A ESTRUTURA DE CERTOS ANÉIS COM DIVISÃO

UMA CONJECTURA DE ALBERT

HELOISA DARUIZ BORSARI

DISSERTAÇÃO APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA OBTENÇÃO DO GRAU DE MESTRE
EM
MATEMÁTICA

ORIENTADOR:

Prof.Dr. FRANCISCO CÉSAR POLCINO MILIES

Durante a elaboração deste trabalho, a autora recebeu apoio financeiro da FAPESP e da FINEP.

São Paulo, maio de 1982

Aos meus pais, com muito carinho.

AGRADECIMENTOS

Muitas foram as pessoas que, de uma forma ou de outra, colaboraram na elaboração desta dissertação. Dentre elas, gostaria de agradecer especialmente ao Prof. César Polcino, pelo incentivo e orientação; aos colegas Fernando Quadros Gouvêa, Sonia Pitta Coelho e Nair Alexandre Fernandes, pelo interesse e por suas valiosas sugestões e principalmente ao Daciberg, pelo sentido maior que tem dado à minha vida e com quem hoje partilho a satisfação de concluir esta etapa.

Agradeço ainda a Regina Helena da Silva e Luzia do Carmo Namiki pela datilografia deste trabalho.

Heloisa Daruiz Borsari

Í N D I C E

Página

INTRODUÇÃO . . . . . (i)

CAPÍTULO I - ÁLGEBRAS DE QUATÉRNIOS GENERALIZADAS

§ 1. Álgebras de Quatérnios Generalizadas: definição e propriedades 2

§ 2. Algumas caracterizações das álgebras de quatérnios com divisão 12

CAPÍTULO II - ANÉIS COM INVOLUÇÃO E ÁLGEBRAS DE QUATÉRNIOS

§ 3. Anéis simples com involução: Algumas caracterizações 22

§ 4. Involução do primeiro tipo: Fatos gerais 31

§ 5. Álgebras com divisão de dimensão 16 sobre seu centro 44

CAPÍTULO III - SOBRE UMA CONJECTURA DE ALBERT

§ 6. Produto tensorial de álgebras de quatérnios 53

Página

§ 7. Produtos Cruzados Abelianos. 59

§ 8. Produtos Cruzados Abelianos de grau 8 com involução 102

§ 9. Produtos Cruzados Abelianos Genéricos . 124

§ 10. O contra-exemplo. 140

APÊNDICE - Um teorema de Herstein-Procesi-Schacher 147

BIBLIOGRAFIA 169

INTRODUÇÃO

A classificação das álgebras simples centrais de dimensão finita, como um anel de matrizes com coeficientes em um anel com divisão, é devida a J.H.Wedderburn e data de 1907.

A partir de então, o problema de classificar as álgebras com divisão de dimensão finita sobre seu centro, foi considerado relevante. Nesse sentido, sabe-se que se D é uma tal álgebra de centro Z e $[D:Z] = p_1^{m_1} \dots p_r^{m_r}$, onde cada p_i é primo, então existem anéis com divisão $D_1,\dots,D_r$, de centro Z, tais que $D \simeq D_1 \otimes_Z \dots \otimes_Z D_r$ e $[D_i:Z]=p_i^{m_i}$, $1 \leq i \leq r$.

Dessa forma, podemos reduzir o problema a classificar as álgebras com divisão, cuja dimensão sobre o centro é potência de um primo.

No Capítulo I desse trabalho, classificamos as álgebras simples de dimensão 4 sobre seu centro. Para isso, estendemos a construção dos quatérnios reais de Hamilton, introduzindo a noção de álgebras de quatérnios generalizadas. Além disso, obtemos também algumas caracterizações das álgebras com divisão de dimensão 4 sobre seu centro.

No Capítulo II, estudamos algumas propriedades de anéis simples com involução e apresentamos uma nova demonstração de um teorema de A.A.Albert, que classifica as álgebras

com divisão de dimensão 16 sobre seu centro, como produto tensorial de álgebras de quatérnios generalizadas.

Este resultado deu origem a uma famosa conjectura de A.A.Albert. Seriam as álgebras com divisão, de dimensão 2^{2m} sobre seu centro, com involução, isomorfas a um produto tensorial de álgebras de quatérnios?

O capítulo III constitui-se essencialmente da construção de um contra-exemplo para esta conjectura.

Finalmente, no apêndice desta dissertação, apresentamos um resultado de I.N.Herstein, C.Procesi e M.Schacher, que é utilizado no Capítulo I.

CAPÍTULO I

ÁLGEBRAS DE QUATÉRNIOS GENERALIZADAS

O objetivo deste capítulo é classificar as álgebras simples de dimensão quatro sobre seu centro.

O primeiro exemplo de uma álgebra com divisão, não comutativa, foi construído por W.R.Hamilton, em 1946. Trata-se de uma extensão dos números complexos, cujos elementos são somas formais do tipo $a + bi + cj + dk$, onde a,b,c,d são números reais. A adição é definida da maneira usual e a multiplicação se faz distributivamente, de acordo com as seguintes regras:

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \end{cases}$$

Tal álgebra ficou conhecida como a álgebra dos quatérnios e verifica-se facilmente que se trata de um anel com divisão, de dimensão quatro sobre seu centro, que é $\mathbb{R}$ (corpo dos números reais).

Hamilton parece ter levado 10 anos para construir esta tábua de multiplicação e talvez isto se deva ao fato de seu objetivo ter sido, durante algum tempo, o de construir um corpo de dimensão três sobre os reais, o que sabemos hoje, ser impossível.

Para obtermos a classificação das álgebras simples centrais de dimensão quatro, generalizaremos a construção de Hamilton, de maneira bastante natural. As referências básicas para este capítulo são [4] , [16] e [18].

§ 1 - ÁLGEBRAS DE QUATÉRNIOS GENERALIZADAS: PROPRIEDADES BÁSICAS.

1.1 - DEFINIÇÃO - Seja F um corpo de característica diferente de dois. Uma álgebra de quatérnios (generalizada) sobre F é uma F-álgebra de dimensão 4, com base $\{1, i, j, k\}$ satisfazendo as seguintes condições:

$$\begin{cases} i^2 = \alpha, \quad j^2 = \beta \qquad \text{onde } 0 \neq \alpha, \beta \in F \\ ij = k = -ji \end{cases}$$

Uma tal álgebra será denotada por $Q_F(\alpha,\beta)$. Toda base de $Q_F(\alpha,\beta)$ nas condições da definição acima diz-se uma <u>base de quatérnios</u> da álgebra.

1.2 - <u>EXEMPLO</u> - Consideremos $\mathbb{H}$ a álgebra dos quatérnios reais. Então $\mathbb{H}$ é uma $\mathbb{R}$-álgebra de dimensão 4, com base $\{1,i,j,k\}$ e $i^2 = j^2 = -1$, $ij = k = -ji$. ; portanto a definição acima generaliza a construção de Hamilton.

1.3 - <u>EXEMPLO</u> - Seja F um corpo de característica diferente de 2 e consideremos $A = M_2(F)$, o anel das matrizes 2×2, com coeficientes em F. Então A é uma F-álgebra de dimensão 4. Além disso, se considerarmos

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad k = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

temos que $\{1,i,j,k\}$ é uma base de A sobre F satisfazendo $i^2=1$, $j^2=-1$, $ij=-ji$. Logo, $M_2(F)$ é também uma F-álgebra de quatérnios.

Baseados nos dois exemplos acima, podemos observar que uma álgebra de quatérnios generalizada pode ou não, ser uma álgebra com divisão. O teorema que se segue, estabelece uma condição necessária e suficiente para que tal álgebra seja com divisão.

1.4 - TEOREMA - $Q_F(\alpha,\beta)$ é uma álgebra com divisão se e somente se a equação $x^2-\alpha y^2 = \beta$ não admite solução em F.

DEMONSTRAÇÃO

Suponhamos que existam a, b $\in$ F tais que $a^2-\alpha b^2 = \beta$. Consideremos então $q = a+bi+j$ e $q^* = a-bi-j$.

Temos:

$$q.q^* = (a+bi+j)(a-bi-j) = a^2-b^2\alpha-\beta = 0$$

Como $q,q^* \neq 0$, segue-se que $Q_F(\alpha,\beta)$ possui divisores de zero e portanto não é álgebra com divisão.

Reciprocamente, suponhamos que a equação $x^2-\alpha y^2 = \beta$ não admita solução em F. Devemos mostrar que $Q_F(\alpha,\beta)$ é álgebra com divisão. Dividiremos a demonstração deste fato em vários passos:

1º PASSO - Mostraremos inicialmente que nas hipóteses do teorema, α não é quadrado de nenhum elemento de F.

Suponhamos que exista a $\in$ F tal que $\alpha=a^2$. Se considerarmos $x_o = \frac{\beta+1}{2}$ e $y_o = \frac{\beta-1}{2a}$, teremos que $x_o^2 - \alpha y_o^2 = \beta$.

Assim, a equação $x^2 - \alpha y^2 = \beta$ admite solução em F, o que é uma contradição.

2º PASSO - Todo elemento não nulo de $Q_F(\alpha,\beta)$, da forma $q=a+bi$

é inversível em F(i).

De fato, seja $0 \neq q = a+bi \in F(i)$ e consideremos $q^* = a-bi$. Então $q.q^* = a^2-\alpha b^2$. Como pelo 1º passo α não é quadrado em F, temos que ou $b=0$ ou $b \neq 0$ e $a^2-\alpha b^2 \neq 0$. Se $b=0$ então $0 \neq q \in F$ é inversível em F. Se $b \neq 0$ e $a^2-\alpha b^2 \neq 0$, temos que

$$q.\frac{q^*}{a^2-\alpha b^2} = 1 \text{ , donde } q^{-1} = \frac{q^*}{a^2-\alpha b^2} \in F(i), \text{ com o}$$

que concluímos a prova do 2º passo.

<u>3º PASSO</u> - Todo elemento de $Q_F(\alpha,\beta)$ da forma $a + bi + j$ é inversível em $Q_F(\alpha,\beta)$.

De fato, seja $q = a+bi+j \in Q_F(\alpha,\beta)$ e consideremos $q^* = a-bi-j$. Então

$q.q^* = a^2-\alpha b^2 - \beta \neq 0$, pois a equação $x^2-\alpha y^2 = \beta$ não admite solução em F. Logo, $q^{-1} = \dfrac{q^*}{a^2-\alpha b^2-\beta} \in Q_F(\alpha,\beta)$ e temos

$q.q^{-1} = q^{-1}.q = 1$, donde q é inversível em $Q_F(\alpha,\beta)$.

<u>4º PASSO</u> - Todo elemento não nulo de $Q_F(\alpha,\beta)$ é inversível.

Seja $0 \neq q = a+bi+cj+dk$. Se $c+di=0$, então como $cj+dk = (c+di)j$, temos que $q = a+bi$ e portanto é inversível em $Q_F(\alpha,\beta)$.

Se $c+di \neq 0$ então pelo 2º passo, $c+di$ é inversível

em $F(i)$. Logo, temos:

$$(c+di)^{-1}q = (c+di)^{-1}[(a+bi)+(c+di)j] = (c+di)^{-1}(a+bi)+j$$

Como $(c+di)^{-1}(a+bi)$ é da forma $x+yi$, com $x,y \in F$, pelo 3º passo segue-se que $(c+di)^{-1}(a+bi)+j$ é inversível em $Q_F(\alpha,\beta)$. Consequentemente, q é inversível em $Q_F(\alpha,\beta)$.

Portanto, se a equação $x^2-\alpha y^2 = \beta$ não admite solução em F, $Q_F(\alpha,\beta)$ é álgebra com divisão. $\square$

Daqui por diante, caminharemos no sentido de classificar as álgebras simples de dimensão 4 sobre seu centro. Começaremos mostrando que $Q_F(\alpha,\beta)$ é uma F-álgebra simples central.

Depois, mostraremos que se A é uma F-álgebra simples central de dimensão 4 sobre F, então existem $0 \neq \alpha, \beta \in F$ tais que $A = Q_F(\alpha,\beta)$.

1.5 - <u>PROPOSIÇÃO</u> - Seja $A = Q_F(\alpha,\beta)$ uma álgebra de quatérnios sobre F. Então A é uma F-álgebra simples central.

<u>DEMONSTRAÇÃO</u>

Mostraremos, inicialmente, que $F = Z(A)$, o centro de A.

Seja $q = a+bi+cj+dk \in Z(A)$. Então $qi = iq$, donde

se conclui facilmente que $c=d=0$. Logo, $q = a+bi \in Z(A)$. Novamente, como $q.j=j.q$ segue-se que $b=0$. Assim $q = a \in F$ e portanto $Z(A) \subseteq F$. A inclusão contrária é imediata.

Provaremos agora que A é simples. Seja $(0) \neq I$ um ideal (bilateral) de A. Queremos mostrar que $I=A$. Para isto será suficiente provar que I contém um elemento não nulo de F.

Seja então $q = a+bi+cj+dk$ um elemento não nulo de I. Se $q \notin F$, pelo menos um dos coeficientes b, c ou d deve ser diferente de zero. Suponhamos que $b \neq 0$. Então $[q,j]= qj-jq= =2(bi+dk)j \in I$ pois I é ideal bilateral. Como car $F\neq 2$, $j^2=\beta\in F$ e $\beta\neq 0$, temos que $y = bi+dk \in I$. Assim $yi+iy = 2b\alpha \in F\cap I$ e $2b\alpha\neq 0$. Consequentemente, se $b\neq 0$, I contém um elemento não nulo de F e portanto $I=A$.

Os casos $c\neq 0$ e $d\neq 0$ são análogos e omitiremos a demonstração.

Portanto A é uma F-álgebra simples central, como queríamos provar. □

O lema que se segue é um primeiro passo no sentido de demonstrar a recíproca da proposição anterior. Daqui por diante, F designará sempre um corpo de característica diferente de 2.

1.6 - <u>LEMA</u> - Seja D uma álgebra com divisão de dimensão 4 sobre seu centro F. Então D é uma álgebra de quatérnios sobre F.

DEMONSTRAÇÃO

Novamente, a prova deste resultado será feita em vários passos.

1º PASSO - Mostraremos que todo elemento de D é algébrico sobre F de grau menor ou igual a 2.

É claro que todo elemento $a \in D$ satisfaz um polinômio de grau menor ou igual a 4, com coeficientes em F, pois $(1,a,a^2,a^3,a^4)$ são linearmente dependentes sobre F.

Suponhamos que exista $a \in D$ tal que o polinômio minimal de a seja de grau 4. Então $(1,a,a^2,a^3)$ são linearmente independentes sobre F e como $[D:F] = 4$, segue-se que $(1,a,a^2,a^3)$ é base de D sobre F. Mas isto implica que D é comutativa, o que é uma contradição.

Logo, todo elemento de D satisfaz um polinômio de grau menor ou igual a 3.

Novamente, se para algum $a \in D$ o polinômio minimal de a é de grau 3, então $(1,a,a^2)$ são linearmente independentes sobre F e existe $b \in D$ tal que $b \notin F(a)$.

Neste caso, segue-se facilmente que $(1,a,a^2,b,ab,a^2b)$ são linearmente independentes sobre F, o que é uma contradição.

Logo, todo elemento de D é algébrico sobre F de grau

menor ou igual a dois.

<u>2º PASSO</u> - Dados $a \in D$, $a \notin F$ e $b \notin F(a)$ temos que $(1,a,b,ab)$ é base de D sobre F.

Sejam $a,b \in D$ nas condições acima e consideremos $\alpha_o, \alpha_1, \alpha_2, \alpha_3 \in F$ tais que

$$\alpha_o + \alpha_1 a + \alpha_2 b + \alpha_3 ab = 0$$

Então:

$$\alpha_o + \alpha_1 a = -(\alpha_2 + \alpha_3 a)b$$

Se $\alpha_2+\alpha_3 a \neq 0$ então $\alpha_2+\alpha_3 a$ é inversível em $F(a)$ e teríamos $b \in F(a)$, contradição. Logo $\alpha_2+\alpha_3 a = 0$. Como $(1,a)$ é base de $F(a)$ sobre F, temos que $\alpha_2=\alpha_3=0$. Mas então $\alpha_o+\alpha_1 a= 0$ e novamente, $\alpha_o=\alpha_1=0$.

Assim $(1,a,b,ab)$ são linearmente independentes sobre F. Como $[D:F] = 4$, segue-se que $(1,a,b,ab)$ é base de D sobre F.

<u>3º PASSO</u>: D é uma álgebra de quatérnios sobre F.

Seja $a \in D$, $a \notin F$. Então $(1,a)$ é base de $F(a)$ sobre F, pelo primeiro passo.

Consideremos ainda $b \in D$, $b \notin F(a)$. Pelo 2º passo ,

$(1,a,b,ab)$ é base de D sobre F. Além disso sabemos que o polinômio minimal de b (que indicaremos por m_b) sobre F é de grau 2.

Como car $F \neq 2$, podemos supor que

$$m_b = x^2 + 2\,\delta x + \gamma, \qquad \text{onde } \delta,\ \gamma \in F.$$

Consideremos $j = b+\delta$. Então $j \notin F(a)$ pois $b \notin F(a)$. Pelo 2º passo, $(1,a,j,aj)$ é base de D sobre F. Além disso,

$$0 \neq j^2 = (b+\delta)^2 = b^2+2\delta b+\delta^2 = -\gamma+\delta^2 = \beta \in F$$

Seja agora $j_o = a^{-1}ja$. Se $j_o=j$, então a comuta com j e como $\{1,a,j,aj\}$ é base de D sobre F, teríamos que D é comutativa, contradição. Assim, $j_o \neq j$. Por outro lado, $j_o^2=j^2\in F$. Logo, se tomarmos $c=j-j_o$, temos que $c\neq 0$ e $cj+j_oc = (j-j_o)j + +j_o(j-j_o) = 0$. Portanto

$$-j = c^{-1}\,a^{-1}\,jac = (ac)^{-1}\,jac.$$

Consideremos então $i=ac$. Por construção, $ij=-ji$.

Ainda, se $i \in F$ ou $j \in F(i)$ então j comuta com i . Consequentemente, teríamos:

$$-j = i\,j\,i^{-1} = j, \qquad \text{donde } j=0 \text{ pois car}(F)\neq 2.$$

Logo, $i \notin F$ e $j \notin F(i)$.

Novamente, pelo 2º passo, segue-se que $\{1,i,j,ij\}$ é base de D sobre F.

Para mostrarmos que D é álgebra de quatérnios sobre F, é suficiente agora, verificar que $i^2 \in F$, já que $i \neq 0$.

Para isto, consideremos o polinômio minimal de i sobre F, que denotamos por m_i, e que é da forma:

$$m_i = x^2 + 2\eta x + \rho, \quad \text{com} \quad \eta, \rho \in F.$$

Como $-i = j^{-1}ij$, é fácil verificar que $-i$ é também raiz de m_i. Logo

$$i^2 + 2\eta i + \rho = i^2 - 2\eta i + \rho = 0$$

Portanto $2i^2 + 2\rho = 0$ e temos que $i^2 = -\rho \in F$.

Assim, $\{1,i,j,ij\}$ é base de quatérnios de D sobre F, com o que concluímos a demonstração. $\square$

1.7 - <u>TEOREMA</u> - Seja A uma álgebra simples central de dimensão 4 sobre seu centro F. Então A é uma álgebra de quatérnios sobre F.

<u>DEMONSTRAÇÃO</u>

Como A é simples de dimensão finita sobre seu centro então, pelo teorema de Wedderburn [cf. 5, Teorema 2.16] ,

$A \simeq M_n(D)$, para algum inteiro positivo n e algum anel com divisão D. Consequentemente, computando dimensões, temos:

$$4 = [A:F] = [M_n(D):F] = n^2 \, [D:F].$$

Logo, n=1 ou n=2. Se n=1 então $A \simeq D$ e portanto A é álgebra com divisão de dimensão 4 sobre seu centro F. Pelo lema (1.6) segue-se que A é álgebra de quatérnios sobre F. Se n=2 então D=F e portanto $A \simeq M_2(F)$. Pelo exemplo (1.3), segue-se também que A é uma álgebra de quatérnios sobre F. $\square$

Observemos que da demonstração do teorema anterior segue-se que uma álgebra de quatérnios (generalizada) sobre F ou é álgebra com divisão ou é isomorfa a $M_2(F)$, o anel de matrizes 2×2 com coeficientes em F.

§ 2 - ALGUMAS CARACTERIZAÇÕES DAS ÁLGEBRAS DE QUATÉRNIOS COM DIVISÃO.

Consideremos D uma álgebra de quatérnios sobre F, com base $\{1,i,j,k\}$. Um elemento $q \in D$ diz-se um quatérnio puro se se escreve na forma $q = ai+bj+ck$, com $a,b,c \in F$. Para todo quatérnio puro q tem-se que $q^2 \in F$. Além disso se q_1, q_2 são quatérnios puros e $q_1+q_2 \neq 0$ então (q_1+q_2) é também quatérnio puro e portanto $(q_1+q_2)^2 \in F$. Reciprocamente é fácil verificar que se $u \in D$ é tal que $u^2 \in F$ então ou $u \in F$ ou u é quatérnio

puro. Assim, se considerarmos

$$D' = \{x \in D \mid x^2 \in F \text{ e } x \notin F\} \cup \{0\}$$

teremos que D' é um subgrupo aditivo de D, não trivial.

Neste parágrafo mostraremos que este fato caracteriza as álgebras de quatérnios com divisão.

Além disso, se D é uma F-álgebra de quatérnios com divisão, é fácil verificar que dados q_1, $q_2 \in D$, $(q_1q_2-q_2q_1)^2 \in F$, isto é, o polinômio $f(x,y) = (xy-yx)^2 \in F\{x,y\}$ é central em D.

Por outro lado, se D é uma álgebra com divisão tal que

$$g(x,y,z) = (xy-yx)^2 z - z(xy-yx)^2 \in F\{x,y,z\}$$

é uma identidade polinomial para D de grau mínimo então pelo teorema de Kaplamsky, [5, Teorema 6.3.1] temos que $[D:Z] = n^2$ onde $n \leq \frac{1}{2}(\partial g)$. Logo, temos que $[D:Z] \leq 4$; donde $[D:Z] = 1$ ou 4. Como $g(x,y,z)$ é uma identidade de grau mínimo para D, segue-se que $[D:Z] \neq 1$ (pois se $[D:Z] = 1$, então D satisfaz $h(x,y) = xy-yx \in F\{x,y\}$ que é de grau 2). Assim, $[D:Z] = 4$ e portanto D é álgebra de quatérnios sobre F.

Neste parágrafo, determinaremos ainda as álgebras com divisão D de centro F que verificam $(xy-yx)^{n(x,y)} \in F$ (pa

ra algum inteiro positivo $n=n(x,y))$ $\forall$ $x,y \in D$.

Começaremos com alguns lemas.

2.1 - LEMA - Seja D um anel com divisão de centro F. Consideremos

$$D' = \{x \in D \mid x^2 \in F \text{ e } x \notin F\} \cup \{0\}$$

Se D' é um subgrupo aditivo de D não trivial então D' é um F-espaço vetorial (à esquerda) e $\dim_F D' > 1$.

DEMONSTRAÇÃO

O fato de que D' é um F-espaço vetorial decorre trivialmente.

Suponhamos por absurdo que $\dim_F D' = 1$ e seja $\{v\}$ uma base de D' sobre F. Consideremos $V = F + D' \subset D$. Como $F \cap D' = (0)$, segue-se que $V = F \oplus D'$. Além disso $F \oplus D' \not\subseteq F$ pois $D' \not\subseteq F$. Afirmamos que V é invariante por todos os automorfismos internos de D.

De fato, seja $d \in D$, $d \neq 0$ e consideremos $x = k+\lambda v$, $k, \lambda \in F$, um elemento arbitrário de V. Então:

$$dxd^{-1} = d(k+\lambda v)d^{-1} = dkd^{-1} + d(\lambda v)d^{-1} = k + d(\lambda v)d^{-1}$$

É fácil verificar que $d(\lambda v)d^{-1} \notin F$, pois $v \notin F$. Além

disso

$$\left[d(\lambda v)d^{-1}\right]^2 = d(\lambda v)^2 d^{-1} = (\lambda v)^2 \text{ , pois } (\lambda v)^2 \in F$$

Assim, $V = F \oplus D'$ é invariante por todos os automorfismos internos de D.

Por outro lado, é fácil verificar que V é um subanel de D.

Podemos aplicar então o teorema de Brauer-Cartan - Hua [cf. 10, pág. 186] , e concluímos que $D = F \oplus D'$. Logo, todo elemento de D se escreve na forma $d = k+\lambda v$, onde $k, \lambda \in F$ e $v \in D'$, o que implica facilmente que D é comutativo. Mas neste caso, $D=F$ e $D' = \{x \in D \mid x^2 \in F \text{ e } x \notin F\} \cup \{0\} = \{0\}$, contradição. □

2.2 - <u>TEOREMA</u> - Seja D um anel com divisão de centro F, $\mathrm{car}F \neq 2$. Então D é uma álgebra de quatérnios sobre F se e somente se

$$D' = \{x \in D \mid x^2 \in F \text{ e } x \notin F\} \cup \{0\}$$

é um subgrupo aditivo de D, <u>não trivial</u>.

<u>DEMONSTRAÇÃO</u>

Se D é uma F-álgebra de quatérnios com base $\{1,i,j,k\}$ então é fácil ver que

$$\{x \in D \mid x^2 \in F \text{ e } x \notin F\} = \{ai+bj+ck \mid a,b,c \in F\}$$

Logo, a afirmação decorre imediatamente.

A demonstração da recíproca será feita em vários passos.

<u>1º PASSO</u> - Existem elementos $u,v \in D'$ tais que (u,v,uv) são linearmente independentes sobre F e $uv = -vu$.

Consideremos $Q:D' \longrightarrow F$ a aplicação definida por $Q(x)=x^2$. para todo $x \in D'$. Seja ainda $B(x,y)= \frac{1}{2}(Q(x+y)-Q(x)-Q(y))$ a forma bilinear associada à forma quadrática Q. Observemos que $B(x,y)=\frac{1}{2}(xy+yx)$, donde $B(x,y) = 0$ se e só se $xy = -yx$.

Pelo lema (2.1), sabemos que $\dim_F D' > 1$. Logo, existem $u,v' \in D'$ linearmente independentes sobre F. Definimos:

$$a = \frac{B(u,v')}{Q(u)} \in F \quad \text{e} \quad v = au-v'$$

Então $v \neq 0$ pois (u,v') são linearmente independentes sobre F. Além disso, $v \in D'$ pois $au \in D'$ e $v' \in D'$.

Por outro lado, um cálculo simples mostra que $B(u,v)=0$ donde decorre que $uv = -vu$.

O fato de que (u,v,uv) são linearmente independentes sobre F segue trivialmente pois $B(u,uv) = B(v,uv) = B(u,v)=0$.

Resta portanto mostrar que $uv \in D'$. Mas $uv=-vu$; logo temos:

$$(uv)^2 = (uv)(uv) = u(vu)v = u(-uv)v = -u^2v^2$$

Assim, como $u,v \in D'$, segue-se que $(uv)^2 \in F$. Além disso, $uv \notin F$, pois caso contrário teríamos:

$$0 = B(u,v) = B(u, \frac{uv.u}{u^2}) = \frac{uv}{u^2} B(u,u) = 2uv$$

o que é absurdo, já que D é álgebra com divisão e u,v são não nulos.

<u>2º PASSO</u> - $\dim_F D' = 3$

Seja V o subespaço de D' gerado por (u,v,uv), onde u,v satisfazem as condições do 1º passo. Então $\dim_F V = 3$.

Se $V \subsetneq D'$ então existe $w \in D'$ tal que $w \notin V$. Consideremos $W = V+F.w$; então (u,v,uv,w) é base de W sobre F. Seja

$$t = w - \frac{B(u,w)}{B(u,u)} u - \frac{B(v,w)}{B(v,v)} v - \frac{B(uv,w)}{B(uv,uv)} uv.$$

Então $t \in W$ e $t \neq 0$.

Além disso, é fácil verificar que $B(t,u) = B(t,v) = B(t,uv) = 0$.

Assim, temos:

$$t(uv) = (tu)v = (-ut)v = u(-tv) = u(vt) = (uv)t.$$

Por outro lado, $t(uv) = -(uv)t$. Logo $2uvt=0$, donde $uvt=0$, contradição.

