y., GONÇALVES, A., POMAREDA, R. -
Tópicos em teoria dos grupos finitos. IV Escola
de Álgebra, S.B.M., São Paulo (1976).

- [18] ROTMAN, J. J. - *Notes on homological algebra*. Van
Nostrand, New York, (1970).

- [19] TUCKER, P. A. - *On the reduction of induced representations
of finite groups*. Amer. J. Math. 84 (1962), 400-420.

- [20] ——— - *Note on the reduction of induced re-
presentations*. Amer. J. Math. 85 (1963), 53-58.

- [21] ——— *Endomorphism ring of an induced module*.
Mich. Math. J. 12 (1965), 197-202.

- [22] ——— *On the reduction of induced indecomposable
representations*. Amer. J. Math. 87 (1965), 798-806.

- [23] WARD, H. N. - *The analysis of representations induced
from a normal subgroup*. Mich. Math. J. 15 (1968),
417-428.

- [24] YAMAZAKI, K. - *On projective representations and ring extensions of finite groups.* J. Fac. Sci. Univ. Tokyo, Sect. I 10 (1964), 147-195.