Assim, $V = D'$ e portanto $\dim_F D' = 3$.

<u>3º PASSO</u> - $D = F \oplus D'$ e portanto D é uma F-álgebra de quatérnios, com base $(1,u,v,uv)$.

É claro que $F + D'$ é um subanel de D e que $F+D' \not\subset F$. Além disso $F + D'$ é invariante por todos os automorfismos internos de D, pois F é fixo e D' é invariante. Logo, pelo teorema de Brauer-Cartan-Hua [10, pág. 186], segue-se que $D=F \oplus D'$ e portanto D é uma F-álgebra de quatérnios.

$\square$

O teorema que se segue é uma aplicação de um resultado de Herstein-Procesi-Schacher, cuja demonstração pode ser encontrada no apêndice desta dissertação.

2.3 - <u>TEOREMA</u> - Seja D um anel com divisão de centro F tal que dados $x,y \in D$ existe um inteiro positivo $n=n(x,y)$ satisfazendo $(xy-yx)^{n(x,y)} \in F$. Então ou D é um corpo ou D é álgebra de quatérnios sobre F.

<u>DEMONSTRAÇÃO</u>

Seja $F\{x,y\}$ o anel dos polinômios nas variáveis não comutativas x e y, com coeficientes em F. Consideremos

$f(x,y) = xy-yx \in F\{x,y\}$. Então D e f satisfazem as hipóteses do teorema de Herstein-Procesi-Schacher (ver apêndice, teor. (11.7)). Assim, segue-se que $[D:F] = n^2$ onde $n \leq \frac{1}{2}(\partial f+2)$. Como $\partial f = 2$, temos que $n \leq 2$. Portanto $[D:F] = 1$ ou $[D:F] = 4$. Logo, ou D é um corpo ou, pelo lema (1.6), D é álgebra de quatérnios sobre F.

$\square$

CAPÍTULO II

ANÉIS COM INVOLUÇÃO E ÁLGEBRAS DE QUATÉRNIOS

Este capítulo compõe-se de duas partes, relativamente independentes.

Na primeira parte, estudaremos certas propriedades de anéis com involução, que nos fornecerão algumas caracterizações das álgebras de quatérnios generalizadas. Para isto, as referências básicas são [6] e [7].

Na segunda parte, demonstraremos um resultado de A.A.Albert, que caracteriza os anéis com divisão, com involução, de dimensão 16 sobre seu centro. Duas foram as razões que nos levaram a incluir tal resultado neste texto.

1ª.) Este teorema originou a famosa conjectura de Al

bert, já citada na introdução desta dissertação e que será objeto de estudo no capítulo III.

2ª.) A demonstração aqui apresentada e que se deve a L.H.Rowen, é bem mais simples que a prova original de Albert.

Para esta segunda parte, as referências básicas são [1] e [15].

§ 3 - ANÉIS SIMPLES COM INVOLUÇÃO: ALGUMAS CARACTERIZAÇÕES.

Em todo este parágrafo, R denotará um anel associativo, não necessariamente com unidade, cujo centro indicaremos por $Z = Z(R)$.

3.1 - DEFINIÇÃO - Uma aplicação $*:R \to R$ diz-se uma involução em R se $*$ é um anti-automorfismo de R de grau 2, isto é, se $*$ verifica as seguintes condições:

$$(a+b)^* = a^* + b^*$$

$$(a.b)^* = b^* . a^*$$

$$(a^*)^* = a \qquad \forall\, a,b \in R.$$

Diz-se que $*$ é do 1º tipo se $\alpha^* = \alpha$, para todo elemento $\alpha \in Z(R)$; caso contrário $*$ diz-se do 2º tipo.

Um elemento $x \in R$ diz-se $*$-simétrico se $x^*=x$ e $*$-an

ti-simétrico se $x^*=-x$.

Em todo este capítulo denotaremos por $S=\{x\in R|x^*=x\}$ o conjunto dos elementos de R *-simétricos, e por $K=\{x\in R|x^* = -x\}$ o conjunto dos elementos de R *-anti-simétricos.

Observemos que se R é um anel simples de característica diferente de 2, com involução *, então $R=S+K$ (como conjuntos) e $S\cap K=\{0\}$. Se assumirmos ainda que * é do 1º tipo, então é fácil ver que $R=S\oplus K$, como $Z(R)$-módulos.

3.2 - EXEMPLO - Seja F um corpo de característica diferente de 2 e consideremos $A = Q_F(\alpha,\beta)$ uma F-álgebra de quatérnios. Consideremos ainda $\{1,i,j,k\}$ uma base de quatérnios de A sobre F.

A aplicação que a cada elemento $q = a+bi+cj+dk$ de $Q_F(\alpha,\beta)$ associa $\bar{q} = a-bi-cj-dk$ é uma involução em A.

Além disso, temos que:

$$S = \{q\in A|\bar{q} = q\} = F$$

e

$$K = \{q\in A|\bar{q} = -q\} = \{ai+bj+ck|a,b,c\in F\}$$

Logo, esta involução é do 1º tipo.

□

3.3 - DEFINIÇÃO - Um subgrupo aditivo $U\subset R$ diz-se um ideal de Lie de R se para todo par de elementos $x \in R$ e $u \in U$ temos que

$[x,u] = xu-ux \in U$.

3.4 - <u>TEOREMA</u> (Herstein, [6]) - Seja R um anel simples de característica diferente de 2, com involução *. Seja <S> o subanel gerado por S. Se <S> $\neq$ R então ou R é um corpo ou R é uma álgebra de quatérnios sobre seu centro.

<u>DEMONSTRAÇÃO</u>

Faremos a demonstração deste resultado em vários passos.

<u>1º PASSO</u> - Mostraremos que <S> é um ideal de Lie de R.

Para isto devemos provar que dados $x \in$ <S> e $r \in R$ então $[x,r] = xr - rx \in$ <S>. Já vimos que r se escreve na forma

$$r = r_1 + r_2 \quad , \quad \text{com} \quad r_1 \in S \quad \text{e} \quad r_2 \in K.$$

Então

$$[x,r] = [x,r_1] + [x,r_2]$$

Mas $[x,r_1] = xr_1 - r_1x \in$ <S> , pois x e r_1 pertencem ambos a <S>. Para verificarmos que $[x,r_2] \in$ <S>, escrevemos

$$x = \sum_{i_1,\ldots,i_m} s_{i_1} \ldots s_{i_m} \quad , \text{ onde cada } s_{i_k} \in S$$

Vamos mostrar agora que dados $s_1,\ldots,s_m \in S$ e dado $r_2 \in K$ temos que $[s_1 \ldots\ldots s_m, r_2] \in \langle S\rangle$.

Com efeito

$$[s_1 \ldots\ldots s_m, r_2] = [s_1,r_2]s_2 \ldots\ldots s_m + \ldots$$
$$+ s_1 \ldots\ldots s_{i-1}[s_i,r_2]s_{i+1}\ldots s_m +$$
$$+ \ldots + s_1 \ldots\ldots s_{m-1}[s_m,r_2]$$

Mas

$$[s_i,r_2]^* = (s_i r_2 - r_2 s_i)^* = r_2^* s_i^* - s_i^* r_2^* =$$

$$= -r_2 s_i + s_i r_2 = [s_i,r_2]$$

Logo, $[s_i,r_2] \in S$ para todo $i = 1,\ldots,m$. Assim $[s_1\ldots s_m, r_2] \in S$, para todo $s_1,\ldots\ldots s_m \in S$ e para todo $r_2 \in K$.

Portanto

$$[x,r_2] = \sum_{i_1,\ldots i_m} [s_{i_1}\ldots\ldots s_{i_m}, r_2] \in \langle S\rangle$$

Consequentemente, $[x,r] \in \langle S\rangle$.

<u>2º PASSO</u> - R tem centro não trivial.

Como $\langle S\rangle$ é um subanel de R que é um ideal de Lie de R por [6, teorema 1.2] segue-se que $\langle S\rangle = R$ ou $\langle S\rangle \subset Z(R)$. Como por hipótese $\langle S\rangle \neq R$, temos que $\langle S\rangle \subset Z(R)$.

Mostraremos agora que isto implica que $Z(R) \neq (0)$.

De fato, suponhamos por absurdo que $Z(R) = (0)$. Então $S = (0)$ e portanto todo elemento de R é *-anti-simétrico. Mas neste caso, para todo elemento $a \in R$, temos que $a^2 \in S$, donde $a^2 = 0$.

Assim, pelo teorema de Levitsky [12], R contém um ideal nilpotente não nulo, absurdo pois R é simples.

Logo, $Z(R) \neq (0)$. Portanto sendo R simples de centro não trivial, segue-se que R tem unidade.

<u>3º PASSO</u> - R satisfaz a identidade polinomial

$$\left[[x^2,y] \ , \ [x,y]\right] = 0.$$

Seja $a \in R$ um elemento arbitrário. Então a se escreve na forma

$$a = s+k \quad , \qquad \text{com} \quad s \in S \quad \text{e} \quad k \in K.$$

Como $S \subset Z(R)$, temos que a comuta com s. Logo, $(a-s)^2 = a^2-2as+s^2$, donde

$$a^2 - 2as + (s^2-k^2) = 0$$

Mas $s \in Z(R)$ e $s^2-k^2 \in S \subset Z(R)$. Portanto, todo elemento de R satisfaz um polinômio de grau 2, com coeficientes em $Z(R)$.

Consideremos agora $a,b \in R$ arbitrários e sejam $\alpha,\beta \in Z(R)$ tais que

$$a^2 - 2\alpha a + \beta = 0$$

Temos então:

$$0 = [a^2-2\alpha a+\beta,b] = [a^2,b] -2\alpha[a,b]$$

Comutando a igualdade acima com $[a,b]$, obtemos

$$\Big[[a^2,b],\ [a,b]\Big] -2\alpha\Big[[a,b],\ [a,b]\Big] = 0,$$

donde

$$\Big[[a^2,b],\ [a,b]\Big] = 0$$

Logo R satisfaz a identidade polinomial

$$\Big[[x^2,y],[x,y]\Big] = 0$$

<u>4º PASSO</u> - R é um corpo ou R é uma álgebra de quatérnios sobre seu centro.

Pelo 2º passo, R é um anel primitivo, pois é simples com unidade [5, pág. 40].

Além disso, no 3º passo verificamos que R satisfaz uma identidade polinomial de grau 5. Logo, pelo teorema de Kaplansky [5, teorema 6.3.1], segue-se que $[R:Z(R)] = n^2$, onde $n \leq 2$.

Assim $[R:Z(R)] = 1$ ou $[R:Z(R)] = 4$. Se $[R:Z(R)] = 1$ então $R = Z(R)$ é um corpo. Se $[R:Z(R)] = 4$, pelo teorema (1.7), temos que R é uma álgebra de quatérnios sobre seu centro. □

3.5 - OBSERVAÇÃO - Da demonstração do teorema anterior, decorre que se R é um anel simples de característica diferente de 2, com involução * tal que $\langle S \rangle \neq R$, então R tem unidade e $\langle S \rangle \subset Z(R)$. Logo, todo elemento de S não nulo é inversível, pois Z(R) é um corpo.

Uma pergunta que pode-se colocar então é a seguinte: o que se pode concluir sobre R, supondo-se apenas que todo elemento não nulo de S seja inversível? Este é o conteúdo do teorema que se segue, devido a J.M.Osborn.

3.6 - TEOREMA - Seja R um anel simples com unidade de característica diferente de 2, com involução *. Suponhamos que todo elemento não nulo de S seja inversível em R. Então ou R é um anel com divisão ou R é uma álgebra de quatérnios sobre seu centro.

DEMONSTRAÇÃO

Consideremos $\langle S\rangle$, o subanel gerado por S. Se $\langle S\rangle \neq R$, então pelo teorema (3.4), temos que ou R é um corpo ou R é uma álgebra de quatérnios sobre seu centro.

Podemos supor então que $\langle S\rangle = R$. Vamos mostrar que, neste caso, R é um anel com divisão.

Seja x um elemento não nulo de R. Como R é simples de característica diferente de 2, com involução, temos que $x = s+k$, onde $s \in S$ e $k \in K$.

Estudaremos separadamente dois casos.

1º CASO - $s \neq 0$.

Suponhamos por absurdo que x não seja inversível. Então $x.x^*$ e $x^*.x$ não são inversíveis. Como $x.x^*$ e $x^*.x$ são elementos de S, temos que

$$xx^* = x^*x = 0$$

Logo, como car $R \neq 2$ e $xx^* - x^*x = 0$, segue-se facilmente que $sk = ks$. Novamente, como $xx^* = 0$ temos que $s^2 = k^2$, pois agora s e k comutam.

Como $s \in S$ e $s \neq 0$ temos que s é inversível em R e portanto podemos considerar $c = s^{-1}k$.

Dos cálculos acima efetuados, decorre que $c^* = -c$ e $c^2 = 1$.

Vamos mostrar que $c \in Z(R)$. Como $\langle S \rangle = R$, é suficiente provar que c comuta com todo elemento de S.

Seja então $t \in S$ arbitrário. Como $c^* = -c$ e $c^2 = 1$, segue-se facilmente que

$$(1+c)\ t(1-c) \in S \quad e \quad [(1+c)\ t(1-c)]^2 = 0$$

Logo $(1+c)\ t(1-c) = 0$. Analogamente $(1-c)t(1+c) = 0$.

Desenvolvendo os produtos acima e comparando as igualdades obtidas, concluímos que $2(ct-tc) = 0$, donde $ct = tc$, para todo $t \in S$. Assim, $c \in Z(R)$. Como $Z(R)$ é um corpo e $c^2 = 1$, temos que $c = \pm 1$.

Mas $c = s^{-1}k$. Logo $k = \pm s$, absurdo pois $s \neq 0$ e $K \cap S = (0)$. Portanto dado $x \in R$, $x = s+k$ com $s \neq 0$, temos que x é inversível em R.

<u>2º CASO</u> - $s = 0$ (e portanto $x \in K$).

Se existe $t \in S$ tal que $tx \notin K$, então pela parte anterior, tx é inversível, donde x é inversível.

Se para todo $t \in S$ temos que $tx \in K$, então:

$$(tx)^* = -tx = -xt$$

Logo, $tx = xt$, pata todo $t \in S$ e portanto $x \in Z(R)$. Como $Z(R)$ é um corpo, segue-se que x é inversível.

Assim, R é anel com divisão.

□

3.7 - COROLÁRIO - Seja R um anel simples de característica diferente de 2, não comutativo. Então R é uma álgebra de quatérnios sobre seu centro se e somente se existe uma involução $*:R \longrightarrow R$ tal que $\langle S \rangle \neq R$.

DEMONSTRAÇÃO

Se R é uma álgebra de quatérnios sobre seu centro $Z(R)$, então, fixada uma base de quatérnios $\{1,i,j,k\}$ de R sobre $Z(R)$, a aplicação que associa a cada elemento $q=a+bi+cj+dk$ o elemento $\bar{q} = a-bi-cj-dk$; satisfaz as condições exigidas.

A recíproca segue trivialmente do teorema (3.4).

□

§ 4 - INVOLUÇÕES DO PRIMEIRO TIPO: FATOS GERAIS

Em todo este parágrafo, salvo menção explícita em contrário, todas as involuções consideradas serão do primeiro tipo.

Seja R um anel com involução $*$ e consideremos um elemento inversível $r \in R$, tal que $r^* = \pm r$. Então, é fácil verificar que a aplicação

$$J(x) = rx^{*}r^{-1} \quad , \quad x \in R$$

é uma involução em R, do primeiro tipo. Em particular, temos ainda que

$$J(r) = r^{*} = \pm r.$$

A proposição que se segue nos mostra que sob determinadas condições sobre R este processo determina todas as involuções de R.

4.1 - PROPOSIÇÃO - Seja R um anel cujo centro Z(R) é um domínio e tal que todo Z(R)-automorfismo é interno. Sejam ainda ψ e Ψ duas involuções em R. Nestas condições, temos:

(a) Existe um elemento inversível $r \in R$ tal que $\psi(r) = \pm r$ e $\Psi(x) = r\psi(x)\, r^{-1}$, para todo $x \in R$. Além disso, $\psi(r) = \Psi(r)$.

(b) Um elemento $r \in R$ nas condições acima está determinado, salvo multiplicação por elementos de Z(R).

DEMONSTRAÇÃO

Consideremos a aplicação composta $\eta = \Psi o \psi$. Então η é um Z(R)-automorfismo de R, pois ψ e Ψ são involuções do primeiro tipo. Assim, η é um automorfismo interno de R e portanto existe um elemento inversível $r \in R$ tal que

$$\eta(x) = rxr^{-1}, \qquad \text{para todo } x \in R$$

Como $\psi^2 = I$, temos que $\eta o \psi = \Psi$, donde

$$\Psi(x) = r\psi(x)\, r^{-1}, \quad \text{para todo } x \in R$$

Resta portanto mostrar que $\Psi(r) = \psi(r) = \pm r$. Para isto, consideremos um elemento $x \in R$ arbitrário. Então:

$$\left[\psi(r)r^{-1}\right]\Psi(x)\left[\psi(r)r^{-1}\right]^{-1} = \psi(r)\left[r^{-1}\Psi(x)r\right]\psi(r^{-1}) =$$

$$= \psi(r)\psi(x)\psi(r^{-1}) = \psi(r^{-1}xr) = \psi(\psi(\Psi(x))) = \Psi(x)$$

Como Ψ é bijetora, segue-se que $\psi(r)r^{-1} = c \in Z(R)$. Logo $\psi(r) = cr$ e temos:

$$r = \psi(\psi(r)) = c\psi(r) = c^2 r.$$

Como r é inversível, segue-se que $c^2 = 1$. Mas $c \in Z(R)$ e $Z(R)$ é um domínio. Assim, $c = \pm 1$, donde $\psi(r) = \pm r$.

Agora, $\Psi(r) = r\psi(r)r^{-1} = \psi(r)$, com o que concluímos a prova da parte (a).

Para mostrarmos (b), seja $t \in R$ nas condições da parte (a), isto é, suponhamos que

$$\Psi(x) = t\psi(x)t^{-1}, \text{ para todo } x \in R$$

e

$$\psi(t) = \Psi(t) = \pm t.$$

Então dado um elemento $x \in R$ arbitrário, temos:

$$\left[t^{-1}r\right]\psi(x)\left[t^{-1}r\right]^{-1} = t^{-1}\left[r\psi(x)r^{-1}\right]t =$$

$$= t^{-1}\Psi(x)t = t^{-1}(t\psi(x)t^{-1})t = \psi(x)$$

Logo, $t^{-1}r \in Z(R)$, donde existe $\alpha \in Z(R)$ tal que $r = \alpha t$.

$\square$

Seja R um anel nas condições da proposição anterior. Consideremos J_1 e J_2 duas involuções em R. Dizemos que J_1 é equivalente a J_2 (e escrevemos $J_1 \sim J_2$) se existe um elemento inversível $r \in R$ tal que $J_1(r) = r$ e

$$J_2(x) = r\, J_1(x) r^{-1}, \quad \text{para todo } x \in R.$$

Da parte (b) da proposição anterior segue-se que a relação acima está bem definida. Além disso, é fácil verificar que se trata de uma relação de equivalência.

Assim, dado um anel R nas condições da proposição anterior, existem <u>no máximo</u> duas classes de equivalência de involuções.

4.2 - <u>EXEMPLO</u> - Seja F um corpo e consideremos $R = M_n(F)$ o anel das matrizes $n \times n$ com coeficientes em F. A aplicação $t: M_n(F) \longrightarrow M_n(F)$ que associa a cada matriz $A = (a_{ij})$ a sua <u>transposta</u> $A^t = (b_{ij})$, onde $b_{ij} = a_{ji}$, $1 \leq i,j \leq n$ é uma involução em R, do primeiro tipo.

Se $n = 2m$, definimos também a involução <u>simplética</u>, da seguinte forma: a cada matriz

$$X = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in M_n(F) \quad , \quad \text{onde } A,B,C,D \in M_m(F),$$

associamos a matriz

$$X^s = \begin{bmatrix} D^t & -B^t \\ -C^t & A^t \end{bmatrix} \in M_n(F)$$

Consideremos $U = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \in M_n(F)$,

onde I denota a matriz identidade de $M_m(F)$.

É fácil ver que U é inversível e que

$$U^t = U^s = -U = U^{-1}$$

Além disso, um cálculo explícito mostra que

$$X^s = U\, X^t\, U^{-1} \, , \qquad X \in M_n(F)$$

Assim, se $n=2m$ e car $F \neq 2$, temos que as involuções (t) e (s) são <u>não</u> equivalentes em $M_n(F)$.

Consideremos novamente um anel R nas condições da proposição (4.1), e seja J uma involução em R. Denotaremos por (R,J) o par formado pelo anel R, munido da involução J.

Diremos ainda que (R,J_1) é isomorfo a (R,J_2) (e escreveremos $(R,J_1) \simeq (R,J_2)$) se existe um $Z(R)$-isomorfismo $\psi: R \to R$ que preserva a involução, isto é, tal que

$$\psi(J_1(x)) = J_2(\psi(x)) \quad , \quad \text{para todo} \quad x \in R.$$

Nosso objetivo será demonstrar que se F é um corpo algébricamente fechado de característica diferente de 2, e $R = M_n(F)$ denota o anel das matrizes $n \times n$ com coeficientes em F, então dadas duas involuções J_1 e J_2 em $M_n(F)$, temos que:

$$J_1 \sim J_2 \quad \text{se e somente se} \quad (M_n(F),J_1) \simeq (M_n(F),J_2)$$

Para isto, observemos que uma classe de equivalência de involuções em $M_n(F)$ está representada pela transposição. A outra existe se e somente se existirem matrizes anti-simétricas (em relação a transposição) inversíveis em $M_n(F)$.

Consequentemente, existirão duas classes de equivalência de involuções em $M_n(F)$ se e somente se n for par e car(F) $\neq 2$, (já que o determinante de uma matriz anti-simétri-

ca de ordem ímpar é zero).

Nesta situação, isto é, se n for par e car(F) $\neq 2$, então a outra classe de equivalência estará representada pela involução simplética, já introduzida no exemplo (4.2).

Com estas considerações, estamos em condições de demonstrar o resultado acima mencionado.

4.3 - PROPOSIÇÃO - Seja F um corpo algebricamente fechado de característica diferente de 2 e consideremos $M_n(F)$ o anel das matrizes n×n com coeficientes em F. Dadas duas involuções J_1 e J_2 em $M_n(F)$, temos que $J_1 \sim J_2$ se e somente se $(M_n(F), J_1) \simeq (M_n(F), J_2)$.

DEMONSTRAÇÃO

Suponhamos $(M_n(F), J_1) \simeq (M_n(F), J_2)$. Então existe um F-automorfismo ψ de $M_n(F)$ tal que

$$\psi(J_1(X)) = J_2(\psi(X)) \quad , \quad \text{para todo } X \in M_n(F)$$

Como $M_n(F)$ é simples, pelo teorema de Skolem-Noether [5, teorema 4.3.1] segue-se que ψ é um automorfismo interno. Assim, existe um elemento inversível $S \in M_n(F)$ tal que

$$\psi(X) = SXS^{-1} \quad , \quad \text{para todo } X \in M_n(F).$$

Seja $A = S.J_1(S) \in M_n(F)$. Então A é inversível e $J_1(A) = A$. Além disso, temos:

$$AJ_1(X)A^{-1} = SJ_1(S)J_1(X)J_1(S^{-1})S^{-1} =$$

$$= SJ_1(S^{-1}XS)S^{-1} =$$

$$= \psi(J_1(S^{-1}XS)) = J_2(\psi(S^{-1}XS)) =$$

$$= J_2(X) \quad , \quad \text{para todo } X \in M_n(F).$$

Logo, $J_1 \sim J_2$.

Sejam agora J_1 e J_2 involuções <u>equivalentes</u> em $M_n(F)$. Dividiremos a demonstração da recíproca em dois casos:

<u>1º CASO</u> - Se $J_1 \sim t$, onde t denota a transposição então

$$(M_n(F), J_1) \simeq (M_n(F), t)$$

Como $J_1 \sim t$ existe um elemento inversível $A \in M_n(F)$ tal que

$$A^t = A \quad e \quad J_1(X) = AX^tA^{-1} \quad , \text{ para todo } X \in M_n(F)$$

Sendo A uma matriz simétrica inversível, por [9 , pág. 317], existe uma matriz inversível M tal que

$$M^t AM = I$$

onde I denota a matriz identidade de $M_n(F)$.

Logo $A = N.N^t$, onde $N = M^{-1}$. Definimos então:

$$\psi(X) = NX\,N^{-1}, \quad \text{para todo } X \in M_n(F).$$

Assim, ψ é um F-automorfismo de $M_n(F)$ e

$$J_1(\psi(X)) = J_1(NX\,N^{-1}) = A(NXN^{-1})^t\,A^{-1} =$$

$$= A(N^{-1})^t\,X^t\,N^t\,A^{-1} = NX^t\,N^{-1} = \psi(X^t)$$

Portanto, $(M_n(F),J_1) \simeq (M_n(F),t)$.

Observemos que se existe apenas <u>uma</u> classe de equivalência de involuções em $M_n(F)$, então a proposição decorre facilmente do 1º caso. Assim, podemos supor que existem exatamente <u>duas</u> classes de equivalência de involuções em $M_n(F)$. Logo $n=2m$ e a segunda classe está representada pela involução <u>simplética</u>, que denotamos por s.

<u>2º CASO</u> - Se $J_1 \sim s$ então

$$(M_n(F),J_1) \simeq (M_n(F),s)$$

Como $J_1 \sim s$, existe uma matriz inversível $A \in M_n(F)$ tal que $A^s = A$ e $J_1(X) = AX^sA^{-1}$, para todo $X \in M_n(F)$.

Observemos ainda que como $A^s = A$ então A se escreve

na forma

$$A = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_1^t \end{bmatrix} \quad \text{onde } A_1, A_2, A_3 \in M_m(F),$$

$$A_2^t = -A_2 \quad \text{e} \quad A_3^t = -A_3$$

Consideremos agora $U = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \in M_n(F)$, onde I denota a matriz identidade de $M_m(F)$. Então $(AU)^t = -(AU)$. Além disso, AU é inversível; logo por [9, pág. 325] existe uma matriz inversível $V \in M_n(F)$ tal que

$$V(A.U)\ V^t = U$$

Assim

$$A.U = (V^{-1})\ U(V^{-1})^t \qquad \text{e}$$

portanto

$$A = V^{-1}\ U(V^{-1})^t\ U^{-1}$$

Mas pelo exemplo (4.2) temos que

$$U(V^{-1})^t\ U^{-1} = (V^{-1})^s$$

Consequentemente, $A = (V^{-1})(V^{-1})^s$.

Finalmente, definimos:

$$\psi(X) = V^{-1}\ XV\ , \quad \text{para todo } X \in M_n(F)$$

Então ψ é um F-automorfismo de $M_n(F)$ e

$$J_1(\psi(X)) = J_1(V^{-1}XV) = A(V^{-1}XV)^s A^{-1} =$$

$$= AV^s X^s (V^{-1})^s A^{-1} = V^{-1}X^s V =$$

$$= \psi(X^s)$$

Portanto, $(M_n(F), J_1) \simeq (M_n(F), S)$, com o que concluímos a demonstração. $\square$

Seja agora R uma F-álgebra simples central de grau n (isto é, $[R:F] = n^2$), com involução *. Se $\bar{F}$ denota o fecho algébrico de F então podemos estender * a uma involução em $M_n(\bar{F}) = R \otimes_F \bar{F}$, definindo

$$(\sum_i r_i \otimes \bar{\alpha}_i)^* = \sum_i r_i^* \otimes \bar{\alpha}_i \text{ , onde}$$

$r_i \in R$ e $\alpha_i \in \bar{F}$.

Diremos então que a involução * é do <u>tipo ortogonal</u> (resp., do tipo <u>simplético</u>) se $*\sim t$ (resp., $*\sim s$) em $M_n(\bar{F})$.

Estamos interessados nas involuções do tipo <u>simplético</u>, pois para estas vale o seguinte resultado:

4.4 - <u>PROPOSIÇÃO</u> - Seja $(R,*)$ uma F-álgebra simples central de grau 2n, com involução * do tipo <u>simplético</u>. Então todo elemento *-simétrico de R é algébrico sobre F de grau menor ou igual a n.

DEMONSTRAÇÃO

Consideremos $\bar{F}$ o fecho algébrico de F. Então $M_{2n}(\bar{F}) = R \otimes_F \bar{F}$ e como * é do tipo simplético, temos que *-s em $M_{2n}(\bar{F})$.

Seja $x \in R$ tal que $x^* = x$. Então $X = x \otimes 1$ é *-simétrico. Como $(M_{2n}(\bar{F}),*) \simeq (M_{2n}(\bar{F}),s)$ existe um $\bar{F}$-automorfismo ψ de $M_{2n}(\bar{F})$ tal que

$$\psi(Y^*) = \psi(Y)^s \text{ , para todo } Y \in M_{2n}(\bar{F}).$$

Como $X^* = X$, então $[\psi(X)]^s = \psi(X)$. Assim, $\psi(X) \in M_{2n}(\bar{F})$ é simétrico em relação à involução simplética. Portanto $\psi(X)$ é algébrico sobre $\bar{F}$ de grau menor ou igual a n [11, pág. 230]. Logo X é algébrico sobre $\bar{F}$ de grau menor ou igual a n. Usando agora as propriedades do produto tensorial, segue-se facilmente que x é algébrico sobre F de grau menor ou igual a n.

□

Para concluirmos este parágrafo, gostaríamos de mencionar um resultado de Albert, que caracteriza as álgebras com divisão de dimensão finita sobre seu centro que possuem involução. Este resultado será utilizado no parágrafo 9.

Para isto, precisamos introduzir algumas noções sobre o grupo de Brauer de um corpo F. Os resultados aqui citados podem ser encontrados em [5, pág. 93].

Seja F um corpo e $\mathcal{A}$ o conjunto das F-álgebras sim-

ples centrais de dimensão finita. Dadas duas álgebras A_1 e A_2 $\in \mathcal{A}$, sabemos, pelo teorema de Wedderburn, que existem inteiros positivos m e n e anéis com divisão D_1 e D_2 tais que

$$A_1 \simeq M_m(D_1) \quad \text{e} \quad A_2 \simeq M_n(D_2)$$

Além disso, D_1 e D_2 estão determinados, salvo isomorfismo.

Diremos então que A_1 é <u>similar</u> a A_2 se D_1 é isomorfo a D_2. Pode-se demonstrar que a relação de similaridade é uma relação de equivalência.

Consideremos então $B(F) = \mathcal{A}/\sim$, o conjunto quociente de $\mathcal{A}$ por esta relação e denotemos por $[A]$ a classe de um elemento $A \in \mathcal{A}$ em $B(F)$.

Podemos dar a $B(F)$ uma estrutura de grupo, através da seguinte operação:

$$[A].[B] = [A \otimes_F B] \quad , \qquad A,B \in \mathcal{A}.$$

Pode-se demonstrar que o produto acima está bem definido e que $(B(F),.)$ é um grupo abeliano, de torção; $B(F)$ é chamado o <u>grupo de Brouer de F</u>.

Assim, dada uma F-álgebra simples central A de dimensão finita, definimos o <u>expoente de A</u> como a ordem de $[A]$ no grupo de Brouer de F.

Pode-se demonstrar ainda que se $[A:F] = n^2$ então o expoente de A em B(F) e n possuem os mesmos fatores primos, [5, pág. 120].

De posse destas noções, podemos agora enunciar o teorema de Albert anteriormente mencionado, cuja demonstração pode ser encontrada em [1, pág. 161].

4.5 - TEOREMA - Seja D uma álgebra com divisão de dimensão finita sobre seu centro F. Então D possui uma involução (do 1º tipo) se e somente se o expoente de D no grupo de Brouer de F for 1 ou 2.

Observemos ainda que se D é uma álgebra com divisão de dimensão finita sobre seu centro F, com involução, então $[D:F] = 2^{2m}$, para algum inteiro positivo m, já que os fatores primos do expoente de D em B(F) e de $n = \sqrt{[D:F]}$ são os mesmos.

§ 5 - ÁLGEBRAS COM DIVISÃO DE DIMENSÃO 16 SOBRE SEU CENTRO, COM INVOLUÇÃO

Neste parágrafo utilizaremos os resultados anteriores para classificar as álgebras com divisão de dimensão 16 sobre seu centro, com involução.

Começaremos estudando algumas propriedades das involuções em álgebras com divisão.

5.1 - PROPOSIÇÃO - Seja (D,J) uma álgebra com divisão de centro F, com involução J e consideremos K um F-subcorpo de D não maximal. Se K possui um F-automorfismo ψ de grau 2 então existe um elemento não nulo $y \in D$ (que podemos escolher simétrico ou anti-simétrico em relação a J) tal que

$$\psi(k)^J = y\,k\,y^{-1} \quad , \quad \text{para todo } k \in K.$$

DEMONSTRAÇÃO

Seja K^J a imagem de K pela involução J. Então K^J é um F-subcorpo de D pois J é do 1º tipo. Além disso, $J\circ\psi$ é um F-isomorfismo de K em K^J. Logo, pelo teorema de Skolem - Noether [5, teorema 6.3.1] , existe um elemento não nulo $y_1 \in D$ tal que $(J\circ\psi)\ (k) = y_1 k\, y_1^{-1}$, para todo elemento $k \in K$, ou seja,

$$\psi(k)^J = y_1 k\, y_1^{-1} \quad , \quad \text{para todo } k \in K.$$

Portanto, temos:

$$(y_1^{-1}y_1^J)^{-1}k(y_1^{-1}y_1^J) = (y_1^J)^{-1}(y_1 k y_1^{-1})y_1^J = (y_1^J)^{-1}\ \psi(k)^J\ y_1^J =$$

$$= (y_1^{-1})^J\ \ \psi(k)^J\ y_1^J = (y_1\psi(k)y_1^{-1})^J$$

$$= [\psi(\psi(k))^J]^J = [k^J]^J = k,$$

para todo $k \in K$.

Consideremos $K' = C_D(K)$, o centralizador de K em D.

Então o cálculo acima mostra que $y_1^{-1}\, y_1^J \in K'$, donde $y_1^J \in y_1.K'$. Portanto, $y_1+y_1^J \in y_1K'$ e $y_1-y_1^J \in y_1K'$. Além disso, é claro que podemos substituir y_1 por qualquer elemento não nulo de $y_1.K'$.

Resta portanto mostrar que $y_1.K'$ possui elementos simétricos e anti-simétricos não nulos.

Suponhamos que todo elemento de $y_1.K'$ seja simétrico. Então dado um elemento $a \in K'$ qualquer, temos:

$$(y_1.a)^J = y_1.a = a^J y_1$$

Logo

$$y_1\, a\, y_1^{-1} = a^J, \text{ para todo } a \in K'$$

Sejam agora $a_1, a_2 \in K'$

Então

$$(a_1a_2)^J = a_2^J\, a_1^J = (y_1\, a_2\, y_1^{-1})(y_1\, a_1\, y_1^{-1})$$

$$= y_1(a_2a_1)\, y_1^{-1} = (a_2\, a_1)^J$$

Logo, $a_1\, a_2 = a_2\, a_1$, para todo $a_1, a_2 \in K'$ e portanto K' é comutativo. Mas é fácil ver que nesta situação K é maximal; contradição.

Analogamente mostra-se que y_1K' possui elementos si

métricos não nulos, com o que concluímos a demonstração.

□

5.2 - COROLÁRIO - Sejam (D,J) uma álgebra com divisão de centro F, com involução J e K um F-subcorpo de D não maximal. Suponhamos que K possua um F-automorfismo ψ de grau 2. Então existem involuções J_1 e J_2 em D, de tipo simplético e ortogonal, respectivamente, cujas restrições a K são iguais a ψ.

DEMONSTRAÇÃO

Pela proposição anterior, existem elementos não nulos $y_1, y_2 \in D$ tais que

$$y_1^J = y_1 \ , \quad y_2^J = -y_2 \qquad \text{e}$$

$$\psi(k)^J = y_1 k y_1^{-1} = y_2 k y_2^{-1}, \text{ para todo } k \in K.$$

Dado $x \in D$ arbitrário, definimos:

$$J_1(x) = y_1^{-1} x^J y_1 \qquad \text{e} \qquad J_2(x) = y_2^{-1} x^J y_2.$$

É claro que J_1 e J_2 são involuções em D, não equivalentes. Além disso, dado $k \in K$, temos:

$$k^{J_1} = y_1^{-1} k^J y_1 = y_1^{-1}(y_1 \psi(k) y_1^{-1}) y_1 = \psi(k)$$

Analogamente demonstra-se que $k^{J_2} = \psi(k)$, para todo $k \in K$. $\square$

Finalmente estamos em condições de obter a classificação das álgebras com divisão de dimensão 16 sobre seu centro.

5.3 - TEOREMA - Seja $(D,*)$ uma álgebra com divisão de dimensão 16 sobre seu centro F, de característica diferente de 2, com involução de tipo simplético $*$. Então $D \cong Q_1 \otimes_F Q_2$, onde Q_1 e Q_2 são F-álgebras de quatérnios invariantes sob a involução $*$.

DEMONSTRAÇÃO

Pela proposição (4.4), sabemos que todo elemento de D, simétrico em relação a involução $*$, é algébrico sobre F de grau menor ou igual a 2. Consideremos então um elemento não nulo $d \in D$ tal que $d \notin F$, $d^2 \in F$ e $d^* = d$. Seja $K = F(d)$, o subcorpo de D gerado por F e d. Então $[K:F] = 2$ e existe um F-automorfismo $\psi: K \to K$ de grau 2. Pela proposição (5.2) existe um elemento simétrico não nulo $y \in D$ tal que

$$\psi(d) = y\, d\, y^{-1} = -d.$$

Seja Q_1 a F-álgebra gerada por $\{1, y, d, yd\}$. É fácil verificar que Q_1 é uma álgebra com divisão de dimensão 4 sobre seu cen

tro, que é F. Logo, pelo lema (1.6), segue-se que Q_1 é uma F-álgebra de quatérnios. Além disso é imediato que Q_1 é *-invariante. Consideremos $Q_2 = C_D(Q_1)$, o centralizador de Q_1 em D. É fácil ver que Q_2 é *-invariante. Agora, por [5, teorema 4.4.2] segue-se que $D = Q_1 \otimes_F Q_2$ e computando dimensões, concluímos que $[Q_2:F] = 4$. Logo, Q_2 é uma F-álgebra de quatérnios, com o que concluímos a demonstração.

□

5.4 - COROLÁRIO - Seja D uma álgebra com divisão de dimensão 16 sobre seu centro F, de característica diferente de 2, com involução. Então $D = Q_1 \otimes_F Q_2$, onde Q_1 e Q_2 são F-álgebras de quatérnios.

DEMONSTRAÇÃO

Segue imediatamente do corolário (5.2) e do teorema (5.3).

□

CAPÍTULO III

SOBRE UMA CONJECTURA DE ALBERT

Este capítulo tem por objetivo dar uma resposta negativa à seguinte conjectura de Albert:

"Se D é uma álgebra com divisão de dimensão 2^{2m} sobre seu centro, com involução, então D é isomorfa a um produto tensorial de álgebras de quatérnios?"

Para isto, estudaremos os produtos cruzados abelianos, isto é, produtos cruzados $A = (K|_F G, f)$, onde $G = Gal\ (K|_F)$ é abeliano.

Começamos explorando o fato de G ser abeliano, para caracterizar o produto cruzado (K, G, f) em termos de outros parâmetros, mais convenientes. A seguir, passamos a estudar

produtos cruzados abelianos de grau 8 e estabelecemos uma condição necessária e suficiente para que tais álgebras possuam uma involução do primeiro tipo.

Posteriormente, introduzimos os produtos cruzados abelianos genéricos, que são álgebras com divisão. Esses produtos cruzados são chamados "genéricos", pois todo produto cruzado abeliano é imagem homomorfa de um produto cruzado abeliano genérico.

Por outro lado, mostramos também que todo produto cruzado abeliano genérico é, na realidade, um produto cruzado abeliano, em relação a uma extensão de Galois conveniente.

Aplicamos então os resultados anteriormente obtidos, para construir álgebras com divisão, de grau 8 sobre seu centro, com involução.

Finalmente, estabelecemos uma condição necessária e suficiente sobre os parâmetros, para que este tipo de álgebra seja um produto tensorial de álgebras de quatérnios.

Isto feito, construímos um contra-exemplo à conjectura de Albert, ou seja, exibimos uma álgebra com divisão, de grau 8 sobre seu centro, com involução, não isomorfa a um produto tensorial de álgebras de quatérnios.

As referências básicas para este capítulo são [2] e [3].

§ 6 - PRODUTO TENSORIAL DE ÁLGEBRAS DE QUATÉRNIOS

Em todo este capítulo F designará um corpo de característica diferente de 2 e A uma F-álgebra simples central.

6.1 - DEFINIÇÃO - Um conjunto $S = \{r_i\}_{i \in I} \subset A$ diz-se q-gerador se:

(i) $0 \neq r_i^2 \in F$, $\forall i \in I$

(ii) $r_i r_j = \pm r_j r_i$ $\forall i, j \in I$

(iii) Se $i \neq j$ então existe $r_k \in S$ tal que r_i comuta com r_k e r_j anti-comuta com r_k, isto é, $r_i r_k = r_k r_i$ e $r_j r_k = - r_k r_j$.

6.2 - PROPOSIÇÃO

(a) Todo conjunto q-gerador $S \subset A$ é linearmente independente sobre F.

(b) Se $\{r_1, r_2\}$ é q-gerador então $\{1, r_1, r_2, r_1 r_2\}$ é q-gerador e $Q = F + Fr_1 + Fr_2 + Fr_1 r_2$ é uma F-álgebra de quatérnios.

DEMONSTRAÇÃO

(a) Suponhamos por absurdo que S seja linearmente dependente sobre F. Então entre as relações $\sum_{i=1}^{k} \alpha_i r_i = 0$, com

$\alpha_i \in F$, para todo $i = j,\ldots,k$, em que nenhum coeficiente é nulo, podemos escolher uma de menor comprimento k. É claro que $k \geq 2$ e portanto podemos supor que $\alpha_1, \alpha_2 \neq 0$.

Como S é q-gerador, existe $r \in S$ tal que $r.r_1 = r_1.r$ e $r.r_2 = -r_2.r$.

Temos então:

$$0 = [r, \sum_{i=1}^{k} \alpha_i r_i] = \sum_{i=1}^{k} \alpha_i [r, r_i] \qquad (*)$$

Seja $X = \{m \in \mathbb{N} \mid 1 \leq m \leq k \text{ e } [r, r_m] \neq 0\}$. Notamos que X tem menos de k elementos pois $r_1 \notin X$. Ainda, se $[r, r_m] \neq 0$ então $[r, r_m] = r.r_m - r_m r = 2rr_m$.

Segue-se portanto de (*) que

$$0 = \sum_{i \in X} \alpha_i [r, r_i] = 2 \sum_{i \in X} \alpha_i r r_i$$

Como r é inversível em A e $car(F) \neq 2$, temos que $\sum_{i \in X} \alpha_i r_i = 0$, o que contraria a minimalidade de k.

(b) Se $\{r_1, r_2\}$ é um conjunto q-gerador então, pela condição (iii) da definição (6.1) segue-se que $r_1 r_2 = -r_2 r_1$. Com isto, é fácil ver que $\{1, r_1, r_2, r_1 r_2\}$ é q-gerador e, da parte (a) acima, vem que $Q = F + Fr_1 + Fr_2 + Fr_1 r_2$ é uma F-álgebra de qua-

térnios. $\square$

A proposição que se segue relaciona conjuntos q-geradores com o fato de uma dada álgebra simples central ser um produto tensorial de subálgebras de quatérnios.

6.3 - PROPOSIÇÃO - Suponhamos que $[A:F] = 4^t$. Então A é um produto tensorial de F-álgebras de quatérnios se e somente se A possui um conjunto q-gerador S com 4^t elementos (neste caso, S será uma base de A sobre F).

DEMONSTRAÇÃO

Suponhamos $A = Q_1 \otimes_F \dots \otimes_F Q_t$, onde cada $Q_i, 1 \leq i \leq t$, é uma F-álgebra de quatérnios, com base de quatérnios $\{1, r_{1i}, r_{2i}, r_{1i} \cdot r_{2i}\}$. Denotemos por $r_{0i} = 1$ e $r_{3i} = r_{1i} r_{2i}$, $1 \leq i \leq t$.

Consideremos

$$S = \{r_{i_1 1} \otimes r_{i_2 2} \otimes \dots \otimes r_{i_t t} \mid i_k = 0,1,2,3, \quad 1 \leq k \leq t\}$$

O fato de S ser um conjunto q-gerador com 4^t elementos é agora uma conseqüência imediata das propriedades do produto tensorial e do fato de que $\{1, r_{1i}, r_{2i}, r_{3i}\}$ é q-gerador, $1 \leq i \leq t$.

Reciprocamente, suponhamos que A possua um conjunto q-gerador S com 4^t elementos. Para provarmos que A é produto tensorial de F-subálgebras de quatérnios, faremos indução sob t.

Se t=1, então A possui um conjunto q-gerador S com 4 elementos. Sejam r_1, $r_2 \in S$ tais que $r_1r_2 = -r_2r_1$. Então $S'=\{1, r_1, r_2, r_1r_2\}$ é um conjunto q-gerador e portanto, linearmente independente sobre F, pela proposição anterior. Como $[A:F] = 4$, segue-se que S' é uma base de A sobre F. Assim, $A=F+Fr_1+Fr_2+Fr_1r_2$, donde A é uma F-álgebra de quatérnios.

Suponhamos agora o resultado verdadeiro para toda F-álgebra simples central de dimensão 4^{t-1}. Consideremos S um conjunto q-gerador com 4^t elementos e sejam $r_1, r_2 \in S$ tais que $r_1 . r_2 = -r_2 . r_1$. Seja ainda Q_1 a F-subálgebra de quatérnios de base $\{1, r_1, r_2, r_1r_2\}$.

Por [5, teorema 4.4.2], temos que $A = Q_1 \cdot C_A(Q_1) \simeq Q_1 \otimes C_A(Q_1)$, onde $C_A(Q_1)$ denota o centralizador de Q_1 em A.

Além disso, é fácil ver que dado um elemento $r \in A$, r se escreve na forma

$$r = \sum_{i=0}^{3} r_i \rho_i \text{ , onde } r_0 = 1, \ r_3 = r_1r_2 \quad \text{e}$$

$\rho_i \in C_A(Q_1)$, $0 \leq i \leq 3$. Mais ainda, se $r \in S$ então temos que

apenas um dos ρ_i's é não nulo. Isto decorre do fato de que se $r \in S$ então, como S é q-gerador, $rr_1 = \pm r_1 r$ e $rr_2 = \pm r_2 r$.

Desta forma, temos que S pode ser escrito como união disjunta

$S = S_0 \dot{\cup} S_1 r_1 \cup S_2 r_2 \dot{\cup} S_3 r_1 r_2$, onde cada S_i está contido no $C_A(Q_1)$, $0 \leq i \leq 3$.

Como S é linearmente independente sobre F, segue-se que S_0 e $S_i . r_i$ também o são, $1 \leq i \leq 3$. Mas $[C_A(Q_1):F] = 4^{t-1}$. Assim, cada S_i possui no máximo 4^{t-1} elementos. Como S possui 4^t elementos, segue-se que cada S_i possui exatamente 4^{t-1} elementos. Em particular, $S_0 = S \cap C_A(Q_1)$ possui 4^{t-1} elementos e $S_0 \subset C_A(Q_1)$.

Vamos mostrar agora que S_0 é um conjunto q-gerador.

Como $S_0 \subset S$ segue-se imediatamente que S_o satisfaz as condições (i) e (ii) da definição (6.1). Resta portanto provar que dados $t_1, t_2 \in S_o$, $t_1 \neq t_2$, existe $t \in S_0$ tal que

$$t_1 t = t t_1 \quad e \quad t_2 t = - t t_2.$$

Como $t_1, t_2 \in S_0 \subset S$, sabemos que existe $s \in S$ tal que

$$t_1 s = s t_1 \quad e \quad t_2 s = -s t_2.$$

Logo, se $s \in C_A(Q_1)$ então podemos tomar $t = s$ e segue-se que

S_0 é q-gerador. Ainda, se $s \notin C_A(Q_1)$ então $s = r_i\,\rho$ onde $\rho \in C_A(Q_1)$ e $i \neq 0$. Além disto, como $st_1 = st_1 s$ e $st_2 = -\,t_2 s$, temos que

$$\rho\, t_1 = t_1\, \rho \quad e \quad \rho\, t_2 = -\, t_2\, \rho \qquad (**)$$

Por outro lado, S_0 é uma base de $C_A(Q_1)$ sobre F. Consequentemente, existem $\alpha_1,\ldots,\alpha_k \in F$ tais que $\rho = \sum_{i=1}^{k} \alpha_i s_i$ onde cada $s_i \in S_0$. Como S_0 satisfaz as condições (i) e (ii) da definição (6.1), é linearmente independente sobre F e valem as igualdades (**), temos que

$$s_i\, t_1 = t_1 s_i \quad e \quad s_i\, t_2 = -\, t_2 s_i, \quad 1 \leq i \leq k$$

com $\alpha_i \neq 0$.

Como $\rho \neq 0$, segue-se que existe $1 \leq j \leq k$ tal que $\alpha_j \neq 0$. Seja $t = s_j \in S_0$. Então $tt_1 = t_1 t$ e $tt_2 = -\,t_2\, t$, com o que concluímos a demonstração de que S_0 é q-gerador.

Assim, usando a hipótese de indução temos que existem F-subálgebras de quatérnios $Q_2,\ldots,Q_t$ tais que

$$C_A(Q_1) = Q_2 \otimes_F \cdots \otimes_F Q_t.$$

Como $A = Q_1 \otimes_F C_A(Q_1)$, obtemos $A = Q_1 \otimes_F Q_2 \otimes_F \cdots \otimes_F Q_t$ e o teorema está demonstrado. $\square$

Seja Q uma F-álgebra de quatérnios e consideremos * uma involução em Q do primeiro tipo. Então existe um conjunto q-gerador $S = \{1, r_1, r_2, r_1 r_2\} \subset Q$ tal que $1^* = 1$, $r_1^* = \pm r_1$ e $r_2^* = \pm r_2$. Com esta observação a prova da proposição que se segue é exatamente análoga à da proposição anterior e por isto será omitida.

6.4 - PROPOSIÇÃO - Seja A uma álgebra simples central sobre um corpo F, de dimensão 4^t, que possui uma involução * do primeiro tipo. Então A é um produto tensorial de F-subálgebras de quatérnios invariantes sob * se e somente se A possui um conjunto q-gerador S com 4^t elementos satisfazendo $s^* = \pm s$, para todo $s \in S$.

§ 7 - PRODUTOS CRUZADOS ABELIANOS

Em todo este parágrafo, K/F denotará uma extensão galoisiana, com grupo de Galois abeliano

$$G = \langle \sigma_1 \rangle \times \ldots \times \langle \sigma_r \rangle .$$

Denotaremos por q_i a ordem de σ_i, $1 \leq i \leq r$.

Seja A uma F-álgebra simples central que contém K como subcorpo maximal. Sabemos então, pelo teorema de Skolem-Nöether [5, teorema 4.3.1] que cada σ_i pode ser estendido a um auto-

morfismo interno de A, isto é, existem elementos inversíveis $z_i \in A$, $1 \leq i \leq r$ tais que

$$\sigma_i(x) = z_i \, x \, z_i^{-1}, \quad 1 \leq i \leq r, \quad \forall \, x \in K.$$

Por outro lado, todo elemento $\sigma \in G$ se escreve de modo único na forma

$$\sigma = \sigma_1^{m_1} \ldots \sigma_r^{m_r} \quad \text{onde } 0 \leq m_i < q_i \quad \text{e} \quad 1 \leq i \leq r.$$

Consideremos então o elemento z_σ de A definido por $z_\sigma = z_1^{m_1} \ldots z_r^{m_r}$. Desta forma, podemos considerar a aplicação $f: G \times G \longrightarrow K^*$ definida por

$$f(\sigma, \tau) = z_\sigma \, z_\tau \, (z_{\sigma\tau})^{-1}, \quad (\sigma, \tau) \in G \times G.$$

O fato de A ser associativa nos garante que f é um conjunto de fatores de G sobre K e ainda que A é o <u>produto cruzado de K e G relativo a f</u>, isto é,

$$A = (K, G, f).$$

Nosso objetivo agora será explorar o fato de G ser abeliano, para caracterizarmos o produto cruzado através de outros parâmetros. Para isto, consideremos os elementos

$$u_{ij}=z_i\ z_j\ z_i^{-1}\ z_j^{-1} \quad \text{e } b_i = z_i^{q_i} \qquad 1 \leq i,j \leq r.$$

Como K é um subcorpo maximal de A, segue-se que $K = C_A(K)$, ou seja, K coincide com seu centralizador em A. Além disso, $o(\sigma_i) = q_i$, $1 \leq i \leq r$. Desta forma, é fácil verificar que

$$U = \{u_{ij} | 1 \leq i,j \leq r\} \subset K$$

e

$$B = \{b_i \mid 1 \leq i \leq r\} \subset K$$

Observamos ainda que podemos calcular $f(\sigma,\tau)$ utilizando apenas os elementos u_{ij}, b_i e a ação dos σ_i sobre estes elementos, $1 \leq i,j \leq r$. (Por exemplo, se $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle$, com

$$o(\sigma_1) = o(\sigma_2) = 2, \quad o(\sigma_3) = 3 \quad ,$$

$$\sigma = \sigma_1\sigma_2 \quad \text{e } \tau = \sigma_2\ \sigma_3^2 \quad \text{temos}$$

$$f(\sigma,\tau) = z_\sigma\ z_\tau (z_{\sigma\tau})^{-1} = (z_1 z_2)(z_2 z_3^2)(z_1 z_3^2)^{-1} =$$

$$= z_1\ z_2^2\ z_3^2\ z_3^{-2}\ z_1^{-1} = z_1\ z_2^2\ z_1^{-1} =$$

$$= z_1\ b_2\ z_1^{-1} = \sigma_1\ (b_2)\ z_1\ z_1^{-1} = \sigma_1\ (b_2)$$

Deste modo, os conjuntos U, B $\subseteq$ K determinam o conjunto de fatores f de G sobre K e portanto determinam a álgebra A.

Denotaremos então por A = (K, G, U, B) o <u>produto cruzado abeliano de K e G</u>.

Passaremos a estudar algumas propriedades dos conjuntos U e B acima definidos, que nos servirão posteriormente para caracterizar os produtos cruzados abelianos. Para isto, precisamos do seguinte lema.

<u>7.1 - LEMA</u> - Sejam R um anel não comutativo e x um elemento inversível de R. Consideremos o automorfismo $\sigma: R \to R$ definido por $\sigma(y) = x\, y\, x^{-1}$, $y \in R$. Então:

(a) $(yx)^n = y\,\sigma(y) \ldots \sigma^{n-1}(y)\, x^n$, $\forall\, y \in R$, $\forall\, n \in \mathbb{N}$.

(b) Se $y \in R$ e $u = \sigma(y)\, y^{-1}$ temos:

$$x^n\, y\, x^{-n} = \sigma^{n-1}(u) \ldots \sigma(u)\, u\, y, \quad \forall\, n \in \mathbb{N}.$$

<u>DEMONSTRAÇÃO</u>:

A prova segue facilmente, usando-se indução sobre n e por isto será omitida.

Dado um elemento $x \in K$, denotemos por

$N_i(x) = \prod_{k=0}^{q_i-1} \sigma_i^k(x)$. É fácil ver que se $x, y \in K$ então:

$$N_i(xy) = N_i(x)\, N_i(y) \,, \qquad 1 \leq i \leq r$$

e

$$N_i(\sigma_j(x)) = \sigma_j(N_i(x)), \qquad 1 \leq i,j \leq r.$$

<u>(7.2) - PROPOSIÇÃO</u> - Sejam U, $B \subset K$ os conjuntos definidos anteriormente. Então

(1) $u_{ii} = 1$ e $u_{ij}^{-1} = u_{ji}$

(2) $\sigma_i(u_{jk})\, \sigma_j(u_{ki})\, \sigma_k(u_{ij}) = u_{jk}\, u_{ki}\, u_{ij}$

(3) $N_i(N_j(uij)) = 1$

(4) $\sigma_j(b_i) = N_i(u_{ji})\, b_i \qquad 1 \leq i,j,k \leq r.$

<u>DEMONSTRAÇÃO</u>:

(1) segue imediatamente da definição.

Para provarmos (4) lembramos que $\sigma_j(b_i) = z_j\, b_i\, z_j^{-1}$. Temos então:

$$\sigma_j(b_i) = z_j\, z_i^{q_i}\, z_j^{-1} = (z_j\, z_i\, z_j^{-1})^{q_i} = (u_{ji}\, z_i)^{q_i}.$$

Usando a parte (a) do lema (7.1), temos:

$$\sigma_j(b_i) = u_{ji}\ \sigma_i(u_{ji}) \ldots \sigma_i^{q_i-1}(u_{ji})\ z_i^{q_i} = N_i\ (u_{ji})\ b_i$$

De (4) temos que

$N_i(u_{ji}) = \sigma_j(b_i)b_i^{-1}$. Assim,

$$N_i(u_{ij}) = N_i(u_{ji}^{-1}) = N_i(u_{ji})^{-1} = b_i\ \sigma_j(b_i^{-1})$$

Logo,

$$N_j(N_i(u_{ij})) = N_j(b_i\sigma_j(b_i^{-1})) = N_j(b_i)N_j(\sigma_j(b_i^{-1})) =$$

$$= N_j(b_i)\ \sigma_j(N_j(b_i^{-1}) =$$

$$= N_j(b_i)\ N_j(b_i^{-1}) = 1.$$

Portanto,

$N_j(N_i(u_{ij})) = 1$, donde vale (3).

Para provarmos (2), observemos que $z_i\ z_j = u_{ij}\ z_j\ z_i$. Conjugando esta igualdade por z_k, por um lado, obtemos:

$$z_k(z_i\ z_j)\ z_k^{-1} = z_k\ z_i(z_k^{-1}\ z_k)\ z_j\ z_k^{-1} =$$

$$= u_{ki}\ z_i\ z_k\ z_j\ z_k^{-1} =$$

$$= u_{ki}\ z_i\ u_{kj}\ z_j\ z_k\ z_k^{-1} =$$

$$= u_{ki}\ z_i\ u_{kj}\ z_j = u_{ki}\ \sigma_i(u_{kj})\ z_i\ z_j\ .$$

Por outro lado, temos:

$$z_k\ (z_i\ z_j)\ z_k^{-1} = z_k(u_{ij}\ z_j\ z_i)\ z_k^{-1} =$$

$$= \sigma_k\ (u_{ij})\, z_k z_j\, z_i z_k^{-1} =$$

$$= \sigma_k\ (u_{ij})\ u_{kj}\ z_j\ z_k\ z_i\ z_k^{-1} =$$

$$= \sigma_k\ (u_{ij})\ u_{kj}\ z_j\ u_{ki}\ z_i =$$

$$= \sigma_k\ (u_{ij})\ u_{kj}\ \sigma_j(u_{ki})\, z_j\ z_i =$$

$$= \sigma_k\ (u_{ij})\ u_{kj}\ \sigma_j(u_{ki})\ u_{ji}\ z_i\ z_j.$$

Assim, mostramos que:

$$u_{ki}\ \sigma_i(u_{kj})\ z_i\ z_j = \sigma_k(u_{ij})\ u_{kj}\ \sigma_j(u_{ki})\ u_{ji}\ z_i\ z_j.$$

Como z_i, z_j são inversíveis em A, obtemos:

$$u_{ki}\ \sigma_i(u_{kj}) = \sigma_k(u_{ij})\ u_{kj}\ \sigma_j(u_{ki})u_{ji}$$

Ainda, como todos os elementos envolvidos na igualdade acima estão em K, segue-se que eles comutam entre si e podemos então reescrever a igualdade acima da seguinte forma:

$$\sigma_i(u_{jk})\ \sigma_j(u_{ki})\ \sigma_k(u_{ij}) = u_{jk}\ u_{ki}\ u_{ij}\ ,$$

com o que concluímos a demonstração da proposição. $\square$

Vamos mostrar agora que as propriedades (1), (2) e (4) da proposição anterior, determinam (a menos de isomorfismo) o produto cruzado abeliano. Mas precisamente, seja $K|_F$ uma extensão galoisiana com grupo de Galois abeliano $G = \langle \sigma_1 \rangle \times \ldots \times \langle \sigma_r \rangle$, onde $o(\sigma_i) = q_i$, $1 \leq i \leq r$. Sejam ainda

$$U^* = \{u^*_{ij}/1 \leq i,j \leq r\} \quad e \quad B^* = \{b^*_i/1 \leq i \leq r\}$$

subconjuntos de K satisfazendo as relações (1), (2) e (4) da proposição anterior. Mostraremos que existem uma F-álgebra simples central A, que possui K como subcorpo maximal, e elementos inversíveis $z_i \in A$, $1 \leq i \leq r$, tais que

$$A = (K, G, U, B)\ , \quad \text{onde}$$

$$u_{ij} = u^*_{ij} \quad e \quad b_i = b^*_i\ , \qquad 1 \leq i,j \leq r.$$

Além disso, veremos que A é única a menos de isomorfismo.

Para isso, consideramos inicialmente um conjunto de r indeterminadas <u>não comutativas</u> $\{x_1,\ldots,x_r\}$ e construímos o conjunto

$$A_r = \left\{ \sum_{i_1,\ldots i_r} k_{i_1\ldots i_r} x_1^{i_1}\ldots x_r^{i_r} \,\middle|\, k_{i_1\ldots i_r} \in K \right\}$$

Vamos dar a A_r uma estrutura de K-álgebra. Definimos a igualdade e a adição de dois elementos de A_r, componente a componente. Além disso, definimos o produto distributivamente, por

$$x_i\, k = \sigma_i(k)\, x_i \quad \text{e} \quad x_i x_j = u^*_{ij}\, x_j x_i \,,$$

$$1 \leq i,j \leq r, \quad k \in K.$$

A álgebra A que procuramos será definida como um quociente de A_r.

Dividiremos a construção de A em vários passos.

<u>7.3 - LEMA</u> - Seja M o ideal à esquerda de A_r gerado pelo conjunto

$$\{x_i^{q_i} - b_i^* \mid 1 \leq i \leq r\} .$$

Então M é ideal bilateral de A_r.

DEMONSTRAÇÃO

Para provarmos a afirmação acima, mostraremos primeiro que $M_i = A_r(x_i^{q_i} - b_i^*)$ é um ideal bilateral de A_r para cada $i = 1,\ldots,r$.

Para isso, é suficiente verificar que $(x_i^{q_i}-b_i^*)\, x_t \in A_r\,(x_i^{q_i}- b_i)$, para todo t, $1 \leq t \leq r$ e que $(x_i^{q_i} - b_i^*)\, k \in A_r\,(x_i^{q_i} - b_i^*)$, para todo $k \in K$. Mas

$$(x_i^{q_i} - b_i^*)\, x_t = x_i^{q_i} x_t - b_i^* x_t =$$

$$= u_{it}^* \sigma_i(u_{it}^*) \ldots \sigma_i^{q_i-1}(u_{it}^*) x_t x_i^{q_i} - b_i^* x_t =$$

$$= N_i(u_{it}^*)\, x_t\, x_i^{q_i} - b_i^*\, x_t =$$

$$= x_t\, \sigma_t^{-1}(N_i(u_{it}^*))\, x_i^{q_i} - x_t\, \sigma_t^{-1}(b_i^*)$$

Por (4) temos que $b_i^* = \sigma_t(b_i^*)\, N_i(u_{it}^*)$.

Logo, $\sigma_t^{-1}(b_i^*) = b_i^*\, \sigma_t^{-1}(N_i(u_{it}^*)) = \sigma_t^{-1}(N_i(u_{it}^*))\, b_i^*$.

Assim,

$$(x_i^{q_i} - b_i^*)\, x_t = x_t \left[\sigma_t^{-1}(N_i(u_{it}^*))\, x^{q_i} - \sigma_t^{-1}(N_i(u_{it}^*))\, b_i^*\right] =$$

$$= x_t\ \sigma_t^{-1}(N_i(u_{it}^*))(x_i^{q_i} - b_i^*) \in M_i, \quad 1 \leq t \leq r.$$

Seja k um elemento qualquer de K. Então:

$$(x_i^{q_i} - b_i^*)k = x_i^{q_i}\ k - b_i^*\ k = \sigma_i^{q_i}(k)\ x_i^{q_i} - k\ b_i^* =$$

$$= k\ x_i^{q_i} - k\ b_i^* = k(x_i^{q_i} - b_i^*) \in M_i\ ,$$

pois $o(\sigma_i) = q_i$.

Finalmente, como cada M_i, $1 \leq i \leq r$ é um ideal bilateral de A_r, segue-se trivialmente que

$M = \langle\ x_i^{q_i} - b_i^* \mid 1 \leq i \leq r\ \rangle$ também é um ideal bilateral de A_r. □

<u>7.4 - LEMA</u> - Com as notações acima, tem-se que:

(i) $\prod_{k=1}^{q_j} \sigma_j^{-k}\ (N_i(u_{ij}^*)) = 1, \quad 1 \leq i,j \leq r.$

(ii) $(x_i^{q_i} - b_i^*)(x_j^{q_j} - b_j^*) = (x_j^{q_j} - b_j^*)(x_i^{q_i} - b_i^*)\ ,$

$1 \leq i,j \leq r.$

DEMONSTRAÇÃO

Por (4) temos que

$$N_i(u^*_{ij}) = b^*_i \; \sigma_j(b^{*-1}_i)$$

Logo

$$\sigma_j^{-k}(N_i(u^*_{ij})) = \sigma_j^{-k}(b^*_i) \; \sigma_j^{-k+1}(b^{*-1}_i), \quad 1 \leq k \leq q_j$$

Assim,

$$\prod_{k=1}^{q_j} \sigma_j^{-k}(N_i(u^*_{ij})) = \prod_{k=1}^{q_j} \left[\sigma_j^{-k}(b^*_i) \; \sigma_j^{-k+1}(b^{*-1}_i)\right] =$$

$$= b^{*-1}_i \; \sigma_j^{-q_j}(b^*_i) = 1 \; ,$$

pois $o(\sigma_j) = q_j$.

Para provarmos (ii), observemos que, como no lema anterior, temos:

$$(x_i^{q_i} - b^*_i)x_j^{q_j} = x_j^{q_j} \; \sigma_j^{-q_j}(N_i(u^*_{ij}))\ldots\sigma_j^{-1}(N_i(u^*_{ij}))(x_i^{q_i} - b_i) =$$

$$= x_j^{q_j}\left[\prod_{k=1}^{q_j} \sigma_j^{-k}((N_i(u^*_{ij}))\right](x_i^{q_i} - b^*_i)$$

$$= x_j^{q_j}(x_i^{q_i} - b^*_i)$$

Mas já vimos na demonstração do lema anterior, que $(x_i^{q_i} - b_i^*)$ comuta com b_j^*. Logo, temos:

$$(x_i^{q_i}-b_i^*)(x_j^{q_j}-b_j^*) = (x_i^{q_i}-b_i^*)x_j^{q_j} - (x_i^{q_i}-b_i^*)\, b_j^* =$$

$$= x_j^{q_j}(x_i^{q_i}-b_i^*) - b_j^*\,(x_i^{q_i}-b_i^*) =$$

$$= (x_j^{q_j}-b_j^*)(x_i^{q_i}-b_i^*)\ ,$$

com o que concluímos a demonstração. □

Introduziremos agora algumas notações que facilitarão nossos cálculos. Se $\bar{m} = (m_1,\ldots,m_r)$ é uma r-upla de números naturais e $a = (a_1,\ldots,a_r)$ é uma r-upla de elementos de um grupo, anel, etc., indicaremos por $a^{\bar{m}}$ o elemento

$$a^{\bar{m}} = a_1^{m_1} \ldots a_r^{m_r}$$

Em particular, todo elemento do grupo G tem a forma $\sigma^{\bar{m}} = \sigma_1^{m_1} \ldots \sigma_r^{m_r}$. Além disso, é claro que os <u>monômios</u>

$$\{x^{\bar{m}} = x_1^{m_1} \ldots x_r^{m_r} \mid m_i \in \mathbb{N},\ 1 \leq i \leq r\}$$

formam uma base de A_r como espaço vetorial (à esquerda) sobre K.

Por outro lado, dados dois monômios $x^{\bar{m}}$ e $x^{\bar{n}}$ temos que

$$x^{\bar{m}} \cdot x^{\bar{n}} = a\, x^{\bar{m}+\bar{n}}$$, para algum $a \in K$. Deste modo,

definimos o grau de um monômio $x^{\bar{m}} = x_1^{m_1} \ldots x_r^{m_r}$ como a r-upla de números naturais $\bar{m} = (m_1, \ldots, m_r)$ e indicaremos $\partial(x^{\bar{m}}) = \bar{m}$.

<u>7.5 - LEMA</u> - Seja $A = \frac{A_r}{M}$. Então o conjunto

$$\{z^{\bar{m}} = x^{\bar{m}} + M = x_1^{m_1} \ldots x_r^{m_r} + M \mid 0 \leq m_i < q_i \quad 1 \leq i \leq r\}$$

é uma base de A sobre K.

<u>DEMONSTRAÇÃO</u>

Começaremos demonstrando que todo elemento $f(x) \in A_r$ pode ser escrito na forma

$$f(x) = (x_i^{q_i} - b_i^*)\, g(x) + h(x)$$

onde todo monômio de $h(x)$ tem grau menor que q_i na variável x_i.

Seja então $f(x) = f(x_1, \ldots, x_r) \in A_r$.

É claro que podemos escrever f como soma de monômios em $(x_1, \ldots, x_r)$ de modo a variável x_i apareça sempre em primeiro lugar, em todos os monômios nos quais ela ocorre. Além disso, podemos escrever f na forma $f = f_1 + f_2$, onde $f_1, f_2 \in A_r$ satisfazem as seguintes condições:

(i) A variável x_i ocorre em todos os monômios de f_1 com expoente maior ou igual a q_i.

(ii) Se a variável x_i ocorre em algum monômio de f_2, então o expoente de x_i neste monômio é menor que q_i.

Com estas considerações, é claro que basta demonstrar a afirmação para f_1, ou seja, podemos assumir que a variável x_i ocorre em <u>todos</u> os monômios de f, em primeiro lugar, com expoente maior ou igual a q_i.

Seja então

$$M = x_i^m \, a \, x_1^{m_1} \ldots x_{i-1}^{m_{i-1}} \, x_{i+1}^{m_{i+1}} \ldots x_r^{m_r}$$

um monômio qualquer de f. Então $m \geq q_i$ e podemos escrever $m = q_i \, t + s$ onde $0 \leq s < q_i$.

Assim, temos

$$x_i^m \, a \, x_1^{m_1} \ldots x_{i-1}^{m_{i-1}} \, x_{i+1}^{m_{i+1}} \ldots x_r^{m_r} = (x_i^{q_i})^t \, x_i^s \, a \, x_1^{m_1} \ldots x_{i-1}^{m_{i-1}} \, x_{i+1}^{m_{i+1}} \ldots x_r^{m_r} =$$

$$= (x_i^{q_i t} - b_i^{*t}) \, x_i^s \, a \, x^{m_1} \ldots x_r^{m_r} + b_i^{*t} \, x_i^s \, a \, x_1^{m_1} \ldots x_r^{m_r}$$

Como $x_i^{q_i n} \, b_i^* = \sigma_i^{q_i n}(b_i^*) \, x_i^{q_i n} = b_i^* \, x_i^{q_i n}$, para todo $n \in \mathbb{N}$, segue-se que $(x_i^{q_i} - b_i^*) \mid (x_i^{q_i t} - b_i^{*t})$.

Logo, existe $g_1 \in A_r$ tal que $(x_i^{q_i} - b_i^*) g_1 = (x_i^{q_i t} - b_i^{*t})$.

Desta forma, obtemos:

$$M = (x_i^{q_i} - b_i^*) g_1 \; x_i^s \; a \prod_{k \neq i} x_k^{m_k} + b_i^{*t} x_i^s \; a \prod_{k \neq i} x_k^{m_k} \; , \quad e$$

$0 \leq s < q_i$.

Portanto, mostramos que todo monômio de f se escreve na forma

$M = (x^{q_i} - b_i^*) \; g(x) + h(x)$, onde $g(x)$, $h(x) \in A_r$ e todo monômio de $h(x)$ tem expoente menor que q_i em x_i.

Finalmente, podemos mostrar que o conjunto $\{z^{\bar{m}} = x^{\bar{m}} + M = x_1^{m_1} \ldots x_r^{m_r} + M \; / \; 0 \leq m_i < q_i, \; 1 \leq i \leq r\}$ é uma base de $A = \frac{A_r}{M}$ sobre K.

Seja $f(x)$ um elemento qualquer de A_r. Pelas considerações feitas acima, segue-se que podemos escrever f na forma: $f(x) = (x_1^{q_1} - b_1^*) g_1(x) + \ldots + (x_r^{q_r} - b_r^*) \; g_r(x) + h(x)$, onde todo monômio de $h(x)$ tem grau menor que q_i na variável x_i, $1 \leq i \leq r$.

Deste modo, $f(x) + M = h(x) + M$ e portanto o conjunto

$$\{z^{\bar{m}} = x_1^{m_1} \ldots x_r^{m_r} + M \mid 0 \leq m_i < q_i, \; 1 \leq i \leq r\}$$

gera A sobre K.

Resta provar que o conjunto acima é linearmente in-

dependente sobre K. Para isto é suficiente mostrar que se $f \in M$ é tal que todo monômio de f tem grau menor que q_i na variável x_i, $1 \leq i \leq r$, então f é o polinômio nulo. Consideremos pois um tal f. Então $f = \sum_{j=1}^{r} (x_j^{q_j} - b_j)\, h_j(x)$. Seja $j < r$ fixado. Podemos escrever

$$h_j(x) = (x_r^{q_r} - b_r^*)\, g_j(x) + h'_j(x)$$

onde todo monômio de h'_j tem grau menor que q_r em x_r. Logo ,

$$(x_j^{q_j} - b_j^*)\, h_j(x) = (x_j^{q_j} - b_j^*)(x_r^{q_r} - b_r^*)\, g_j(x) +$$

$$+ (x_j^{q_j} - b_j^*)\, h'_j(x) =$$

$$= (x_r^{q_r} - b_r^*)(x_j^{q_j} - b_j^*)\, g_j(x) +$$

$$+ (x_j^{q_j} - b_j^*)\, h'_j(x)$$

Portanto

$$f(x) = (x_r^{q_r} - b_r^*)\, h_r(x) + \sum_{j<r} \left[(x_r^{q_r} - b_r^*)(x_j^{q_j} - b_j^*)\, g_j(x)\right] +$$

$$+ \sum_{j<r} (x_j^{q_j} - b_j^*)\, h'_j(x) =$$

$$= (x_r^{q_r} - b_r^*) \left[h_r(x) + \sum_{j<r} ((x_j^{q_j} - b_j^*)\, g_j(x))\right] +$$

$$+ \sum_{j<r} (x_j^{q_j} - b_j)\, h_j'(x)$$

Se $g(x) = h_r(x) + \sum_{j<r} \left[(x_j^{q_j} - b_j^*)\, g_j(x)\right]$ não é o polinômio nulo, então existe um monômio M de $g(x)$ de grau máximo m na variável x_r. Assim, $(x_r^{q_r} - b_r^*)\, M$ é um monômio de f (pois não se cancela com nenhum monômio de $\sum_{j<r} (x^{q_j} - b_j^*)\, h_j'(x)$. Mas o grau de x_r em $(x_r^{q_r} - b_r^*)\, M$ é maior ou igual a q_r, absurdo. Logo, $g(x)$ é o polinômio nulo, donde

$$f(x) = \sum_{j<r} (x_j^{q_j} - b_j)\, h_j'(x)$$

Repetindo o argumento para $r-1, \ldots, 1$, concluímos que f é o polinômio nulo.

Assim, demonstramos que o conjunto

$\{z^{\bar{m}} = x_1^{m_1} \ldots x_r^{m_r} + M \mid 0 \leq m_i < q_i,\ 1 \leq i \leq r\}$ é uma base de $A = \frac{A_r}{M}$ sobre K. Conseqüentemente, $[A:K] = q_1 \ldots q_r = n = |G|$. $\square$

<u>7.6 - PROPOSIÇÃO</u> - Com as notações acima, tem-se que $F = Z(A)$, o centro de A.

DEMONSTRAÇÃO

É claro que $F \subset Z(A)$. Reciprocamente, consideremos $f = \sum_{\bar{m}} a_{\bar{m}} z^{\bar{m}} \in Z(A)$. Em particular, f comuta com todo elemento de K. Logo, se $\alpha \in K$, temos:

$$\alpha \left(\sum_{\bar{m}} a_{\bar{m}} z^{\bar{m}} \right) = \left(\sum_{\bar{m}} a_{\bar{m}} z^{\bar{m}} \right) \alpha$$

Conseqüentemente,

$$\sum_{\bar{m}} (\alpha - \sigma^{\bar{m}}(\alpha))\, a_{\bar{m}} z^{\bar{m}} = 0 \text{ , para todo } \alpha \in K.$$

Como o conjunto $\{z^{\bar{m}}\}$ é linearmente independente sobre K, temos que $(\alpha - \sigma^{\bar{m}}(\alpha)) a_{\bar{m}} = 0$, para todo $\alpha \in K$ e todo $\bar{m}$.

Se para alguma r-upla $\bar{m} = (m_1, \ldots m_r)$, $a_{\bar{m}} \neq 0$ então $\alpha - \sigma^{\bar{m}}(\alpha) = 0$ para todo $\alpha \in K$ e portanto $\bar{m} = (0, 0, \ldots, 0)$. Assim, $f = a_{(0,\ldots,0)} \in K$.

Por outro lado, se $f = a \in K \cap Z(A)$ então $z^{\bar{m}} a = a z^{\bar{m}}$, para toda r-upla $\bar{m} = (m_1, \ldots, m_r)$ tal que $0 \leq m_i < q_i, 1 \leq i \leq r$. Daí decorre imediatamente que $\sigma^{\bar{m}}(a) = a$, para todo $\bar{m}$ nessas condições. Então $a \in K$ é fixo por todos os automorfismos de G, donde $a \in F$.

Mostramos assim, que A é uma álgebra de centro F e $[A:F] = n^2$.

$\square$

7.7 - TEOREMA - Ainda, com as notações acima, existem elementos inversíveis $z_1,\ldots,z_r \in A$ tais que:

$$z_i z_j = u^*_{ij}\, z_j z_i \;, \quad b^*_i = z_i^{q_i} \qquad 1 \leq i,j \leq r$$

e

$$A = (K,\ G,\ U, B) \quad \text{onde}$$

$$U = \{u^*_{ij} \mid 1 \leq i,j \leq r\} \quad e \quad B = \{b^*_i \mid 1 \leq i \leq r\}$$

DEMONSTRAÇÃO

Consideremos os elementos $z_i = x_i + M \in A$, $1 \leq i \leq r$. Vamos mostrar que z_i é inversível em A, $1 \leq i \leq r$. Para isto, calculemos:

$$x_i(x_i^{q_i-1}\, b_i^{*-1}) - 1 = x_i^{q_i}\, b_i^{*-1} - 1 =$$

$$=(x_i^{q_i} - b_i^*)\, b_i^{*-1} \in M$$

Assim,

$$x_i(x_i^{q_i-1}\, b_i^{*-1}) + M = 1 + M.$$

Logo

$$(x_i+M)\ (x_i^{q_i-1}\, b_i^{*-1} + M) = 1 + M.$$

Por outro lado

$$(x_i^{q_i-1} b_i^{*-1}) x_i = x_i^{q_i-1} (b_i^{*-1} x_i) = x_i^{q_i} (x_i b_i^{*-1} x_i)$$

$$= x_i^{q_i} \sigma_i^{-1} (b_i^{*-1})$$

Mas o conjunto $B^* = \{b_i^* | 1 \leq i \leq r\}$ verifica a condição (4) da proposição (7.2).

Logo, $\sigma_i(b_i^*) = N_i(u_{ii}^*) b_i^* = b_i^*$. Assim,

$$(x_i^{q_i-1} b_i^{*-1}) x_i = x_i^{q_i} b_i^{*-1}.$$

Portanto,

$$(x_i^{q_i-1} b_i^{*-1}) x_i - 1 = x_i^{q_i} b_i^{*-1} - 1 = (x_i^{q_i} - b_i^*) b_i^{*-1} \in M$$

Conseqüentemente,

$$(x_i^{q_i-1} b_i^{*-1} + M) (x_i + M) = 1 + M$$

donde, $z_i = x_i + M$ é inversível em A, $1 \leq i \leq r$.

Por outro lado, dados $\sigma, \tau \in G$ sabemos que eles se escrevem de modo único na forma:

$$\tau = \sigma_1^{m_1} \ldots \sigma_r^{m_r}, \quad \tau = \sigma_1^{n_1} \ldots \sigma_r^{n_r} \quad \text{onde}$$

$$0 \leq m_i, n_i < q_i, \quad 1 \leq i \leq r.$$

Consideremos então $\bar{m} = (m_1,\ldots,m_r)$, $\bar{n} = (n_1,\ldots,n_r)$ e $\bar{p} = (p_1,\ldots,p_r)$, onde $p_i \equiv (m_i+n_i) \bmod q_i$ e $0 \leq p_i < q_i$, $1 \leq i \leq r$.

Deste modo, podemos definir

$f: G \times G \to K^*$ por

$$f(\sigma,\tau) = z^{\bar{m}}\, z^{\bar{n}}\, (z^{\bar{p}})^{-1}$$

Observemos que $f(\sigma,\tau) \in K^*$ para todo par $(\sigma,\tau) \in G \times G$, pois K é um subcorpo maximal de A.

Além disso, o fato de A ser associativa implica que f é um conjunto de fatores de G sobre K e $A = (K|F, G, f)$.

Logo, para provarmos que $A = (K, G, U, B)$ basta verificar que

(i) $u_{ij}^* + M = z_i\, z_j\, z_i^{-1}\, z_j^{-1}$

e $\qquad 1 \leq i,j \leq r$.

(ii) $b_i^* + M = z_i^{q_i}$

A segunda condição é imediata pois $x_i^{q_i} - b_i^* \in M$.

Para provarmos (i), calculemos:

$$z_i\, z_j\, z_i^{-1}\, z_j^{-1} = (x_i+M)\,(x_j+M)\,(x_i+M)^{-1}\,(x_j+M)^{-1} =$$

$$= (x_i x_j+M)\,(x_i+M)^{-1}(x_j+M)^{-1} =$$

$$= (u_{ij}^*\, x_j x_i + M)\,(x_i+M)^{-1}\,(x_j+M)^{-1} =$$

$$= (u^*_{ij}+M)\ (x_j+M)\ (x_i+M)\ (x_i+M)^{-1}\ (x_j+M)^{-1} =$$

$$= u^*_{ij} + M.$$

Assim, $A = (K, G, U, B)$, onde $z_i = x_i+M$, $1 \leq i \leq r$,

$$U = \{u_{ij} = u^*_{ij} + M \mid 1 \leq i,j \leq r\}$$

$$B = \{b_i = b^*_i + M \mid 1 \leq i \leq r\}$$

$\square$

Estamos interessados em mostrar que a álgebra A acima construída é única a menos de isomorfismo. Para isso, começaremos verificando quando dois produtos cruzados abelianos são isomorfos.

<u>7.8 - PROPOSIÇÃO</u> - Sejam $A_1 = (K,G,U,B)$ e $A_2=(K,G,U',B')$ produtos cruzados abelianos de K sobre G. Então A_1 e A_2 são isomorfos como F-álgebras se e somente se existem elementos $a_i \in K$, $1 \leq i \leq r$ tais que:

(i) $b'_i = N_i(a_i)b_i$

(ii) $u'_{ij} = u_{ij}\ \sigma_i\ (a_j)a_j^{-1}\ a_i\sigma_j(a_i^{-1})$, $1 \leq i,j \leq r$

DEMONSTRAÇÃO

Suponhamos que $\psi: A_1 \to A_2$ seja um F-isomorfismo. Então é fácil verificar que $\psi(K)$ é um subcorpo maximal de A_2. Logo, $\psi^{-1}\Big|_{\psi(K)} : \psi(K) \to K$ é um F-isomorfismo de subálgebras simples de A_2. Pelo teorema de Skolem-Nöether, [5, teorema 4.3.1] existe um F-automorfismo interno $\alpha: A_2 \to A_2$ que estende $\psi^{-1}\Big|_{\psi(K)}$.

Seja $\Psi = \alpha \circ \psi$. Então $\Psi: A_1 \to A_2$ é um F-isomorfismo e $\Psi(k) = \alpha(\psi(k)) = \psi^{-1}(\psi(k)) = k$, para todo $k \in K$.

Mostramos portanto que se $A_1 \cong A_2$ como F-álgebras, então existe um isomorfismo $\psi: A_1 \to A_2$ tal que $\psi(k) = k$, para todo $k \in K$.

Sejam agora $z_i \in A_1$ e $z'_i \in A_2$, $1 \leq i \leq r$ tais que

$$z_i z_j = u_{ij} z_j z_i \qquad z'_i z'_j = u'_{ij} z'_j z'_i$$

$$z_i k = \sigma_i(k) z_i \qquad z'_i k = \sigma_i(k) z'_i$$

$$z_i^{q_i} = b_i \qquad z_i'^{q_i} = b'_i$$

$$1 \leq i,j \leq r, \quad k \in K.$$

Definimos então $a_i = z'_i \psi(z_i)^{-1}$, $1 \leq i \leq r$.

Dado um elemento $k \in K$ qualquer temos:

$$a_i \, k \, a_i^{-1} = z_i' \, \psi(z_i)^{-1} \, k \, \psi(z_i) \, z_i'^{-1} =$$

$$= z_i'(\psi(z_i^{-1} \, k \, z_i)) \, z_i'^{-1} = z_i' \, \psi(\sigma_i^{-1}(k)) \, z_i'^{-1} =$$

$$= z_i' \, \sigma_i^{-1}(k) \, z_i'^{-1} = \sigma_i(\sigma_i^{-1}(k)) = k \, ,$$

$$1 \leq i \leq r \, .$$

Logo, $a_i \in C_{A_2}(K) = K$, $1 \leq i \leq r$, pois K é subcorpo maximal de A_2.

Para provarmos que os elementos $a_i \in K$, $1 \leq i \leq r$, verificam (i) e (ii), observamos que dado um elemento $k \in K$ qualquer, temos:

$$\psi(\sigma_i(k) = \psi(z_i \, k \, z_i^{-1}) = \psi(z_i) \, \psi(k) \, \psi(z_i^{-1}) = \psi(z_i) k \, \psi(z_i)^{-1}$$

Sendo ψ um K-isomorfismo, temos:

$$\psi(\sigma_i(k)) = \sigma_i(k) = z_i \, k \, z_i^{-1} \, .$$

Conseqüentemente,

$$\sigma_i(k) = \psi(z_i) \, k \, \psi(z_i)^{-1}, \quad 1 \leq i \leq r, \quad k \in K.$$

Portanto

$$N_i(a_i) = a_i\ \sigma_i(a_i) \ldots \sigma_i^{q_i-1}(a_i) =$$

$$= a_i\left[\psi(z_i)a_i\ \psi(z_i)^{-1}\right] \ldots \left[\psi(z_i)^{q_i-1}\ a_i\psi(z_i)^{-q_i+1}\right] =$$

$$= \left[a_i\ \psi(z_i)\right]^{q_i-1}\ a_i\ \psi(z_i)^{-q_i+1}$$

Logo,

$$N_i(a_i)b_i = N_i(a_i)\ \psi(b_i) = N_i(a_i)\ \psi(z_i)^{q_i} =$$

$$= \left[a_i\ \psi(z_i)\right]^{q_i-1}\left[a_i\psi(z_i)\right] = \left[a_i\psi(z_i)\right]^{q_i} =$$

$$= z_i'^{q_i} = b_i' \quad , \quad 1 \leq i \leq r\ .$$

Além disso,

$$u_{ij}' = z_i'\ z_j'\ z_i'^{-1}\ z_j'^{-1} = a_i\ \psi(z_i)\ a_j\ \psi(z_j)(a_i\ \psi(z_i))^{-1}(a_j\psi(z_j))^{-1} =$$

$$= \psi(a_i\ z_i\ a_j\ z_j\ (a_i\ z_i)^{-1}\ (a_j\ z_j)^{-1}) =$$

$$= \psi(a_i\sigma_i(a_j)\ z_i\ z_j\ z_i^{-1}\ a_i^{-1}\ z_j^{-1}\ a_j^{-1}) =$$

$$= \psi(a_i\sigma_i(a_j)\ z_i\ z_j\ z_i^{-1}\ z_j^{-1}\ \sigma_j(a_i^{-1})\ a_j^{-1}) =$$

$$= \psi(a_i \sigma_i(a_j)\ u_{ij}\ \sigma_j(a_i^{-1})\ a_j^{-1}) =$$

$$= u_{ij}\ a_i\ \sigma_i(a_j)\ a_j^{-1}\ \sigma_j\ (a_i^{-1}) \qquad 1 \leq i,j \leq r.$$

Portanto o conjunto $\{a_i \mid 1 \leq i \leq r\}$ verifica (i) e (ii).

Reciprocamente, suponhamos que existam elementos $a_i \in K$, $1 \leq i \leq r$ verificando (i) e (ii). Sejam $z_i' = a_i\ z_i$, $1 \leq i \leq r$. É fácil verificar que

$$u_{ij}' = z_i'\ z_j'\ z_i'^{-1}\ z_j'^{-1}$$

$$b_i' = z_i'^{q_i}$$

$$z_i'\ k = \sigma_i(k)\ z_i'.$$

Por outro lado, dado $\sigma \in G$, σ se escreve de modo único na forma $\sigma = \sigma_1^{m_1} \ldots \sigma_r^{m_r}$, onde $0 \leq m_i < q_i$, $1 \leq i \leq r$. Definimos então

$$z_\sigma' = (a_1\ z_1)^{m_1} \ldots (a_r\ z_r)^{m_r} = z_1'^{m_1} \ldots z_r'^{m_r}$$

É fácil ver que dado $\sigma \in G$ existe um único $a_\sigma \in K$ não nulo tal que

$$z_\sigma' = a_\sigma\ z_\sigma \quad \text{onde} \quad z_\sigma = z_1^{m_1} \ldots z_r^{m_r}.$$

Seja então $\lambda : G \to K^*$ definida por

$$\lambda(\sigma) = a_\sigma \quad , \quad \sigma \in G.$$

É fácil ver agora que os conjuntos de fatores

$$f : G \times G \to K^* \quad e \quad g : G \times G \to K$$

definidos por

$$f(\sigma,\tau) = z_\sigma \, z_\tau (z_{\sigma\tau})^{-1} \quad e \quad g(\sigma,\tau) = z'_\sigma \, z'_\tau (z'_{\sigma\tau})^{-1}$$

são equivalentes. Logo, por [5, lema 4.4.1], segue-se que A_1 e A_2 são isomorfos como F-álgebras. □

<u>7.9 - TEOREMA</u> - Seja $K|_F$ uma extensão galoisiana com grupo de Galois abeliano G. Sejam ainda U, B $\subseteq$ K satisfazendo as condições (1), (2) e (4) da proposição (7.2). Então:

(a) Existe uma F-álgebra simples central A, que contém K como subcorpo maximal, e existem elementos inversíveis $z_1, \ldots, z_r$ em A tais que

$$A = (K, G, U, B)$$

(b) Além disto, A é única a menos de isomorfismo.

DEMONSTRAÇÃO

A existência de uma tal álgebra A é o conteúdo da proposição (7.7).

A unicidade decorre imediatamente, tomando-se $a_i = 1$, $1 \leq i \leq r$ na proposição (7.8). $\square$

Nosso próximo passo será determinar condições necessárias e suficientes para que um produto cruzado abeliano possua uma involução do primeiro tipo.

Começamos com um lema, que é uma generalização do teorema 90 de Hilbert.

7.10 - LEMA - Seja $K|_F$ uma extensão galoisiana, com grupo de Galois abeliano $G = \langle \sigma_1 \rangle \times \ldots \times \langle \sigma_r \rangle$. Sejam ainda $v_i \in K$ tais que $N_i(v_i) = 1$, $1 \leq i \leq r$. Então existe um elemento $a \in K$ tal que $v_i = \sigma_i(a)\, a^{-1}$, $1 \leq i \leq r$ se e somente se $\sigma_j(v_i)\, v_i^{-1} = \sigma_i(v_j)\, v_j^{-1}$ para todo par (i,j), $1 \leq i,j \leq r$.

DEMONSTRAÇÃO

Suponhamos que exista um elemento $a \in K$ verificando

$$v_i = \sigma_i(a)\, a^{-1}, \quad 1 \leq i \leq r$$

Então

$$\sigma_j(v_i)\ \sigma_i(v_j^{-1}) = \sigma_j(\sigma_i(a)\ a-1)\ \sigma_i(a\ \sigma_j(a^{-1})) =$$

$$= \sigma_j(\sigma_i(a)).\sigma_j(a^{-1}).\sigma_i(a).\sigma_i\sigma_j(a^{-1}) =$$

$$= \sigma_j(\sigma_i(a))\ \sigma_j(\sigma_i(a^{-1}))\ \sigma_j(a^{-1})\ \sigma_i(a) =$$

$$= \sigma_j(a^{-1})\ \sigma_i(a) = a\ \sigma_j(a^{-1})\ a^{-1}\ \sigma_i(a) =$$

$$= v_j^{-1}\ v_i$$

Logo,

$$\sigma_j(v_i)\ v_i^{-1} = \sigma_i(v_j)\ v_j^{-1}\ ,\ 1 \leq i,j \leq r\ .$$

Para demonstrarmos a recíproca usaremos indução sob $\underline{r}$.

Se $r=1$, então $G = \langle \sigma_1 \rangle$ é cíclico e o nosso lema é exatamente o Teorema 90 de Hilbert.

Suponhamos então o resultado verdadeiro para $r-1$. Logo, existe $a' \in K$ tal que $v_i = \sigma_i(a')a'^{-1}$, $1 \leq i \leq r-1$. Consideremos

$$K_r = \{x \in K \mid \sigma_i(x) = x\ ,\ 1 \leq i \leq r-1\}\ .$$

Então o conjunto $\{\sigma_r^k : K_r \to K / k = 0,\ldots,q_r-1\}$ é linearmente independente sobre K_r, pois $o(\sigma_r) = q_r$ e $[K:K_r] = q_r$, [12, teorema 30]. Assim, existe um elemento $b \in K_r$ tal que

$$a = \sum_{k=0}^{q_r-1} [\sigma_r^k(ba') \prod_{i<k} \sigma_r^i (v_r^{-1})] \neq 0 .$$

Vamos mostrar agora que $\sigma_j(a)\, a^{-1} = v_j$, $1 \leq j \leq r$.

Seja $1 \leq j < r$ fixado. Então:

$$v_j^{-1}\, \sigma_j(a) = \sum_{k=o}^{q_r-1} [v_j^{-1}\, \sigma_j(\sigma_r^k(ba')) \prod_{i<k} \sigma_r^i\, (\sigma_j(v_r^{-1}))] =$$

$$= \sum_{k=0}^{q_r-1} [v_j^{-1}\sigma_r^k(\sigma_j(ba')) \prod_{i<k} \sigma_r^i(v_r^{-1}\, \sigma_r(v_j^{-1})v_j)] =$$

$$= \sum_{k=0}^{q_r-1} [v_j^{-1}\sigma_r^k(bv_ja') \prod_{i<k} \sigma_r^i(v_r^{-1})\sigma_r^{i+1}(v_j^{-1})\sigma_r^i(v_j)] =$$

$$= \sum_{k=0}^{q_r-1} [\sigma_r^k(ba')\sigma_r^k(v_j)v_j^{-1} \prod_{i<k} \sigma_r^i(v_r^{-1}) \prod_{i<k} \sigma_r^{i+1}(v_j^{-1}) \prod_{i<k} \sigma_r(v_j)] =$$

$$= \sum_{k=0}^{q_r-1} [\sigma_r^k(ba') \prod_{i<k} \sigma_r^i(v_r^{-1})v_j^{-1}\, \sigma_r^k(v_j) \prod_{i<k} \sigma_r^{i+1}(v_j^{-1}) \prod_{i<k} \sigma_r^i(v_j)] .$$

Mas

$$v_j^{-1}\ \sigma_r^k(v_j) \prod_{i<k} \sigma_r^{i+1}(v_j^{-1}) \prod_{i<k} \sigma_r^i(v_j) = 1$$

Logo,

$$v_j^{-1}\ \sigma_j(a) = \sum_{k=0}^{q_r-1} \left[\sigma_r^k(ba') \prod_{i<k} \sigma_r^i\ (\hat{v}_r^{-1})\right] = a$$

Portanto,

$$\sigma_j(a)a^{-1} = v_j\ , \quad 1 \leq j < r\ .$$

Resta discutir o caso j=r.

Nesta situação temos:

$$v_r^{-1}\ \sigma_r(a) = v_r^{-1}\ \sigma_r\ (\sum_{k=0}^{q_r-1} (\sigma_r^k(ba') \prod_{i<k} \sigma_r^i(v_r^{-1}))) =$$

$$= v_r^{-1} \sum_{k=0}^{q_r-1} \left[\ \sigma_r^{k+1}(ba') \prod_{i<k} \sigma_r^{i+1}(v_r^{-1})\right] =$$

$$= \sum_{k=0}^{q_r-1} \left[\sigma_r^{k+1}(ba')\ v_r^{-1}\ \sigma_r(v_r^{-1}) \ldots \sigma_r^k\ (v_r^{-1})\right] =$$

$$= \sum_{k=0}^{q_r} \left[\sigma_r^{k+1}(ba') \prod_{i<k+1} \sigma_r^i(v_r^{-1})\right] =$$

$$= \sum_{k=1}^{q_r} [\sigma_r^k (ba') \prod_{i<k} \sigma_r^i (v_r^{-1})] =$$

$$= \sum_{k=1}^{q_r-1} [\sigma_r^k (ba') \prod_{i<k} \sigma_r^i (v_r^{-1})] + \sigma_r^{q_r}(ba') N_r(v_r^{-1}) =$$

$$= \sum_{k=1}^{q_r-1} [\sigma_r^k (ba') \prod_{i<k} \sigma_r^i (v_r^{-1})] + ba' = a$$

Assim , $v_r^{-1} \sigma_r(a) = a$ e o lema está demonstrado. □

Voltamos agora a estudar as propriedades dos u_{ij}'s e dos b_i's.

<u>7.11 - Observações</u> - Seja $K|_F$ uma extensão galoisiana, com grupo de Galois abeliano $G = \langle\sigma_1\rangle \times \ldots \times \langle\sigma_r\rangle$. Sejam $U = \{u_{ij} / 1 \leq i,j \leq r\}$ e $B = \{b_i / 1 \leq i \leq r\}$ subconjuntos de K. Consideremos ainda as relações (1),(2),(3) e (4) da proposição (7.2). Temos:

(a) A condição (2) é consequência apenas da condição (1), salvo quando os índices i, j, k são dois a dois distintos.

De fato, suponhamos por exemplo, que i=j. Então:

$$\sigma_i(u_{jk})\ \sigma_j(u_{ki})\ \sigma_k(u_{ij}) = \sigma_i(u_{ik})\ \sigma_i(u_{ki})\ \sigma_k(u_{ii}) =$$

$$= \sigma_i(u_{ik})\ \sigma_i(u_{ik})^{-1} = 1.$$

Por outro lado,

$$u_{jk}\ u_{ki}\ u_{ij} = u_{ik}\ u_{ki}\ u_{ii} = u_{ik}\ (u_{ik})^{-1} = 1.$$

(b) Se $b_i \in B$ satisfaz a condição (4) então $\alpha\ b_i$ também satisfaz (4) para todo $\alpha \in F$.

De fato,

$$\sigma_k(\alpha b_i) = \alpha\,\sigma_k(b_i) = \alpha\ N_k(u_{ki})\ b_i =$$

$$= N_k(u_{ki})\ (\alpha bi)\ .$$

(c) Se U e B satisfazem (1), (2) e (4), então U satisfaz (3).

Com efeito,

$$N_i\ (N_j(u_{ij})) = N_i(\sigma_i(b_j)\ b_j^{-1}) =$$

$$= N_i(\sigma_i(b_j))N_i(b_j^{-1}) =$$

$$= \sigma_i(N_i(b_j)N_i(b_j^{-1}) =$$

$$= N_i(b_j)N_i(b_j^{-1}) = 1.$$

(d) Se $U \subset K$ satisfaz (1), (2) e (3) então existe $B \subset K$, determinado a menos de multiplicação por elementos de F, satisfazendo (4).

Seja $1 \leq j \leq r$ <u>fixado</u> .

Então para cada i, $1 \leq i \leq r$, definimos:

$v_i = N_j\ (u_{ij})$

Como U satisfaz (3), segue-se que $N_i\ (v_i) = 1$, $1 \leq i \leq r$.

Vamos mostrar agora que os v_i's satisfazem a hipótese do lema (7.10).

Sejam $1 \leq i, k \leq r$. Então:

$$\sigma_k(v_i)\ \sigma_i(v_k^{-1}) = \sigma_k(N_j(u_{ij}))\ \sigma_i(N_j(u_{jk})) =$$

$$= N_j(\sigma_k(u_{ij}))\ N_i(\sigma_i(u_{jk})) =$$

$$= N_j(\sigma_k(u_{ij})\sigma_i(u_{jk})) =$$

$$= N_j(u_{jk}\ u_{ki}\ u_{ij}\ \sigma_j(u_{ki})^{-1}) =$$

$$= N_j(u_{ij})\ N_j(u_{jk})\ N_j(u_{ki}\ \sigma_j(u_{ki})^{-1}) =$$

$$= v_i\ v_k^{-1}\ N_j(u_{ki})\ \sigma_j(N_j(u_{ik})) =$$

$$= v_i\ v_k^{-1}\ N_j(u_{ki}) N_j(u_{ik}) = v_i\ v_k^{-1}\ .$$

Logo,

$$\sigma_k(v_i)\ v_i^{-1} = \sigma_i(v_k)\ v_k^{-1}\ ,\quad 1 \leq i,k \leq r.$$

Assim, pelo lema (7.10), temos que para cada j, $1 \leq j \leq r$, existe $b_j \in K$ tal que

$$v_i = \sigma_i(b_j)\ b_j^{-1}\quad ,\quad 1 \leq i \leq r.$$

Portanto

$$\sigma_i(b_j) = N_j(u_{ij})\ b_j \qquad 1 \leq i,j \leq r.$$

Conseqüentemente, existe $B=\{b_j/1 \leq j \leq r\}$ satisfazendo a condição (4).

Resta mostrar que o conjunto B está determinado salvo multiplicação por elementos de F.

Sejam então $B=\{b_i/1 \leq i \leq r\}$ e $B'=\{b_i'/1 \leq i \leq r\}$ subconjuntos de K, satisfazendo (4). Temos:

$$\sigma_j(b_i')b_i'^{-1} = \sigma_j(b_i)b_i^{-1}, \quad 1 \leq i,j \leq r.$$

Conseqüentemente,

$$\sigma_j(b_i' \, b_i^{-1}) = b_i' \, b_i^{-1} \qquad 1 \leq i,j \leq r.$$

Portanto, $b_i' \, b_i^{-1} \in F$, $1 \leq i \leq r$, donde

$b_i' = \alpha_i \, b_i$, $\alpha_i \in F$, $1 \leq i \leq r$. $\square$

Daqui por diante assumiremos que G é abeliano da forma $G = \langle \sigma_1 \rangle \times \ldots \times \langle \sigma_r \rangle$, com $o(\sigma_i) = 2$, $1 \leq i \leq r$.

<u>7.12 - TEOREMA</u> - Sejam $A = (K, G, U, B)$ e $\tau \in G$. As seguintes condições são equivalentes:

(i) A possui uma involução do 1º tipo.

(ii) A possui uma involução, cuja restrição a K coincide com τ.

(iii) Existem $\bar{U}=\{\bar{u}_{ij}/1 \leq i,j \leq r\}$ e $\bar{B}=\{\bar{b}_i/1 \leq i \leq r\}$ subconjuntos de K e $\{\bar{z}_1,\ldots,\bar{z}_r\} \subset A$ tais que $A=(K, G, \bar{U}, \bar{B})$, de modo que $\bar{U}$ e $\bar{B}$ verificam ainda as seguintes condições:

(5) $\tau(\bar{u}_{ij}) \, \sigma_i \, \sigma_j \, (\bar{u}_{ij}) = 1$

$$(6)\quad \tau(\bar{b}_i) = \bar{b}_i \qquad 1 \leq i,j \leq r.$$

Mais ainda, podemos escolher uma involução * e elementos $\{\bar{z}_1,\ldots,\bar{z}_r\}$ tais que $\bar{z}_i^* = \pm\, \bar{z}_i$, $1 \leq i \leq r$, e a restrição de * a K coincide com τ.

DEMONSTRAÇÃO

(i) => (ii)

Seja $* : A \to A$ uma involução do primeiro tipo. Consideremos $K^* = \{k^* \mid k \in K\}$. Então a composição de * e τ é um isomorfismo de F-subálgebras simples de A. Logo, pelo teorema de Skolem-Nöether, [5, teorema 4.3.1], existe um elemento inversível $y \in A$ tal que

$$\tau(k)^* = y\, k\, y^{-1}, \text{ para todo } k \in K.$$

Em outras palavras, existe um elemento inversível $y \in A$ tal que

$$\tau(k) = (y^{-1})^*\, k^*\, y^*, \quad \forall\, k \in K.$$

Se $y + y^* = 0$, então $y^* = -y$ e definimos $J(x) = y^{-1} x^* y$, $x \in A$. É fácil ver que J é uma involução em A. Vamos mostrar que $J|_K = \tau$.

Com efeito, seja $k \in K$ qualquer.

Temos:

$$\tau(k) = (y^{-1})^* k^* y^* = y^{-1} k^* y = J(k).$$

Se $y + y^* \neq 0$, consideremos $\alpha = y + y^*$. Então $\alpha^* = \alpha$ e $(y^{-1})^* y \in C_A(K) = K$, pois $\tau^2 = I_K$. Logo, $y^* \in yK$. Como $y \in yK$, decorre que $\alpha \in yK$. Suponhamos então que $\alpha = y\, k_0$, com $k_o \in K$. Definimos

$$J(x) = \alpha^{-1} x^* \alpha, \quad x \in A .$$

Novamente é fácil verificar que J é uma involução em A. Resta provar que $J|_K = \tau$. Para isto, consideremos um elemento $k \in K$, qualquer. Temos então:

$$\tau(k)^* = y\, k\, y^{-1} = \alpha(k_0^{-1}\, k\, k_0)\, \alpha^{-1} - \alpha k \alpha^{-1} .$$

Como $\alpha^* = \alpha$, segue-se que

$$\tau(k) = (\alpha^{-1})^* k^* \alpha^* = \alpha^{-1} k^* \alpha = J(k) .$$

(ii) => (i)

Se A possui uma involução, cuja restrição a K coincide com τ, então é claro que esta involução é do primeiro tipo, pois $F \subset K$ e τ fixa os elementos de F.

(ii) => (iii)

Seja * uma involução em A cuja restrição a K é τ. Sejam ainda $\{z_1,\ldots,z_r\} \subset A$ tais que $z_i z_j = u_{ij} z_j z_i$ e $b_i = z_i^2$, $1 \leq i,j \leq r$. Suponhamos, por um instante, que $z_i^{-1} z_i^* \in K$, $1 \leq i \leq r$. Neste caso, $z_i^* \in z_i K$ e portanto $z_i + \alpha z_i^* \in z_i K$, para todo $\alpha \in F$, $1 \leq i \leq r$. Desta forma, para cada índice i, $1 \leq i \leq r$, podemos escolher $\mu_i \in \{-1,1\}$ de modo que

$$\bar{z}_i = z_i + \mu_i z_i^* \in z_i K - \{0\} .$$

Assim, existem $k_1,\ldots,k_r \in K$ não nulos tais que $\bar{z}_i = z_i k_i$, $1 \leq i \leq r$. É fácil verificar que nesta situação

$$\sigma_i(k) = \bar{z}_i k \bar{z}_i^{-1}, \quad \forall \ k \in K.$$

Vamos mostrar que, de fato, $z_i^{-1} z_i^* \in K$, $1 \leq i \leq r$. Para isto, consideremos um elemento qualquer $k \in K$. Então $z_i k = \sigma_i(k) z_i$, $1 \leq i \leq r$. Logo

$$(z_i k)^* = (\sigma_i(k) z_i)^* = z_i^* \sigma_i(k)^* .$$

Mas a restrição de * a K é τ, donde segue-se que:

$$\tau(k) z_i^* = z_i^* \tau(\sigma_i(k)), \quad \forall \ k \in K, \quad 1 \leq i \leq r.$$

Substituindo k por $\tau(\sigma_i(k))$ na igualdade acima e lembrando que $o(\sigma_i) = o(\tau) = 2$, $1 \leq i \leq r$, obtemos:

$$\sigma_i(k)\ z_i^* = z_i^*\ k\ ,\quad \forall\ k \in K,\quad 1 \leq i \leq r.$$

Logo,

$$(z_i^{-1}z_i^*)\ k = z_i^{-1}\ \sigma_i(k)\ z_i^* = k(z_i^{-1}z_i^*),\quad \forall\ k \in K\ ,$$
$$1 \leq i \leq r\ .$$

Assim, $z_i^{-1}z_i^* \in C_A(K) = K,\quad 1 \leq i \leq r.$

Definimos então

$$\bar{u}_{ij} = \bar{z}_i\bar{z}_j\bar{z}_i^{-1}\bar{z}_j^{-1} \quad \text{e}\ \bar{b}_i = \bar{z}_i^2\ ,\quad 1 \leq i,j \leq r.$$

Se indicarmos $\bar{U} = \{\bar{u}_{ij} \mid 1 \leq i,j \leq r\}$ e $\bar{B} = \{\bar{b}_i \mid 1 \leq i \leq r\}$ então é claro que $A = (K\ ,\ G,\ \bar{U},\ \bar{B})$. Vamos mostrar que os conjuntos $\bar{U}$ e $\bar{B}$ satisfazem as relações (5) e (6). Para isto, observemos que $\bar{z}_i^* = \mu_i\bar{z}_i$, onde $\mu_i \in \{-1,1\}$, $1 \leq i \leq r$.

Com isto, temos:

$$\tau(\bar{b}_i) = \tau(\bar{z}_i^2) = (\bar{z}_i^2)^* = \bar{z}_i^*.\bar{z}_i^* = (\bar{z}_i)^2 = \bar{b}_i,\quad 1 \leq i \leq r$$

e

$$\tau(\bar{u}_{ij}) = (\bar{z}_i\bar{z}_j\bar{z}_i^{-1}\bar{z}_j^{-1})^* = \mu_j\bar{z}_j^{-1}\mu_i\bar{z}_i^{-1}\mu_j\bar{z}_j\mu_i\bar{z}_i = \mu_i^2\mu_j^2\bar{z}_j^{-1}\bar{z}_i^{-1}\bar{z}_j\bar{z}_i =$$

$$= \bar{z}_j^{-1}\bar{z}_i^{-1}\ \bar{u}_{ji}\bar{z}_i\bar{z}_j = \sigma_j^{-1}(\sigma_i^{-1}(\bar{u}_{ji})) = \sigma_i(\sigma_j(\bar{u}_{ji}))\ ,$$

já que $o(\sigma_k) = 2$, $1 \leq k \leq r$, e G é abeliano.

Logo,

$$\tau(\bar{u}_{ij})\ \sigma_i(\sigma_j(\bar{u}_{ij}))=1, \quad 1 \leq i,j \leq r .$$

(iii) $\Longrightarrow$ (ii)

Suponhamos que existam $\bar{U}$, $\bar{B} \subset K$ e $\{\bar{z}_1,\ldots,\bar{z}_r\} \subset A$ tais que $\bar{U}$, $\bar{B}$ satisfaçam (5) e (6) e $A = (K, G, \bar{U}, \bar{B})$.

É fácil ver que todo elemento de A se escreve de modo único na forma

$\sum_\alpha k_\alpha \bar{z}_1^{\alpha_1} \ldots \bar{z}_r^{\alpha_r}$, onde a soma se estende a todas as r-uplas $\alpha = (\alpha_1,\ldots,\alpha_r) \in \{0,1\}^r$ e $k_\alpha \in K$.

Definimos então $*: A \to A$ por

$$\left(\sum_\alpha k_\alpha \bar{z}_1^{\alpha_1} \ldots \bar{z}_r^{\alpha_r}\right)^* = \sum_\alpha \bar{z}_r^{\alpha_r} \ldots \bar{z}_1^{\alpha_1}\ \tau(k_\alpha)$$

Devemos mostrar que * é uma involução em A cuja restrição a K é τ. Para isto, observemos os seguintes fatos:

a) $k^* = \tau(k), \quad \forall\ k \in K.$

b) $(k_1k_2)^* = \tau(k_1k_2) = \tau(k_1k_2) = (k_2k_1)^*, \ \forall\ k_1,k_2 \in K.$

c) $(k\bar{z}_1)^* = \bar{z}_i\ \tau(k) = \bar{z}_i^*\ k^* \quad \forall\ k \in K, \quad 1 \leq i \leq r.$

d) $(\bar{z}_i^2)^* = \bar{b}_i^* = \tau(\bar{b}_i) = \bar{b}_i = (\bar{z}_i^*)^2, \quad 1 \leq i \leq r$

e) Se $i < j$ então $(\bar{z}_i\bar{z}_j)^* = \bar{z}_j\bar{z}_i = \bar{z}_j^*\,\bar{z}_i^*$

Se $i > j$ então

$$(\bar{z}_i\bar{z}_j)^* = (\bar{u}_{ij}\bar{z}_j\bar{z}_i) = \bar{z}_i\bar{z}_j \quad \tau(\bar{u}_{ij}) =$$

$$= \bar{z}_i\bar{z}_j \;\sigma_i(\sigma_j(\bar{u}_{ji})) = z_i\sigma_j(\sigma_i(\sigma_j(\bar{u}_{ji})))\bar{z}_j =$$

$$= \bar{z}_i\sigma_i(\bar{u}_{ji})\bar{z}_j = \sigma_i^2(\bar{u}_{ji})\;\bar{z}_i\bar{z}_j =$$

$$= \bar{u}_{ji}\;\bar{z}_i\bar{z}_j = \bar{z}_j\;\bar{z}_i = \bar{z}_j^*\;\bar{z}_i^*$$

Logo, * é um anti-automorfismo de A e portanto só resta provar que $(x^*)^* = x$, $\forall\, x \in A$.

Seja $x = \sum_\alpha k_\alpha\, z_1^{\alpha_1}\ldots z_r^{\alpha_r}$. Então

$$(x^*)^* = \Big(\sum_\alpha \bar{z}_r^{\alpha_r}\ldots\bar{z}_1^{\alpha_1}\;\tau(k_\alpha)\Big)^* = \sum_\alpha (\bar{z}_r^{\alpha_r}\ldots\bar{z}_1^{\alpha_1}\;(k\alpha))^*$$

$$= \sum_\alpha \tau(k_\alpha)^*\,\bar{z}_1^{\alpha_1}\ldots\bar{z}_r^{\alpha_r} = \sum_\alpha \tau(\tau(k\alpha))\;\bar{z}_1^{\alpha_1}\ldots\bar{z}_r^{\alpha_r}$$

$$= \sum_\alpha k_\alpha\,\bar{z}_1^{\alpha_1}\ldots\bar{z}_r^{\alpha_r} = x \qquad \square$$

§ 8 - PRODUTOS CRUZADOS ABELIANOS DE GRAU 8 COM INVOLUÇÃO

Em todo este parágrafo $K/_F$ denotará uma extensão galoisiana, com grupo de Galois abeliano $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle$ onde $o(\sigma_i) = 2$, $1 \leq i \leq 3$.

Observemos que, nesta situação, existem elementos $\xi_1, \xi_2, \xi_3 \in K$ com as seguintes propriedades:

(a) $\xi_i^2 = \alpha_i \in F - \{0\}$

(b) $\sigma_i(\xi_i) = -\xi_i$ e $\sigma_i(\xi_j) = \xi_j$ se $i \neq j$, $1 \leq i,j \leq 3$.

(c) $K = F(\xi_1, \xi_2, \xi_3)$.

Passaremos a estudar propriedades dos conjuntos $U, B \subset K$ introduzidos anteriormente nesta circunstância particular, que serão usadas mais tarde quando da construção dos contra-exemplos à conjectura de Albert, formulada na introdução deste trabalho.

Dada uma permutação $\Pi \in S_3$, denotaremos abreviadamente $\Pi_i = \Pi(i)$, $i = 1,2,3$.

8.1 - PROPOSIÇÃO (a) Seja $U \subset K$ satisfazendo as condições

(1) e (2) da proposição (7.2) e (5) do teorema (7.12), para $\tau = \sigma_1\sigma_2\sigma_3$.

Sejam $v_3=u_{12}$, $v_2=u_{31}$ e $v_1=u_{23}$. Então para toda permutação $\Pi \in S_3$ temos que $v_{\Pi 3} = (u_{\Pi 1,\Pi 2})^{sg\Pi}$. Além disso, o conjunto $V = \{v_1, v_2, v_3\}$ satisfaz as seguintes relações:

(2') $v_1v_2v_3 = \pm 1$

(3') $N_i(v_i) = 1$, $i = 1,2,3.$

(b) Reciprocamente, se $V = \{v_1,v_2,v_3\} \subset K$ satisfaz (2') e (3') então podemos definir para cada permutação $\Pi \in S_3$

$$u_{\Pi 1,\Pi 2}=(v_{\Pi 3})^{sg\Pi} \quad e \quad u_{ii} = 1, \quad i = 1,2,3 .$$

Então $U = \{u_{ij}/ 1 \leq i,j \leq 3\}$ está bem definido e satisfaz as condições (1) e (2) da proposição (7.2) e (5) da proposição (7.12) para $\tau= \sigma_1\sigma_2\sigma_3$.

<u>DEMONSTRAÇÃO</u>

(a) Seja $\Pi \in S_3$ uma permutação qualquer. O fato de que

$$v_{\Pi 3} = (u_{\Pi 1,\Pi 2})^{sg\Pi}$$

decorre facilmente da definição dos v_i's.

Por outro lado, sendo G abeliano, temos que $\tau = \sigma_1\sigma_2\sigma_3 =$
$= \sigma_{\Pi 1}\sigma_{\Pi 2}\sigma_{\Pi 3}$.

Como U verifica a condição (5) para $\tau = \sigma_1\sigma_2\sigma_3$, temos:

$$\sigma_{\Pi 1}\sigma_{\Pi 2}\sigma_{\Pi 3}\ (u_{\Pi 1,\Pi 2})\sigma_{\Pi 1}\ \sigma_{\Pi 2}\ (u_{\Pi 1,\Pi 2}) = 1.$$

Logo,

$$\sigma_{\Pi 3}(\sigma_{\Pi 1}\sigma_{\Pi 2}\ (u_{\Pi 1,\Pi 2}))\cdot\sigma_{\Pi 1}\sigma_{\Pi 2}\ (u_{\Pi 1,\Pi 2}) =$$

$$= N_{\Pi 3}(\sigma_{\Pi 1}\sigma_{\Pi 2}(u_{\Pi 1,\Pi 2}))=\sigma_{\Pi 1}\sigma_{\Pi 2}(N_{\Pi 3}(u_{\Pi 1,\Pi 2})) = 1.$$

Conseqüentemente,

$$\sigma_{\Pi 1}\sigma_{\Pi 2}(N_{\Pi 3}(v_{\Pi 3})^{sg\Pi}) = 1.$$

Aplicando $\sigma_{\Pi 1}\cdot\sigma_{\Pi 2}$ a ambos os membros desta igualdade e lembrando que $o(\sigma_{\Pi i}) = 2$, $1 \leq i \leq 3$, obtemos:

$$N_{\Pi 3}(v_{\Pi 3}) = \sigma_{\Pi 1}\ \sigma_{\Pi 2}(1) = 1.$$

Assim, $N_i(v_i) = 1$, $1 \leq i \leq 3$.

Como $N_i(v_i) = 1$ então

$v_i\ \sigma_i(v_i) = 1$, para $i = 1,2,3$. Logo,

$$\sigma_i(v_i) = v_i^{-1} \ , \ i = 1, 2, 3.$$

Portanto

$$v_1^{-1} v_2^{-1} v_3^{-1} = \sigma_1(v_1) \ \sigma_2(v_2) \ \sigma_3(v_3) =$$

$$= \sigma_1(u_{23}) \ \sigma_2(u_{31}) \ \sigma_3(u_{12}).$$

Mas U verifica a condição (2) da proposição(7.2).Logo,

$$v_1^{-1} \ v_2^{-1} \ v_3^{-1} = u_{23} \ u_{31} \ u_{12} = v_1 \ v_2 \ v_3$$

Por outro lado, os v_i's são elementos de K, donde comutam entre si. Assim, da igualdade acima decorre imediatamente que $(v_1 v_2 v_3)^2 = 1$, e portanto

$$v_1 v_2 v_3 = \pm 1 \ .$$

(b) É claro que U está bem definido pois dada uma permutação $\Pi \in S_3$, Π está determinada por $\Pi(3) = \Pi 3$ e por $sg(\Pi)$. Vamos provar que U satisfaz a condição (1) da proposição (7.2). Para isso, consideremos uma permutação $\Pi \in S_3$ qualquer e seja $\gamma \in S_3$ definida por

$$\gamma = (\Pi 1 \ , \Pi 2) \ o \ \Pi$$

Então $sg\,\gamma = -sg\Pi$ e temos

$$u_{\Pi 2,\Pi 1} = u_{\gamma 1,\gamma 2} = [v_{\gamma 3}]^{sg\gamma} = v_{\Pi 3}^{-sg\Pi} =$$

$$= [u_{\Pi 1,\Pi 2}]^{-1}.$$

Para provarmos que U satisfaz a condição (5) para $\tau=\sigma_1\sigma_2\sigma_3$, observemos que se i=j então, esta condição se verifica trivialmente. Logo, podemos supor que $i\neq j$ e portanto existe uma permutação $\Pi \in S_3$ tal que $\Pi 1 = i$, $\Pi 2 = j$. Neste caso, por (3') temos:

$$\sigma_{\Pi 1}\ \sigma_{\Pi 2}(N_{\Pi 3}(v_{\Pi 3})^{sg\Pi}) = 1$$

Conseqüentemente,

$$1 = \sigma_{\Pi 1}\sigma_{\Pi 2}(u_{\Pi 1,\Pi 2}\sigma_{\Pi 3}(u_{\Pi 1,\Pi 2})) =$$

$$= \sigma_{\Pi 1}\sigma_{\Pi 2}(u_{\Pi 1,\Pi 2})\ \sigma_{\Pi 1}\ \sigma_{\Pi 2}\ \sigma_{\Pi 3}(u_{\Pi 1,\Pi 2})$$

Mas G é abeliano; logo $\tau = \sigma_1\sigma_2\sigma_3 = \sigma_{\Pi 1}\ \sigma_{\Pi 2}\ \sigma_{\Pi 3}$

Assim

$$\sigma_{\Pi 1}\ \sigma_{\Pi 2}(u_{\Pi 1,\Pi 2}) \cdot \tau(u_{\Pi 1,\Pi 2}) = 1$$

e portanto U verifica a condição (5) para $\tau = \sigma_1\sigma_2\sigma_3$.

Para provarmos que U satisfaz (2), lembremos que se dois dos índices forem iguais, essa condição é conseqüência a

penas da condição (1) (veja observação (7.11, a)). Logo, podemos supor que os índices i,j, k são dois a dois distintos. Assim, existe uma permutação $\Pi \in S_3$ tal que $\Pi 1=i$, $\Pi 2=j$, $\Pi 3=k$. Então:

$$\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij})=\sigma_{\Pi 1}(u_{\Pi 2,\Pi 3})\sigma_{\Pi 2}(u_{\Pi 3,\Pi 1})\sigma_{\Pi 3}(u_{\Pi 1,\Pi 2})$$

Consideremos $\delta = \Pi \circ (1\ 2\ 3)$ e $\gamma = \Pi \circ (1\ 3\ 2)$. Então $sg\,\delta = sg\gamma = sg\Pi$ e temos:

$$\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij})=\sigma_{\delta 3}(u_{\delta 1,\delta 2})\sigma_{\gamma 3}(u_{\gamma 1,\gamma 2})\sigma_{\Pi 3}(u_{\Pi 1,\Pi 2}) =$$

$$=\sigma_{\delta 3}(v_{\delta 3}^{sg\delta})\ \sigma_{\gamma 3}(v_{\gamma 3}^{sg\gamma})\ \sigma_{\Pi 3}(v_{\Pi 3}^{sg\Pi})$$

Por outro lado, como $V = \{v_1,v_2,v_3\}$ satisfaz (2') e (3') é fácil ver que

$$v_1\ v_2\ v_3 = v_1^{-1}\ v_2^{-1}\ v_3^{-1} = \sigma_1(v_1)\ \sigma_2(v_2)\ \sigma_3(v_3)$$

Assim, temos:

$$\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij})=\left[\sigma_{\delta 3}(v_{\delta 3})\sigma_{\gamma 3}(v_{\gamma 3})\ \sigma_{\Pi 3}(v_{\Pi 3})\right]^{sg\Pi} =$$

$$= (v_{\delta 3}\ v_{\gamma 3}\ v_{\Pi 3})^{sg\Pi} =$$

$$= v_{\delta 3}^{sg\delta}\ v_{\gamma 3}^{sg\gamma}\ v_{\Pi 3}^{sg\Pi} =$$

$$= u_{\delta 1,\delta 2} \cdot u_{\gamma 1,\gamma 2} \cdot u_{\Pi 1,\Pi 2} =$$

$$= u_{jk} \cdot u_{ki} \cdot u_{ij} .$$

Logo, U satisfaz a condição (2). $\square$

<u>8.2 - PROPOSIÇÃO</u> - Seja $U \subseteq K$ satisfazendo as condições (1) e (2) da proposição (7.2) e (5) da proposição (7.12) para $\tau = \sigma_1 \sigma_2 \sigma_3$. Sejam ainda $v_3 = u_{12}$, $v_2 = u_{31}$ e $v_1 = u_{23}$. Então existe $B = \{b_1, b_2, b_3\} \subset K$, determinado a menos de multiplicação por elementos de F, satisfazendo as seguintes condições, para toda permutação $\Pi \in S_3$:

$$(4') \quad \sigma_{\Pi 1}(b_{\Pi 2})\, b_{\Pi 2}^{-1} = N_{\Pi 2}\, (v_{\Pi 3})^{sg\Pi}$$

$$(5') \quad \sigma_i(b_i) = b_i \qquad i = 1,2,3.$$

Além disso, os conjuntos U, $B \subseteq K$ satisfazem as condições (3) e (4) da proposição (7.2) e a condição (6) da proposição (7.12), para $\tau = \sigma_1 \sigma_2 \sigma_3$.

<u>DEMONSTRAÇÃO</u>

Vamos mostrar que U satisfaz (3). Pela proposição

anterior, sabemos que $V=\{v_1,v_2,v_3\}$ satisfaz (2') e (3'). Dada uma permutação $\Pi \in S_3$, temos:

$$N_{\Pi 1}(N_{\Pi 2}(u_{\Pi 1,\Pi 2})) = N_{\Pi 1}(N_{\Pi 2}(v_{\Pi 3}{}^{sg\Pi})) =$$

$$= N_{\Pi 1}(N_{\Pi 2}(v_{\Pi 1}^{-1}\ v_{\Pi 2}^{-1}))^{sg\Pi} =$$

$$= N_{\Pi 2}(N_{\Pi 1}(v_{\Pi 1}))^{-sg\Pi}\ N_{\Pi 1}(N_{\Pi 2}(v_{\Pi 2}))^{-sg\Pi} =$$

$$= N_{\Pi 2}(1)\ .\ N_{\Pi 1}(1) = 1.$$

Logo, se $1 \leq i,j \leq 3$ e $i \neq j$, temos que

$$N_i(N_j(u_{ij}) = 1\ .$$

Por outro lado, se $i = j$ então $u_{ij} = 1$ e portanto $N_i(N_i(u_{ii})) = 1$.

Assim, $N_i(N_j(u_{ij})) = 1$, $i,j = 1,2,3$, donde U verifica (3).

Logo, U satisfaz as condições (1), (2) e (3). Assim, pela observação (7.11,d), segue-se que existe $B=\{b_1,b_2,b_3\} \subset K$, determinado salvo multiplicação por elementos de F, satisfazendo a condição (4). Assim,

$$\sigma_j(b_i)\ b_i^{-1} = N_i(u_{ji}) \qquad 1 \leq i,j \leq 3\ .$$

Mas se $j \neq i$ então existe uma permutação $\Pi \in S_3$ tal que $\Pi 1 = j$ e $\Pi 2 = i$. Logo,

$\sigma_{\Pi 1}(b_{\Pi 2})\ b_{\Pi 2}^{-1} = N_{\Pi 2}(u_{\Pi 1, \Pi 2}) = N_{\Pi 2}(v_{\Pi 3})^{sg\Pi}$, donde vale (4').

Se $j=i$ então

$$\sigma_i(b_i)\ b_i^{-1} = N_i(u_{ii}) = N_i(1) = 1.$$

Logo, $\sigma_i(b_i) = b_i \quad 1 \leq i \leq 3$ e portanto vale (5').

Resta agora mostrar que B satisfaz a condição (6) para $\tau = \sigma_1 \sigma_2 \sigma_3$, ou seja, devemos provar que $\tau(b_i) = b_i$, $1 \leq i \leq 3$.

Seja $\Pi \in S_3$ uma permutação qualquer e consideremos $\gamma = (\Pi 1, \Pi 2)$. Então $sg(\gamma_o \Pi = - sg\Pi$. Aplicando a relação (4') a $\gamma_o \Pi \in S_3$, obtemos:

$$\sigma_{\Pi 2}\ (b_{\Pi 1})\ b_{\Pi 1}^{-1} = N_{\Pi 1}\ (v_{\Pi 3})^{-sg\Pi} = N_{\Pi 1}\ (v_{\Pi 1}\ v_{\Pi 2})^{sg\Pi} =$$

$$= N_{\Pi 1}\ (v_{\Pi 2})^{sg\Pi}.$$

Consideremos ainda $\delta = \Pi o\ (132) \in S_3$. Então $sg\delta = sg\Pi$ e aplicando novamente (4') a δ, obtemos:

$$N_{\Pi 1}\ (v_{\Pi 2})^{sg\Pi} = \sigma_{\Pi 3}\ (b_{\Pi 1})\ b_{\Pi 1}^{-1}$$

Assim, comparando as duas igualdades obtidas, vem:

$$\sigma_{\Pi 2}\ (b_{\Pi 1})\ b_{\Pi 1}^{-1} = \sigma_{\Pi 3}\ (b_{\Pi 1})\ b_{\Pi 1}^{-1}$$

Logo,

$$\sigma_{\Pi 2}\ (b_{\Pi 1}) = \sigma_{\Pi 3}\ (b_{\Pi 1}).$$

Mas $\tau(b_{\Pi 1}) = \sigma_{\Pi 1}\ \sigma_{\Pi 2}\ \sigma_{\Pi 3}\ (b_{\Pi 1})$, donde

$$\tau(b_{\Pi 1}) = \sigma_{\Pi 1}\ (\sigma_{\Pi 2}(\sigma_{\Pi 2}(b_{\Pi 1}))) = \sigma_{\Pi 1}\ (b_{\Pi 1}) = b_{\Pi 1}.$$

Assim, $\tau(b_i) = b_i$, $i = 1,2,3$ e portanto $B=\{b_i/1 \leq i \leq 3\}$ verifica (6) para $\tau = \sigma_1\sigma_2\sigma_3$. $\square$

<u>(8.3) - Observação</u> . Da demonstração da proposição anterior , decorre que se $B \subset K$ satisfaz (4') e (5') então para toda permutação $\Pi \in S_3$, temos que:

$$\sigma_{\Pi 2}\ (b_{\Pi 1}) = \sigma_{\Pi 3}\ (b_{\Pi 1}).$$

As proposições (8.1) e (8.2) nos fornecem algumas propriedades interessantes do conjunto $B \subseteq K$ determinado em (8.2).

(8.4) - COROLÁRIO - (a) Seja $B=\{b_1, b_2, b_3\}$ como na proposição (8.2). Então para toda permutação $\Pi \in S_3$, temos que

$$b_{\Pi 1} \in F(\xi_{\Pi 2} \cdot \xi_{\Pi 3}) \cap F(\xi_{\Pi 2})N_{\Pi 1}(K).$$

Em particular,

$$(7) \qquad b_1 \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K).$$

(b) Reciprocamente, seja

$$0 \neq b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K).$$

Então existe $V = \{v_1, v_2, v_3\} \subset K$ satisfazendo as condições (2') e (3') da proposição (8.1) e um correspondente conjunto $B= \{b_1,b_2,b_3\} \subset K$ satisfazendo as condições (4') e (5') da proposição (8.2). Além disso, podemos escolher $b_1 = b$.

DEMONSTRAÇÃO

(a) Seja $\Pi \in S_3$ uma permutação qualquer. Então $\sigma_{\Pi 1}(b_{\Pi 1}) = b_{\Pi 1}$. Além disso, pela observação (8.3), temos que $\sigma_{\Pi 2}(b_{\Pi 1}) = \sigma_{\Pi 3}(b_{\Pi 1})$. Logo, $\sigma_{\Pi 2}(\sigma_{\Pi 3}(b_{\Pi 1})) = b_{\Pi 1}$. Assim, $b_{\Pi 1}$ é invariante por $\sigma_{\Pi 1}$ e $\sigma_{\Pi 2}\sigma_{\Pi 3}$. Daí decorre que $b_{\Pi 1} \in F(\xi_{\Pi 2} \cdot \xi_{\Pi 3})$.

Por outro lado, $N_{\Pi 3}(v_{\Pi 3}) = 1$. Logo, pelo teorema 90

de Hilbert [12, pag. 42] segue-se que existe $z \in K - \{0\}$ tal que $v_{\Pi 3} = \dfrac{z}{\sigma_{\Pi 3}(z)}$. Como $z \in K - \{0\}$, existe $y \in K - \{0\}$ tal que $\sigma_{\Pi 3}(y) = z$. Deste modo, como $o(\sigma_{\Pi 3}) = 2$, temos que $v_{\Pi 3} = \sigma_{\Pi 3}(y) y^{-1}$.

Consideremos $\gamma \in S_3$ definida por $\gamma = (\Pi 1, \Pi 2) \circ \Pi$; Então $sg\gamma = -sg\Pi$. Aplicando (4') a γ e lembrando que $\sigma_{\Pi 3}(b_{\Pi 1}) = \sigma_{\Pi 2}(b_{\Pi 1})$, temos que:

$$\sigma_{\Pi 2}(b_{\Pi 1})\ b_{\Pi 1}^{-1} = N_{\Pi 1}(v_{\Pi 3})^{-sg\Pi}$$

Logo,

$$\sigma_{\Pi 3}(b_{\Pi 1})\ b_{\Pi 1}^{-1} = N_{\Pi 1}(v_{\Pi 3})^{-sg\Pi} =$$

$$= N_{\Pi 1}(\sigma_{\Pi 3}(y)\ y^{-1})^{-sg\Pi}.$$

Consideremos $w = b_{\Pi 1}\ N_{\Pi 1}(y)^{sg\Pi}$. É fácil ver que $\sigma_{\Pi 3}(w) = w$. Por outro lado, $N_{\Pi 1}(y)$ é invariante por $\sigma_{\Pi 1}$. Como $b_{\Pi 1}$ é invariante por $\sigma_{\Pi 1}$, vem que w é invariante por $\sigma_{\Pi 1}$.

Logo, w é invariante por $\sigma_{\Pi 1}$ e $\sigma_{\Pi 3}$, donde decorre que $w \in F(\xi_{\Pi 2})$.

Mas $w = b_{\Pi 1}\ N_{\Pi 1}(y^{sg\Pi})$; conseqüentemente

$$b_{\Pi 1} = w\ N_{\Pi 1}(y^{-sg\Pi}) \in F(\xi_{\Pi 2})\ N_{\Pi 1}(K).$$

Portanto, para toda permutação $\Pi \in S_3$,

$$b_{\Pi 1} \in F(\xi_{\Pi 2} \cdot \xi_{\Pi 3}) \cap F(\xi_{\Pi 2}) \cdot N_{\Pi 1}(K)$$

Em particular, tomando-se Π igual a identidade, vem que:

$$b_1 \in F(\xi_2 \xi_3) \cap F(\xi_2)\ N_1(K).$$

Ainda, tomando-se $\Pi = (23)$, vem que:

$$b_1 \in F(\xi_2 \xi_3) \cap F(\xi_3)\ N_1(K).$$

Logo,

$$b_1 \in F(\xi_2 \xi_3) \cap F(\xi_2)\ N_1(K) \cap F(\xi_3)\ N_1(K).$$

(b) Seja $0 \neq b \in F(\xi_2)\ N_1(K) \cap F(\xi_3)\ N_1(K)$.

Então existem elementos $a_2 \in F(\xi_2)$, $a_3 \in F(\xi_3)$ e $y_2, y_3 \in K$ tais que

$$b = a_2\ N_1(y_2) = a_3\ N_1\ (y_3^{-1})$$

Definimos

$$v_2 = \sigma_2(y_3^{-1})y_3,\ v_3 = \sigma_3(y_2^{-1})y_2 \quad e \quad v_1 = (v_2 v_3)^{-1}$$

É claro que $v_1 v_2 v_3 = 1$, donde $V = \{v_1, v_2, v_3\}$ satisfaz

(2') . Além disso, é fácil ver que $N_2(v_2)=N_3(v_3)=1$. Vamos mostrar que $N_1(v_1)=1$. Para isso, calculemos $N_1(v_3)$ e $N_1(v_2)$. Temos:

$$N_1(v_3)^{-1}=N_1(y_2^{-1})\ N_1(\sigma_3(y_2)) = N_1(y_2)^{-1}\ \sigma_3(N_1(y_2)) =$$

$$= b^{-1}\ a_2\ \sigma_3(a_2^{-1}\ b) = b^{-1}\ a_2\ \sigma_3(a_2)^{-1}\ \sigma_3(b) =$$

$$= b^{-1}\ a_2\ a_2^{-1}\ \sigma_3(b) = b^{-1}\ \sigma_3(b)$$

pois $a_2 \in F(\xi_2)$ e $b \in F(\xi_2\xi_3)$.

$$N_1(v_2) = N_1(y_3)\ N_1(\sigma_2(y_3))^{-1} = N_1(y_3)\ \sigma_2(N_1(y_3^{-1})) =$$

$$= a_3\ b^{-1}\ \sigma_2(a_3^{-1})\ \sigma_2(b) = a_3\ a_3^{-1}\ b^{-1}\ \sigma_2(b) =$$

$$= b^{-1}\ \sigma_2(b) = b^{-1}\ \sigma_3(b),$$

pois $a_3 \in F(\xi_3)$ e $b \in F(\xi_2 \cdot \xi_3)$.

Logo,

$$N_1(v_1)=N_1(v_2v_3)^{-1}=N_1(v_2^{-1})N_1(v_3^{-1})= \sigma_3(b)^{-1}b\ b^{-1}\sigma_3(b) = 1.$$

Assim, $V = \{v_1,v_2,v_3\}$ satisfaz (3'). Portanto, pela proposição (8.1,b), existe $U = \{u_{ij} \mid 1 \leq i,j \leq 3\} \subset K$ sa

tisfazendo as condições (1) e (2) da proposição (7.2) e (5) da proposição (7.12) , para $\tau = \sigma_1\sigma_2\sigma_3$. Conseqüentemente, U satisfaz as hipóteses da proposição (8.2), donde decorre que existe $B = \{b_1, b_2, b_3\} \subset K$ satisfazendo as condições (4') e (5'). Mas de (5') segue-se que $\sigma_1(b_1)=b_1$. Além disso, pela observação (8.3), temos que $\sigma_2(b_1) = \sigma_3(b_1)$; logo $b_1 \in F(\xi_2\xi_3)$. Como $b \in F(\xi_2\xi_3)$, segue-se também que $b.b_1^{-1} \in F(\xi_2\xi_3)$. Vamos mostrar que na realidade $bb_1^{-1} \in F$, donde seguirá, pela observação (7.11,b) que podemos tomar $b_1=b$. Para isto, basta verificar que

$$\sigma_2(bb_1^{-1}) = \sigma_3(bb_1^{-1}) = \sigma_1(bb_1^{-1}) = bb_1^{-1}.$$

Como $bb_1^{-1} \in F(\xi_2\xi_3)$, é imediato que $\sigma_1(bb_1^{-1}) = bb_1^{-1}$.

Por outro lado,

$$\sigma_2(bb_1^{-1})\ (bb_1^{-1})^{-1} = \sigma_2(b)\ \sigma_2(b_1)^{-1}\ b_1\ b^{-1} =$$

$$= \sigma_2(b)\ b^{-1}\ (\sigma_2(b_1)\ b_1^{-1})^{-1} =$$

$$= N_1(v_3)^{-1}\ (\sigma_2(b_1)\ b_1^{-1})^{-1}\ .$$

Mas aplicando a relação (4') para $\Pi = (12)$, vem:

$$\sigma_2(b_1)\ b_1^{-1} = N_1\ (v_3)^{-1}.$$

Logo,

$$\sigma_2(bb_1^{-1})\ (bb_1^{-1}) = N_1(v_3)^{-1}\ N_1(v_3) = 1, \text{ donde}$$

$$\sigma_2(bb_1^{-1}) = bb_1^{-1}$$

Analogamente, demonstra-se que $\sigma_3(bb_1^{-1}) = bb_1^{-1}$.

Logo, $bb_1^{-1} \in F$. $\square$

Seja $H \supset L$ uma extensão finita de corpos e seja T um subconjunto de H. Indicaremos por $N(T;\ H/L)$ o conjunto $\{N(x) \mid x \in T\}$, onde N denota a norma definida em H sobre L. Escreveremos ainda $N(H/L) = N(H;H/L)$.

Observemos que se $K = F(\xi_1,\xi_2,\xi_3)$, com $\xi_i \in K$, $i=1,2,3$ satisfazendo as condições (a), (b) e (c) da introdução deste parágrafo, então $N_i(\xi_i) = -\xi_i^2 = -\alpha_i$, $1 \leq i \leq 3$ e $N_i(\xi_j) = \xi_j^2 = \alpha_j$, se $j \neq i$, $1 \leq i,j \leq 3$. Seja $F_1 = F(\xi_2\xi_3)$. Nessas condições, valem os resultados que se seguem:

8.5 - LEMA

$$N_1(K) \cap F_1 = N(F_1(\xi_1)/F_1).N(F_1(\xi_1\xi_2)/F_1)$$

DEMONSTRAÇÃO

É claro que $N(F_1(\xi_1)|F_1).N(F_1(\xi_1\xi_2)|F_1) \subset N_1(K) \cap F_1$

Para mostramos a inclusão contrária, consideremos $a = N_1(u) \in F_1$, $u \in K$. Se $u \in F_1(\xi_1)$, então

$$a \in N(F_1(\xi_1)|F_1) \subset N(F_1(\xi_1)|F_1).N(F_1(\xi_1\xi_2)|F_1),$$

e o lema está demonstrado. Assim, podemos assumir que $a=N_1(u) \in F_1$ e $u \notin F_1(\xi_1)$.

Como $(1, \xi_2)$ é uma base de K sobre $F_1(\xi_1)$, segue-se que existem $\alpha, \beta \in F_1(\xi_1)$ tais que

$$u = \alpha + \beta\xi_2$$

Além disso, como $u \notin F_1(\xi_1)$, temos que $\beta \neq 0$. Logo,

$$u = \beta^{-1}(\beta\alpha + \xi_2) = u_1(u_2+\xi_2), \text{ onde } u_1, u_2 \in F_1(\xi_1).$$

Portanto

$$a = N_1(u) = N_1(u_1)\ N_1(u_2 + \xi_2) \in F_1.$$

Como $u_1 \in F_1(\xi_1)$, então $N_1(u_1) \in F_1$ e $N_1(u_1) \neq 0$. Consequentemente, $N_1(u_2+\xi_2) \in F_1$.

Mas

$$N_1(u_2+\xi_2) = (u_2+\xi_2)\ \sigma_1(u_2+\xi_2) =$$

$$= N_1(u_2) + \xi_2(u_2+ \sigma_1(u_2)) + \xi_2^2 \in F_1.$$

Assim, $\xi_2(u_2+\sigma_1(u_2)) \in F_1 = F(\xi_2\xi_3)$. Como $u_2 \in F_1(\xi_1)$ e $\xi_2(u_2+\sigma_1(u_2)) \in F(\xi_2\xi_3)$ é fácil ver que $u_2 + \sigma_1(u_2) = 0$. A partir daí, usando o fato de que $u_2 \in F_1(\xi_1)$, decorre que $u_2 = \gamma\ \xi_1$, onde $\gamma \in F(\xi_2 . \xi_3)$.

Logo,

$$a = N_1(u) = N_1(u_1)\ N_1(u_2 + \xi_2) =$$

$$= N_1(u_1)\ \ N_1(\gamma\ \xi_1 + \xi_2) =$$

$$= N_1(u_1)\ \ N_1(\xi_1)\ N_1(\xi_1^{-1})\ N_1(\gamma\ \xi_1 + \xi_2) =$$

$$= N_1(u_1\ \xi_1)\ N_1(\gamma + \ \xi_1^{-1}\ \xi_2) =$$

$$= N_1(u_1\xi_1)N_1(\gamma+\alpha_1^{-1}\xi_1\xi_2) \in N(F_1(\xi_1)|F_1).N(F_1(\xi_1\xi_2)|F_1).$$

Logo,

$N_1(K) \cap F_1 \subset N(F_1(\xi_1)|F_1).N(F_1(\xi_1\xi_2)|F_1)$, com o que concluímos a prova do lema. $\square$

<u>8.6 - COROLÁRIO</u> . Seja $b \in F.(N_1(K) \cap F(\xi_2\xi_3))$. Então

$$N(b;F_1|F) \in N(F(\xi_1)|F).(N(F(\xi_1\xi_2)|F) \cap N(F(\xi_2\xi_3)|F)$$

<u>DEMONSTRAÇÃO</u>

Como $b \in F.(N_1(K) \cap F(\xi_2\xi_3))$, do lema anterior se-

gue-se que $b = \alpha . a$, onde $\alpha \in F$ e $a \in N(F_1(\xi_1)|F_1).N(F_1(\xi_1\xi_2)|F_1)$. Logo, como $a \in F_1$, temos:

$$N(b;F_1|F) = \alpha^2 N(a;F_1|F).$$

Assim, é suficiente mostrar que

$$N(a;F_1|F) \in N(F(\xi_1)| F) . [N(F(\xi_1\xi_2)|F) \cap N(F(\xi_2\xi_3)|F)] ,$$

pois $\alpha^2 \in F$.

Como $a \in N(F_1(\xi_1) F_1) . N(F_1(\xi_1\xi_2)|F_1)$, segue-se que existem elementos $a_1 \in F_1(\xi_1)$ e $a_2 \in F_1(\xi_1\xi_2)$, tais que

$$a = N_1(a_1) . N_1(a_2)$$

Por outro lado, $N(a;F_1|F) = a\ \sigma_2(a) = N_2(a)$.

Logo,

$$N(a;F_1|F) = N_1(a_1)\ N_1(a_2)\ \sigma_2(N_1(a_1)\ N_1(a_2)) =$$

$$= N_1(a_1)\ \sigma_2(N_1(a_1))\ N_1(a_2)\ \sigma_2(N_1(a_2)) =$$

$$= N(N_1(a_1);\ F_1|F).\ N(N_1(a_2);\ F_1|F).$$

Assim,

$$N(a;F_1|F) \in N(N(F_1(\xi_1)|F_1);F_1|F) . N(N(F_1(\xi_1\xi_2)|F_1);F_1|F)$$

Mas

$$N[N(F_1(\xi_1)|F_1);F_1|F] = N(F_1(\xi_1)|F) =$$

$$= N\left[N(F_1(\xi_1)|F(\xi_1));\ F(\xi_1)|F\right] \subset$$

$$\subset N(F(\xi_1)|F)\ ,$$

$$N\left[N(F_1(\xi_1\xi_2)|F_1);\ F_1|F\right] = N(F_1(\xi_1\xi_2)|F) =$$

$$= N\left[N(F_1(\xi_1\xi_2)|F(\xi_1\xi_2));F(\xi_1\xi_2)|F\right] \subset$$

$$\subset N(F(\xi_1\xi_2)|F)$$

e

$$N(F_1(\xi_1\xi_2)|F) = N(N(F_1(\xi_1\xi_2)|F_1);\ F_1|F) \subset N(F_1|\ F)$$

Logo,

$$N(a;F_1|F) \in N(F(\xi_1)|F)\ .\left[N(F(\xi_1\xi_2)|F) \cap N(F(\xi_2\xi_3)|F)\right]$$

com o que concluímos a prova do corolário. $\square$

<u>8.7 - LEMA</u> . Seja $b \in F(\xi_2,\xi_3)$. Então $b \in F(\xi_2).N_1(K)$ se e só se $N_3(b) \in N(F(\xi_1,\xi_2)|F(\xi_2))$.

<u>DEMONSTRAÇÃO</u>

Seja $b \in F(\xi_2)\ N_1(K)$. Então existem $a_2 \in F(\xi_2)$ e $k \in K$ tais que

$$b = a_2 \cdot N_1(k)$$

Logo,

$$N_3(b) = N_3(a_2)\ N_3(N_1(k)) = a_2^2\ N_1(N_3(k)) =$$

$$= N_1(a_2)\ N_1(N_3(k) = N_1(a_2\ N_3(k)) \ ,$$

pois $a_2 \in F(\xi_2)$.

Assim, resta mostrar que $a_2\ N_3(k) \in F(\xi_1,\xi_2)$. Para isso, é suficiente provar que $a_2 \cdot N_3(k)$ é fixo por σ_3. Então

$$\sigma_3(a_2\ N_3\ (k)) = \sigma_3(a_2)\ \sigma_3(N_3(k)) = a_2\ N_3(k) \ ,$$

já que $a_2 \in F(\xi_2)$. Logo, $N_3(b) \in N(F(\xi_1,\xi_2)|F(\xi_2))$.

Reciprocamente, suponhamos que $N_3(b) = N_1(k_o)$, para algum $k_o \in F(\xi_1,\xi_2)$. Consideremos $k = b+k_o$ e $k'_o = k'_o+\sigma_1(k_o)$. Então $k'_o \in F(\xi_2)$ pois é fixo por σ_1 e σ_3. Por outro lado, temos que:

$$N_1(k) = N_1(b+k_o) = (b+k_o)\ \sigma_1(b+k_o) =$$

$$= (b+k_o)\ (b+\sigma_1(k_o), \quad \text{pois } b \in F(\xi_2,\xi_3).$$

Assim,

$$N_1(k) = b^2 + b\ \sigma_1(k_o) + bk_o + k_o\ \sigma_1(k_o) =$$

$$= b^2 + b\,k_o' + N_1(k_o) = b^2 + b\,k_o' + N_3(b) =$$

$$= b^2 + b\,k_o' + b\,\sigma_3(b) = b(b + k_o' + \sigma_3(b)).$$

Mas $[b + \sigma_3(b)] + k_o' \in F(\xi_2)$ pois $k_o' \in F(\xi_2)$ e $b + \sigma_3(b) \in F(\xi_2)$ e $b + \sigma_3(b) \in F(\xi_2)$. Logo, $N_1(k) = b\alpha$, onde $\alpha \in F(\xi_2)$.

Agora, se $\alpha = 0$ então $k = 0$ e portanto $b = -k_o \in F(\xi_1,\xi_2)$. Como $b \in F(\xi_2,\xi_3)$ segue-se que $b \in F(\xi_1,\xi_2) \cap F(\xi_2,\xi_3) = F(\xi_2)$. Logo, $b \in F(\xi_2).N_1(K)$.

Se $\alpha \neq 0$, então $b = \alpha^{-1}N_1(k)$ com $\alpha \in F(\xi_2)$ e $k \in K$; logo $b \in F(\xi_2)N_1(K)$. $\square$

<u>8.8 - COROLÁRIO</u> - Seja $b \in F(\xi_2.\xi_3)$. Então

$$b \in F(\xi_2)\ N_1(K) \cap F(\xi_3)\ N_1(K) \quad \text{se e somente se}$$

$$N_2(b) = N_3(b) \in N[F(\xi_1,\xi_2)|F(\xi_2)] \cap N[F(\xi_1,\xi_2)|F(\xi_3)]$$

<u>DEMONSTRAÇÃO</u>

Como $F(\xi_2.\xi_3) \subset F(\xi_2,\xi_3)$, temos que $b \in F(\xi_2,\xi_3)$.

Se $b \in F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$ então pelo lema anterior segue-se que

$$N_3(b) \in N(F(\xi_1,\xi_2)|F(\xi_2)) \quad \text{e}$$

$N_2(b) \in N(F(\xi_1,\xi_3)/F(\xi_3))$

Assim, resta provar apenas que $N_2(b) = N_3(b)$. Mas $b \in F(\xi_2.\xi_3)$ e $(1, \xi_2.\xi_3)$ é uma base de $F(\xi_2\xi_3)$ sobre F. Logo, existem $\alpha,\beta \in F$ tais que

$$b = \alpha + \beta\ \xi_2\ \xi_3$$

Portanto $\sigma_2(b) = \sigma_3(b)$, donde $N_2(b) = N_3(b)$.

Reciprocamente se $b \in F(\xi_2,\xi_3)$ e $N_2(b) \in N(F(\xi_1,\xi_3)|F(\xi_3))$ então, pelo lema anterior, temos que $b \in F(\xi_3)N_1(K)$.

Analogamente, $b \in F(\xi_2)N_1(K)$, donde, $b \in F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$ e o corolário está demonstrado.

$\square$

§ 9 - PRODUTOS CRUZADOS ABELIANOS GENÉRICOS

Neste parágrafo estabeleceremos condições necessárias e suficientes para que um certo tipo de álgebras com divisão seja isomorfa a um produto tensorial de álgebras de quatérnios. Estas álgebras serão os produtos cruzados abelianos genéricos, que passaremos a construir.

Seja $K|_F$ uma extensão galoisiana, com grupo de Galois abeliano $G = \langle \sigma_1 \rangle \times \ldots \times \langle \sigma_r \rangle$. Denotemos por $q_i = o(\sigma_i)$, $1 \leq i \leq r$. Seja ainda $U = \{u_{ij} \mid 1 \leq i,j \leq r\} \subset K$ satisfazen-

do as condições (1), (2) e (3) da proposição (7.2).

Consideremos $A_r = K\{x_1,\ldots,x_r\}$ o anel de polinômios nas variáveis não comutativas $\{x_1,\ldots,x_r\}$, com as seguintes operações:

$$x_i x_j = u_{ij}\, x_j\, x_i$$

$$x_i\, k = \sigma_i(k) x_i \qquad 1 \leq i,j \leq r, \quad k \in K.$$

Já vimos que podemos definir o grau de um monômio $k\, x_1^{m_1}\ldots x_1^{m_r}$ por

$$(k\, x^{m_1}\ldots x^{m_r}) = \bar{m} = (m_1,\ldots,m_r)$$

e que o grau de $(k\, x_1^{m_1}\ldots x_r^{m_r})\ (k^1\, x_1^{n_1}\ldots x_r^{n_r})$ é $\bar{m} + \bar{n} = (m_1+n_1,\ldots,m_r+n_r)$.

Consideremos $\bar{m} = (m_1,\ldots,m_r)$ e $\bar{n} = (n_1,\ldots,n_r)$ duas r-uplas de números naturais. Dizemos que $\bar{m} < \bar{n}$ se existe i, $1 \leq i \leq r$, tal que $m_j = n_j$ para $j < i$ e $m_i < n_i$.

Deste modo podemos definir o grau de um polinômio $o \neq f \in K\{x_1,\ldots,x_r\}$ como o <u>máximo</u> dos graus dos monômios de f; indiquemos por $\nu(f)$ o monômio de f de maior grau e por $\partial(f)$ o grau do polinômio f. Com estas notações e definições, vale o seguinte resultado, de demonstração simples.

<u>9.1 - LEMA</u> - Sejam $0 \neq f,\ g \in K\{x_1,\ldots,x_r\}$ e $k \in K$. Então

(i) $\partial(f.g) = \partial f + \partial g$

$\nu(f.g) = \nu(f) \,.\, \nu(g)$

(ii) $\nu(k.f) = k \,.\, \nu(f)$

(iii) Se $\partial(f) = \partial(g)$ então $\nu(f) + \nu(g) = 0$

ou $\nu(f+g) = \nu(f) + \nu(g)$.

É fácil ver que $K\{x_1,\ldots,x_r\}$ é um domínio. Na verdade, $K\{x_1,\ldots,x_r\}$ é um domínio de Ore [2, lema 2.2] e portanto pode ser imerso em um anel com divisão. Seja $K(x_1,\ldots,x_r)$ um anel de quocientes à esquerda de $K\{x_1,\ldots,x_r\}$.

<u>9.2 - DEFINIÇÃO</u> - O anel $K(x_1,\ldots,x_r)$ acima construído diz-se um <u>produto cruzado abeliano genérico de K e G</u>.

Como $K(x_1,\ldots,x_r)$ está determinado por K, G e U, denotaremos

$$K(x_1,\ldots,x_r) = (K, G, U).$$

O produto cruzado (K, G, U) é chamado "genérico" pois todo produto cruzado abeliano (K, G, U, B) é imagem homomorfa de (K, G, U).

Nosso objetivo agora será demonstrar que (K, G, U) é, de fato, um produto cruzado abeliano.

Como U satisfaz as condições (1), (2) e (3) da proposição (7.2), sabemos, pela observação (7.11,d), que existe $B = \{b_1,\ldots,b_r\} \subset K$, determinado a menos de multiplicação por

elementos de F, satisfazendo a condição (4) da proposição (7.2). Nesta situação, temos o seguinte resultado:

<u>9.3 - TEOREMA</u> - $A = (K, G, U) = (K', G, U, B)$ onde $K' = K(y_1, \ldots, y_r)$ e $y_i = b_i^{-1} x_i^{q_i}$, $1 \leq i \leq r$.

<u>DEMONSTRAÇÃO</u>

Observemos inicialmente que y_i, $1 \leq i \leq r$, comuta com os elementos de K. De fato, dado um elemento $k \in K$ qualquer, temos:

$$y_i k = (b_i^{-1} x_i^{q_i}) k = b_i^{-1} \sigma_i^{q_i}(k) x_i^{q_i} =$$

$$= b_i^{-1} k x_i^{q_i} = k(b_i^{-1} x_i^{q_i}) = k y_i, \quad 1 \leq i \leq r.$$

Além disso, temos ainda que

$$y_i y_j = (b_i^{-1} x_i^{q_i})(b_j^{-1} x_j^{q_j}) = b_i^{-1} \sigma_i^{q_i}(b_j^{-1}) x_i^{q_i} x_j^{q_j} =$$

$$= b_j^{-1} b_i^{-1} x_i^{q_i} x_j^{q_j} = b_j^{-1} b_i^{-1} N_i(N_j(u_{ij})) x_j^{q_j} x_i^{q_i} =$$

$$= b_j^{-1} b_i^{-1} x_j^{q_j} x_i^{q_i} = b_j^{-1} x_j^{q_j} b_i^{-1} x_i^{q_i} =$$

$$= y_j y_i \quad , \quad 1 \leq i,j \leq r.$$

Assim, os elementos y_i, $1 \leq i \leq r$, comutam entre si e comutam com os elementos de K. Desta forma, podemos cons-

truir $K'=K(y_1,\ldots,y_r)$, o menor subcorpo de A que contém K e $y_1,\ldots,y_r$.

Observemos ainda que, como $b_i \in K$, $1 \leq i \leq r$, então $K' = K(y_1,\ldots,y_r)=K(x_1^{q_1},\ldots,x_r^{q_r})$.

Vamos mostrar agora que K' é um subcorpo maximal de A. Dividiremos esta prova em vários passos:

<u>1º Passo</u> - O conjunto $\{x^{\bar{m}}=x_1^{m_1}\ldots x_r^{m_r} \mid 0 \leq m_i < q_i,\ 1 \leq i \leq r\}$ é uma base de A sobre K'.

É fácil verificar que o conjunto acima é linearmente independente sobre K'. Assim, resta provar que tal conjunto gera A sobre K'.

Para isso, mostraremos que $x_i\ K'\ x^{-1} = K'$, $1 \leq i \leq r$. Esta afirmação decorre imediatamente dos seguintes fatos:

$$x_i\ k\ x^{-1} = \sigma_i(k) \in K \subset K' \ ,\ \forall\ k \in K,\ 1 \leq i \leq r$$

e como B verifica (4) temos também que:

$$x_i y_j x_i^{-1} = x_i(b_j^{-1}\ x_j^{q_j})\ x_i^{-1} = \sigma_i(b_j^{-1})\, x_i x_j^{q_i}\ x_i^{-1} =$$

$$= \sigma_i(b_j^{-1})\ (x_i\ x_j\ x_i^{-1})^{q_j} =$$

$$= \sigma_i\ (b_j^{-1})\ (u_{ij}\ x_j)^{q_j} =$$

$$= \sigma_i\ (b_j^{-1})\ N_j\ (u_{ij})\ x_j^{q_j} =$$

$$= b_j^{-1}\ x_j^{q_j} = y_j \in K',\quad 1 \leq i,j \leq r.$$

Logo, $x_i K' x_i^{-1} = K'$, $1 \leq i \leq r$.

Com isso, é fácil verificar que o conjunto

$$\{x^{\bar{m}} = x_1^{m_1} \ldots x_r^{m_r} \mid 0 \leq m_i < q_i \ , \ 1 \leq i \leq r\}$$

gera A sobre K' se e somente se o subanel gerado por K' e por $\{x_1,\ldots,x_r\}$ for igual a A. Indiquemos por $K'[x_j^1,\ldots,x_r]$ tal subanel. Então $K'[x_1,\ldots,x_r]$ é um subdomínio de A, algébrico sobre K'; logo, $K'[x_1,\ldots,x_r]$ é um anel com divisão. Mas $K[x_1,\ldots,x_r] \subset K'|x_1,\ldots,x_r|$, donde

$$A = K(x_1,\ldots,x_r) \subset K' \ [x_1,\ldots,x_r] \ .$$

Como $K'[x_1,\ldots,x_r] \subset A$, segue-se a afirmação.

Consequentemente

$$[A:K'] = q_1 \ldots q_r = n = |G| \ .$$

<u>2º Passo</u> - Seja $Z = Z(A)$ o centro de A. Então $Z \subset K'$ e $[K':Z] = n$ (donde, K' é um subcorpo maximal de A).

Como vimos no primeiro passo, os elementos x_i, $1 \leq i \leq r$ induzem automorfismos σ_i' em K', da seguinte maneira:

$$\sigma_i'(k) = \sigma_i(k), \qquad k \in K$$

e

$$\sigma_i(y_j) = y_j \qquad 1 \leq i,j \leq r.$$

Consideremos $G' = \langle \sigma_i' \mid 1 \leq i \leq r \rangle$. É fácil verificar que $G' \cong G$. Vamos determinar o corpo fixo de G'. É claro que $K' \cap Z(A)$ está contido no corpo fixo de G'. Por outro la-

do, dado um elemento $k' \in K$, se $\sigma_i'(k') = k'$, $1 \leq i \leq r$ então k' comuta com x_i, $1 \leq i \leq r$. Como $A = K'[x_1,\ldots,x_r]$, segue-se que $k' \in Z(A)$. Assim, o corpo fixo de G' está contido em $K' \cap Z(A)$. Mostramos, portanto, que o corpo fixo de G' é $K' \cap Z(A)$.

Conseqüentemente, computando dimensões, temos

$$|G'| = n = [K':K' \cap Z(A)] = [K'.Z(A) : Z(A)]$$

Mas, $K'.Z(A)$ é um subcorpo de A. Logo,

$$n = [A:K'] \geq [A;K'Z(A)] \geq [K'.Z(A):Z(A)] = n$$

Assim, $[A;K'.Z(A)] = [A:K'] = n$, donde $Z(A) \subset K'$ e portanto $[A:Z(A)] = n^2$. Consequentemente, K' é subcorpo maximal de A.

Vamos mostrar agora que $F'=F(y_1,\ldots,y_r) = Z(A)$.

Como y_i comuta com x_j, $1 \leq i,j \leq r$ e y_i comuta com todo elemento de K', temos que $F' \subset Z(A)$, pois $A=K'[x_1,\ldots,x_r]$.

Por outro lado, y_i é transcendente sobre F, $1 \leq i \leq r$. Logo,

$$[K(y_1,\ldots,y_r):F(y_1,\ldots,y_r)] = [K:F] = n$$

Portanto, $[K':F'] = [K':Z(A)] = n$, donde $Z(A) = F' = F(y_1,\ldots,y_r)$.

Finalmente, se considerarmos $z_i = x_i$, $1 \leq i \leq r$, é fácil verificar que

$$z_i k' = \sigma_i'(k')\, z_i \qquad 1 \leq i \leq r, \quad k' \in K'$$

$$z_i z_j = u_{ij} z_j z_i \qquad 1 \leq i,j \leq r$$

$$z_i^{q_i} = x_i^{q_i} = b_i y_i = b_i' \qquad 1 \leq i \leq r .$$

Observemos que como $y_i \in F'$, $1 \leq i \leq r$, o conjunto $B' = \{b' \mid 1 \leq i \leq r\}$ satisfaz (4). Logo, $A = (K, G, U) = (K'|_{F'}, G', U, B')$. □

A seguir, enunciamos dois corolários que nos darão uma descrição um pouco melhor dos produtos cruzados abelianos genéricos. O primeiro caracteriza os elementos do anel de polinômios $K\{x_1,\ldots,x_r\}$ que são centrais em $K(x_1,\ldots,x_r)$. O segundo nos diz que todo elemento de $K(x_1,\ldots,x_r)$ é na verdade, produto de um elemento de $K[x_1,\ldots,x_r]$ por um elemento do centro de $K(x_1,\ldots,x_r)$.

Estes dois resultados serão utilizados em seguida, quando estabeleceremos uma condição necessária e suficiente para que um produto cruzado abeliano genérico de grau 8 seja um produto tensorial de subálgebras de quatérnios.

As notações utilizadas são as do teorema (9.3).

<u>9.4 - COROLÁRIO</u> - Seja $f \in K\{x_1,\ldots,x_r\}$. Então $f \in F'$ se e somente se cada monômio de f pertence a F'.

DEMONSTRAÇÃO

É suficiente mostrar que se $f \in K\{x_1,\ldots,x_r\} \cap F'$ então $\nu(f) \in F'$ e para isso, mostraremos, em primeiro lugar, que $\nu(f) \in K'$.

Como $f \in K'$, existem polinômios em $x_i^{q_i}$, $1 \leq i \leq r$, $g \in h$, tais que

$$f = g \cdot h^{-1}$$

Consequentemente, $f \cdot h = g$.

Mas os graus de $g \in h$ na variável x_i são múltiplos de q_i. Logo, o grau de f na variável x_i é múltiplo de q_i, $1 \leq i \leq r$, donde $\nu(f) \in K'$.

Para mostrarmos agora que $\nu(f) \in F'$, basta verificar que $\nu(f)$ comuta com x_i, $1 \leq i \leq r$. Para isso, observemos que se $ax_1^{m_1} \ldots x_r^{m_r}$ é um monômio, com $a \in K$, temos

$$x_i(a\, x_1^{m_1} \ldots x_r^{m_r})\, x_i^{-1} = b\, x_1^{m_1} \ldots x_r^{m_r}$$

para algum elemento $b \in K$.

Assim, o monômio de maior grau de $x_i\, f\, x_i^{-1}$ é $x_i\, \nu(f)\, x_i^{-1}$. Mas f é central; logo $x_i\, f\, x_i^{-1} = f$ e portanto $x_i\, \nu(f)\, x_i^{-1} = \nu(f)$. Consequentemente, $\nu(f) \in F'$ e o corolário está demonstrado. $\square$

9.5 - COROLÁRIO - $(K, G, U) = F' . K\{x_1,\ldots,x_r\}$

DEMONSTRAÇÃO

$F' . K\{x_1,\ldots,x_r\}$ é um domínio de dimensão finita sobre F'. Logo, $F' . K\{x_1,\ldots,x_r\}$ é um anel com divisão. Como

$$K\{x_1,\ldots,x_r\} \subset F' . K\{x_1,\ldots,x_r\}$$

segue-se que o anel de quocientes de $K\{x_1,\ldots,x_r\}$ está contido em $F' . K\{x_1,\ldots,x_r\}$. Assim,

$$(K, G, U) \subset F' . K\{x_1,\ldots,x_r\}.$$

Como $F' . K\{x_1,\ldots,x_r\} \subset (K, G, U)$, segue-se a igualdade. $\square$

9.6 - OBSERVAÇÃO - Do corolário anterior, decorre que todo elemento de (K, G, U) pode ser escrito na forma $f.g^{-1}$, com $f \in K\{x_1,\ldots,x_r\}$ e $0 \neq g \in F' \cap K\{x_1,\ldots,x_r\}$. De fato, pelo corolário anterior, é suficiente mostrar que se $f_1, f_2 \in K\{x_1,\ldots,x_r\}$ e $g_1, g_2 \in F' \cap K\{x_1,\ldots,x_r\}$, $g_1 \neq 0$ e $g_2 \neq 0$, então $f_1 g_1^{-1} + f_2 g_2^{-1}$ se escreve na forma $f.g^{-1}$, com $f \in K\{x_1,\ldots,x_r\}$ e $0 \neq g \in F' \cap K\{x_1,\ldots,x_r\}$. Mas

$$(f_1 g_1^{-1} + f_2 g_2^{-1}) = (f_1 g_2 + f_2 g_1)(g_1 g_2)^{-1} ,$$

pois g_1 e g_2 são centrais e F' é um corpo. Como

$$(f_1g_2 + f_2g_1) \in K\{x_1,\ldots,x_r\} \quad \text{e}$$

$$o \neq g_1g_2 \in F' \cap K\{x_1,\ldots,x_r\}\ , \quad \text{segue-se que}$$

$$f_1g_1^{-1} + f_2g_2^{-1} = f\ g^{-1}, \quad \text{com}$$

$$f \in K\{x_1,\ldots,x_r\} \quad \text{e} \quad 0 \neq g \in F' \cap K\{x_1,\ldots,x_r\}.$$

De agora em diante, salvo menção explicita em contrário, $K|_F$ denotará uma extensão galoisiana, com grupo de Galois <u>abeliano</u> $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times,\ldots\langle\sigma_r\rangle$, onde $o(\sigma_i) = 2$, $1 \leq i \leq r$. Consideremos $U = \{u_{ij} \mid 1 \leq i,j \leq r\}$ um subconjunto de K, satisfazendo as condições (1), (2) e (3) da proposição (7.2) e seja (K, G, U) o produto cruzado abeliano genérico relativo a U. Já vimos que (K, G, U) é, de fato, um produto cruzado abeliano. Logo, (K, G, U) será uma álgebra com involução se assumirmos que, em relação a um dado automorfismo $\tau \in G$, U satisfaça a condição (5) e B satisfaça a condição (6), do teorema (7.12).

A hipótese de que B satisfaça a condição (6) para um dado $\tau \in G$ é dispensável nas seguintes situações

(i) $\tau = 1$

ou

(iii) Se $r=3$ e $\tau = \sigma_1\sigma_2\sigma_3$ (neste caso, pela proposição (8.2), vimos que é suficiente que U satisfaça as condições (1) e (2) da proposição (7.2) e a condição (5) do teorema (7.12), para $\tau = \sigma_1\sigma_2\sigma_3$).

Denotaremos por (K, G, U, τ) o produto cruzado abeliano genérico (K, G, U) com involução $*$, cuja restrição a K' é τ. Observemos ainda que dado $f \in K\{x_1,\ldots,x_r\}$, f se escreve de modo único na forma

$$f = \sum_{\mu} k_\mu x^{\mu_1}\ldots x^{\mu_r}, \text{ onde } k_\mu \in K,\ \mu_i \in \mathbb{N},$$
$$1 \leq i \leq r.$$

Consequentemente, $f^* = \sum_{\mu} x_r^{\mu_r}\ldots x_1^{\mu_1}\,\tau(k_\mu)$

Nosso objetivo agora será estabelecer condições necessárias e suficientes para que um produto cruzado abeliano genérico, com involução, de grau 8 seja um produto tensorial de álgebras de quatérnios. Começaremos com um lema que relaciona este fato com os conjuntos g-geradores, definidos no parágrafo § 6.

<u>9.6 - LEMA</u> - Se $A = (K,G,U,\tau)$ é um produto tensorial de subálgebras de quatérnios, então A possui um conjunto q-gerador S, contendo 4^r elementos com as seguintes propriedades:

(i) Todo elemento de S tem a forma $k\, x_1^{\mu_1} \ldots x_r^{\mu_r}$, onde $k \in K$ e $\mu_i \in \{0,1\}$, $1 \leq i \leq r$.

(ii) Para cada $\mu = (\mu_1,\ldots,\mu_r) \in \{0,1\}^r$, existem 2^r elementos de S da forma $k\, x_1^{\mu_1},\ldots,x_r^{\mu_r}$. Em particular, $S \cap K$ em 2^r elementos.

DEMONSTRAÇÃO

Como $[A:F'] = 4^r$, segue-se, pela proposição (6.3), que A possui um conjunto q-gerador $S_1=\{a_1,\ldots,a_t\}$, com $t = 4^r$ elementos. Além disso, pela observação (9.6) cada $a_i \in S_1$, se escreve na forma

$$a_i = f_i\, g_i^{-1}$$

onde $f_i \in K\{x_1,\ldots,x_r\}$ e $g_i \in K\{x_1,\ldots,x_r\} \cap F'$, $1 \leq i \leq t$.

Por outro lado, sendo S_1 um conjunto q-gerador, é fácil ver que $\{f_1,\ldots,f_t\}$ é também q-gerador, pois $g_i \in F'$, $1 \leq i \leq r$. Agora, como $\{f_1,\ldots,f_t\}$ é q-gerador, deduz-se que $\{\nu(f_1),\ldots,\nu(f_t)\}$ é também q-gerador. Mas, para cada i, $1 \leq i \leq t$, tem-se que

$$\nu(f_i) = a_i\, x_1^{i_1} \ldots x_r^{i_r}, \text{ com } a_i \in K.$$

Sejam $j_1 = [i_j/2],\ldots,j_r = [i_r/2]$ e consideremos

$c_i = y_1^{j_1},\ldots,y_r^{j_r}$.

Como $F' = F(y_1,\ldots,y_r)$ é o centro de A, segue-se que cada c_i é central, $1 \leq i \leq t$. Além disso $\nu(f_i)\ c_i^{-1}$ é da forma

$$k_i\ x_1^{\mu_1},\ldots,x_r^{\mu_r}\ ,\ \text{onde}\ k_i \in K$$

e $\mu_1,\ldots,\mu_r \in \{0,1\}$, $1 \leq i \leq t$.

Finalmente como cada c_i é central, $1 \leq i \leq t$, segue-se que

$S = \{\nu(f_1)c_1^{-1},\ldots,\nu(f_t)c_t^{-1}\}$ é um conjunto q-gerador, satisfazendo (i).

Fixemos $\mu = (\mu_1,\ldots,\mu_r) \in \{0,1\}^r$. Então existem no máximo 2^r elementos da forma $k\ x_1^{\mu_1},\ldots,x_r^{\mu_r}$, com $k \in K$, que são linearmente independentes sobre F'. Por outro lado, o número de monômios distintos $x_1^{\mu_1},\ldots,x_r^{\mu_r}$ é 2^r. Como o número de elementos de S é 4^r e S é linearmente independente sobre F', segue-se que para cada $\mu = (\mu_1,\ldots,\mu_r) \in \{0,1\}^r$, existem exatamente 2^r elementos de S da forma $k_i\ x_1^{\mu_1},\ldots,x_r^{\mu_r}$; logo, S satisfaz também a condição (ii). $\square$

Finalmente, estamos em condições de apresentar o critério procurado.

Para isso, sejam $\tau = \sigma_1\sigma_2\sigma_3$ e $U = \{u_{ij} \mid 1 \leq i \leq 3\} \subset K$ satisfazendo as condições (1), (2) e (3) da proposição (7.2).

Já vimos que podemos construir $B = \{b_1, b_2, b_3\} \subset K$ satisfazendo a condição (4). Indiquemos por $A = (K,G,U,\tau)$, o produto cruzado abeliano genérico, com involução, cuja restrição a K' coincide com τ. Nessas condições, temos

9.7 - TEOREMA - $A = (K,G,U,\tau)$ é um produto tensorial de álgebras de quatérnios se e somente se $b_1 \in F \cdot N_1(K)$.

DEMONSTRAÇÃO

Suponhamos que A seja um produto tensorial de álgebras de quatérnios. Então, pela proposição anterior, existe um elemento não nulo $k \in K$ tal que $(k\, x_1)^2 \in F'$. Mas

$$(k\, x_1)^2 = k\, \sigma_1(k) x_1^2 = k\, \sigma_1(k)\, b_1 y_1 ,$$

onde $y_1 = b_1^{-1} x_1^2 \in F'$.

Logo, $k\, \sigma_1(k) b_1 \in F' \cap K = F$,

isto é, $b_1 \in F N_1(K)$.

Reciprocamente, suponhamos que $b_1 \in F N_1(K)$. Então existe um elemento $k \in K$ tal que $(b_1\, k\, \sigma_1(k) \in F$.

Por outro lado, sabemos que podemos encontrar um elemento $\xi_1 \in K$ tal que $0 \neq \xi_1^2 \in F$ e $\sigma_1(\xi_1) = -\xi_1$.

Deste modo, é fácil ver que o conjunto $\{\xi_1, kx_1\}$ é

q-gerador. Seja Q_1 a F'-subálgebra de quatérnios de base $\{1, \xi_1, kx_1, \xi_1 kx_1\}$. Então por [5, teorema 4.4.2], segue-se que $A = Q_1 \otimes_{F'} C_A(Q_1)$, onde $C_A(Q_1)$ denota o centralizador de Q_1 em A. Além disso, A é álgebra com divisão sobre seu centro F', com involução. Logo, pelo teorema (4.5), A tem expoente 2 no grupo de Brauer de F'. Conseqüentemente, $C_A(Q_1)$ também tem expoente 2 em B(F'); donde $C_A(Q_1)$ é uma álgebra com involução. Mas, computando dimensões, vemos que $[C_A(Q_1):F'] = 16$; logo, pelo corolário (5.4), segue-se que $C_A(Q_1)$ é produto tensorial de F'-subálgebras de quatérnios e portanto A é produto tensorial de F'-álgebras de quatérnios. □

Consideremos novamente $K|_F$ uma extensão galoisiana, com grupo de Galois abeliano $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle$, onde $o(\sigma_i) = 2$, $1 \leq i \leq 3$. Sabemos então que existem elementos $\xi_1, \xi_2, \xi_3 \in K$ tais que $K=F(\xi_1,\xi_2,\xi_3)$, $\xi_i^2 = \alpha_i \in F - \{0\}$, $\sigma_i(\xi_i) = -\xi_i$ e $\sigma_i(\xi_j) = \xi_j$, se $j \neq i$, $1 \leq i,j \leq 3$. Consideremos ainda $\tau = \sigma_1 \sigma_2 \sigma_3 \in G$. Nestas condições, temos:

<u>9.8 - TEOREMA</u> - Se existe um elemento $b \in F(\xi_2\xi_3) \cap F(\xi_2) N_1(K) \cap F(\xi_3) N_1(K)$, $b \notin F \cdot N_1(K)$, então existe $U = \{u_{ij} | 1 \leq i,j \leq 3\} \subset K$ tal que $A = (K,U,\tau)$ é uma álgebra com divisão de grau 8 sobre seu centro, com involução, que <u>não</u> é um produto tensorial de subálgebras de quatérnios.

DEMONSTRAÇÃO

Pelo corolário (8.4, b), sabemos que existem $V = \{v_1, v_2, v_3\} \subset K$ satisfazendo as condições (2') e (3') da proposição (8.1) e $B = \{b_1, b_2, b_3\} \subset K$ satisfazendo as condições (4') e (5') da proposição (8.2), de modo que $b_1 = b$. Agora, pela proposição (8.1, b), concluímos que existe $U = \{u_{ij} \mid 1 \leq i,j \leq 3\} \subset K$ satisfazendo as condições (1) e (2) da proposição (7.2) e a condição (5) da proposição (7.12), para $\tau = \sigma_1\sigma_2\sigma_3$. Na verdade os conjuntos U e B satisfazem as condições (1), (2), (3), (4), (5) e (6), para $\tau = \sigma_1\sigma_2\sigma_3$.

Logo, podemos construir o produto cruzado abeliano genérico $A = (K,G,U,\tau)$, com involução. Pelo teorema anterior, A não é um produto tensorial de álgebra de quatérnios $\square$

§ 10 - O CONTRA-EXEMPLO

Nesta parágrafo exibiremos um contra-exemplo a conjectura de Albert, já mencionada. Construiremos uma álgebra com divisão de grau 8 sobre seu centro, com involução, que não é isomorfa a um produto tensorial de álgebras de quatérnios.

Tendo-se em mente os resultados do parágrafo anterior, é razoável esperar que esta álgebra seja um produto cru

zado abeliano genérico. Por essa razão, começaremos construindo uma extensão galoisiana que dará origem, posteriormente, ao produto cruzado que nos fornecerá o contra-exemplo procurado.

<u>10.1 - LEMA</u> - Seja $F = Q(\lambda)$, o corpo das funções racionais em uma indeterminada λ e seja $\bar{F}$ o fecho algébrico de F. Consideremos ainda $\xi_1, \xi_2, \xi_3 \in \bar{F}$ tais que

$$\xi_1^2 = -1, \quad \xi_2^2 = -(\lambda^2 + 1), \quad \xi_3^2 = \lambda.$$

Nessas condições, temos:

(i) $K = F(\xi_1, \xi_2, \xi_3)$ é uma extensão galoisiana de F, com grupo de Galois abeliano $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle$, onde $o(\sigma_i) = 2$, $i = 1,2,3$.

(ii) Se $b = \xi_2\xi_3 \in K$ então,

$$b \in F(\xi_2\xi_3) \cap F(\xi_2)\, N_1(K) \cap F(\xi_3)\, N_1(K)$$

e

$$b \notin F \,.\, N_1(K).$$

<u>DEMONSTRAÇÃO</u>

É fácil ver que $[K:F] = 8$.

Sejam $\sigma_i\ K \to K$ os F-automorfismos definidos por

$$\sigma_i(\xi_i) = -\xi_i \quad e \quad \sigma_i(\xi_j) = \xi_j, \text{ se } j \neq i,\ 1 \leq i,j \leq 3.$$

Então é claro que $o(\sigma_i) = 2$, $i = 1,2,3$. Além disso, é fácil verificar que $\sigma_i\sigma_j = \sigma_j\sigma_i$, $1 \leq i,j \leq 3$. Assim, se

$G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \langle\sigma_3\rangle$, então $|G| = 8$, G é abeliano e ainda o corpo fixo de G é F. Com isto, demonstramos a parte (i) do lema.

Para provarmos (ii), observemos que pelo corolário (8.8), basta mostrar que

$$N_2(b) = N_3(b) \in N\left[F(\xi_1,\xi_2)\,|\,F(\xi_2)\right] \cap \left[N\,|\,F(\xi_1,\xi_3)\,|\,F(\xi_3)\right].$$

Consideremos os elementos

$$x = \frac{1}{2}\ \xi_2((\lambda - 1 - \xi_2) + (\lambda - 1 + \xi_2)\ _1) \in F(\xi_1,\xi_2)$$

e

$$y = \xi_1\xi_3\ (\lambda\ \xi_1 - 1) \in F(\xi_1,\xi_3)\ .$$

Temos então:

$$N(x\,;\,F(\xi_1,\xi_2)\,|\,F(\xi_2)) = N_1(x)$$

e

$$N(y\,;\,F(\xi_1,\xi_3)\,|\,F(\xi_3)) = N_1(y)$$

Além disso, é fácil ver que $N_2(b) = N_3(b) = N_1(x) = N_1(y)$.

Logo,

$b \in F(\xi_2\xi_3) \cap F(\xi_2)\ N_1(K) \cap F(\xi_3).N_1(K)$

Assim, resta mostrar que $b \notin F\ N_1(K)$, o que requer um pouco mais de trabalho. Para isso, pelo corolário (8.6) é suficiente mostrar que

$$N(b;\ F(\xi_2\xi_3)\,|\,F) = N_2(b) \notin N(F(\xi_1)\ F)\ [N(F(\xi_1\xi_2)\,|\,F) \cap N(F(\xi_2\xi_3)/F)]$$

Suponhamos então, por absurdo que existam $f_1 \in F(\xi_1)$, $f_2 \in F(\xi_1\xi_2)$ e $f_3 \in F(\xi_2\xi_3)$ tais que

$$N_2(b) = \lambda(\lambda^2 + 1) = N_1(f_1)\ N_1(f_2) = N_1(f_1)\ N_2(f_3)$$

Deste modo, é fácil verificar que existem polinômios não nulos g, g_1, g_2, g_3, g_4, g_5 e $g_6 \in \mathbb{Z}\ [\lambda]$ tais que

$$f_1^{-1} = (g_1+g_2\ \xi_1)g^{-1}\ ,\ f_2 = (g_3+g_4\ \xi_1\xi_2)g^{-1},\ f_3=(g_5+g_6\ \xi_2\xi_3)g^{-1}$$

Assim,

$$g = f_1(g_1+g_2\ \xi_1)=f_2^{-1}(g_3+g_4\ \xi_1\xi_2)=f^{-1}(g_5+g_6\ \xi_2\xi_3)$$

Como $g \in \mathbb{Z}\ [\lambda] \subset F$, segue-se que

$N_1(g) = N_2(g) = N_3(g) = g^2$, donde decorre que:

$$\lambda(\lambda^2+1)(g_1^2+g_2^2)=g_3^2 - (\lambda^2+1)g_4^2=g_5^2 + \lambda(\lambda^2+1)g_6^2$$

Vamos mostrar agora que a igualdade acima não pode ocorrer.

De fato, se tal igualdade ocorresse, então poderíamos reescolher os elementos g_i, $1 \leq i \leq 6$, de modo que o máximo divisor comum entre eles fosse igual a 1.

Consideramos então o homomorfismo canônico

$$\mathbb{Z}[\lambda] \to \frac{\mathbb{Z}}{2\mathbb{Z}}[\lambda]$$

Se a igualdade acima ocorresse, com

$$\mathrm{mdc}(g_i,\ 1 \leq i \leq 6) = 1,$$

teríamos

$$\bar{\lambda}(\bar{\lambda}+1)^2(\bar{g}_1+\bar{g}_2)^2 = (\bar{g}_3+(\bar{\lambda}+1)\bar{g}_4)^2=\bar{g}_5+\bar{\lambda}(\bar{\lambda}+1)^2\bar{g}_6^2$$

Comparando o grau do polinômio que aparece à esquerda com o do que aparece no meio, vemos que o primeiro tem grau ímpar, enquanto o segundo tem grau par, logo todos os polinômios envolvidos na igualdade acima são nulos, e temos

$$\bar{g}_1 = \bar{g}_2$$

$$\bar{g}_3 = (\bar{\lambda}+1)\bar{g}_4$$

$$\bar{g}_5^2 = \bar{\lambda}(\bar{\lambda}+1)^2\ \bar{g}_6^2$$

Aplicando o mesmo argumento para a igualdade

$$\bar{g}_5^2 = \bar{\lambda}(\bar{\lambda}+1)^2\ \bar{g}_6^2$$

obtemos que $\bar{g}_5 = \bar{g}_6 = 0$, donde $2|g_5$ e $2|g_6$. Assim

$$4|(g_5^2 + \lambda(\lambda^2+1)\ g_6^2) \quad \text{e portanto } 4|(\lambda(\lambda^2+1)(g_1^2+g_2^2)\ .$$

Conseqüentemente $4|(g_1^2+g_2^2)$ e $4|(g_3^2 - (\lambda^2+1)\ g_4^2)$.

Por outro lado, como $\bar{g}_1 = \bar{g}_2$, temos que existe um polinômio $h_1 \in \mathbb{Z}[\lambda]$ tal que $g_1 = g_2 + 2\ h_1$. Como $4|(g_1^2 + g_i^2)$, temos que $4|(\ 2g_2^2 + 4g_2h_1+4h_1^2)$ e portanto $4|2g_2^2$. Logo, $2|g_1^2$ donde $2|g_2$. Conseqüentemente, $2|g_1$.

Além disso, sabemos que existe um polinômio $h_3 \in \mathbb{Z}[\lambda]$ tal que $g_3 = (\lambda+1)g_4 + 2h_3$. Como

$$4|(g_3^2 - (\lambda^2+1)g_4^2)\ , \text{ vem que } 4|(2\lambda g_4^2+4(\lambda+1)h_3g_4+4h_3^2)$$

e portanto $2|\lambda g_4^2$. Logo, $2|g_4$ e $2|g_3$, absurdo pois

$$\text{mdc}(g_i \mid 1 \leq i \leq 6) = 1.$$

Com isto, concluímos a prova do lema. □

<u>10.2 TEOREMA</u> - Existe uma álgebra com divisão de grau 8 sobre seu centro, com involução, não isomorfa a um produto tensori-

al de álgebras de quatérnios.

DEMONSTRAÇÃO

Na notação do lema anterior, consideremos $b = \xi_2\xi_3 \in K$ e $\tau = \sigma_1\sigma_2\sigma_3$. Então

$$b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K) \quad e \quad b \notin F.N_1(K)$$

Conseqüentemente, pelo teorema (9.8) existe $U = \{u_{ij} \mid 1 \leq i,j \leq 3\} \subset K$ tal que $A = (K,G,U,\tau)$ é uma álgebra com divisão de grau 8 sobre seu centro, com involução, não isomorfa a um produto tensorial de álgebras de quatérnios.

$\square$

APÊNDICE

UM TEOREMA DE HERSTEIN-PROCESI-SCHACHER.

No capítulo I, afirmamos que se D é um anel com divisão de centro Z tal que para todo par de elementos $x, y \in D$, existe um inteiro positivo $n=n(x,y)$ verificando $(xy-yx)^n \in Z$, então $[D:Z] \leq 4$.

Esse resultado é, na verdade, uma aplicação imediata de um teorema mais geral, devido a I.N.Herstein, C.Procesi e M.Schacher, cuja prova é o objetivo deste apêndice, e que passamos a enunciar.

<u>TEOREMA</u> - Seja D um anel com divisão de centro Z e $f \in Z\{x_1,\ldots,x_r\}$ um polinômio nas variáveis não comutativas $\{x_1,\ldots,x_r\}$, com coeficientes em Z , verificando as seguintes condições:

(i) Existe um inteiro positivo $d \leq r$, tal que f é homogêneo em $\{x_1, \ldots, x_d\}$.

(ii) Dados $a_1, \ldots, a_r \in D$, existe um inteiro positivo $m = m(a_1, \ldots, a_r)$ tal que $f(a_1, \ldots, a_r)^{m(a_1, \ldots, a_r)} \in Z$.

(iii) Se $car(Z) = p > 0$, assumiremos ainda que f não é uma identidade polinomial para matrizes $p \times p$, em característica p.

Nessas condições, temos:

(1) $[D:Z] = n^2$, onde $n \leq \frac{1}{2}(\partial f + 2)$

(2) Se $n > 1$, f é uma identidade polinomial em $M_{n-1}(Z)$

(3) f^n é um polinômio central em $M_n(Z)$ (e portanto, dados $a_1, \ldots, a_r \in D$, $f(a_1, \ldots, a_r)^n \in Z$).

A referência básica para este apêndice é [8].

Começaremos enunciando uma proposição que será de fundamental importância para a prova do resultado acima mencionado. Sua demonstração pode ser encontrada em [8, lema 3.1].

11.1 - <u>PROPOSIÇÃO</u> - Sejam F um corpo e A uma F-álgebra simples central de dimensão finita n^2. Consideremos
$S = \{\alpha \in A \mid \alpha^{n(\alpha)} \in F$, para algum inteiro positivo $n(\alpha)\}$

Se F é finitamente gerado sobre seu corpo primo, então existe um inteiro positivo N tal que $\alpha^N \in F$, para todo $\alpha \in S$.

11.2 - TEOREMA (Kaplansky) - Sejam K,F corpos, $K \supsetneq F$ tais que dado $a \in K$, existe um inteiro positivo $n=n(a)$ verificando $a^{n(a)} \in F$. Então $car(K)=p>0$ e vale uma das seguintes condições.

(i) K é puramente inseparável sobre F ou

(ii) K é algébrico sobre seu corpo primo P.

DEMONSTRAÇÃO

Se $K|_F$ for puramente inseparável, então como $K \supsetneq F$ segue-se que $car(K)=p>0$ e o teorema está demonstrado. Logo, podemos supor que $K|_F$ não é puramente inseparável.

Neste caso, devemos mostrar que $car(K)=p>0$ e que a extensão $K|_P$ é algébrica. Dividiremos a demonstração desta parte em vários passos.

1º PASSO - Dado um elemento $a \in K$ tal que $a \notin F$ e a é separável sobre F então a é algébrico sobre P.

Seja $a \in K$ nessas condições. Por hipótese, sabemos que existe um inteiro positivo n tal que $a^n \in F$. Assim, a extensão F(a) é algébrica e separável sobre F. Logo, existe uma extensão normal e finita L de F tal que $L \supset F(a)$. Sendo L normal, existe um F-automorfismo $\phi: L \longrightarrow L$ tal que $\phi(a) = b \neq a$. Como $a^n \in F$, temos que $b^n \in F$, logo $b=\nu a$, onde $\nu \neq 1$ é uma raiz n-ésima da unidade.

Por outro lado, $\phi(a+1)=b+1$ e $(a+1)^m \in F$, para algum $m \in \mathbb{N}$. Repetindo o argumento acima, concluímos que existe uma raíz da unidade μ tal que

$$b+1 = \mu(a+1)$$

Observemos que como $\nu \neq 1$, temos que $\nu \neq \mu$. Assim, segue-se que

$$a = \frac{\mu-1}{\nu-\mu}$$

Mas μ e ν são raízes da unidade e portanto são algébricas sobre P. Como $a = \frac{\mu-1}{\nu-\mu}$, temos que a é algébrico sobre P.

<u>2º PASSO</u> - $car(K) = p>0$

Como $K|_F$ não é puramente inseparável sobre F e $K \neq F$, sabemos que existe um elemento $a \in K$, tal que $a \notin F$ e a é separável sobre F. Seja L_o uma extensão normal finita de P que contém a. Então, para todo $k \in \mathbb{Z}$, temos que $(a+k)$ é separável sobre F e $a+k \notin F$.

Da demonstração do primeiro passo, segue-se que

$$a+k = k\,\frac{\mu_k - 1}{\nu_k - \mu_k}$$

onde ν_k e μ_k são raízes da unidade em L_o.

Suponhamos por absurdo que $car(K)=0$. Então $\{a+k|k\in\mathbb{Z}\}$ é infinito. Logo, L_o é uma extensão finita dos racionais que contém um número infinito de raízes da unidade, o que é absurdo.

Assim, $car(K) = p>0$.

<u>3º PASSO</u> - $K|_P$ é algébrica.

Como $K|_F$ é algébrica, basta mostrar que $F|_P$ é algébrica.

Seja $x\in F$ qualquer e seja $a\in K$, $a\notin F$, separável sobre F. Então $(a+x)$ é separável sobre F e $(a+x)\notin F$. Pelo primeiro passo, segue-se que $(a+x)$ é algébrico sobre P. Como a é algébrico sobre P, temos que x é algébrico sobre P.

$\square$

Daqui por diante, salvo menção explícita em contrário, D denotará um anel com divisão de centro Z e $f\in Z\{x_1,\ldots,x_r\}$ será um polinômio nas variáveis não comutativas $\{x_1,\ldots,x_r\}$, com coeficientes em Z, satisfazendo as seguintes condições:

(i) f é homogêneo em $\{x_1,\ldots,x_d\}$ para algum $d\leq r$.

(ii) Dados $a_1,\ldots,a_r \in D$, existe $m=m(a_1,\ldots,a_r)\in \mathbb{N}$ tal que $f(a_1,\ldots,a_r)^m \in Z$.

11.3 - <u>LEMA</u> - Sejam $a_1,\ldots,a_r \in D$ tais que $f(a_1,\ldots,a_r)\neq 0$. Seja $K=C_D(a_1)\cap\ldots\cap C_D(a_r)$. Então K é um corpo, algébrico sobre Z

e vale uma das duas afirmações abaixo.

(a) $K|_Z$ é puramente inseparável ou

(b) Z é algébrico sobre um corpo finito.

DEMONSTRAÇÃO

É claro que K é um anel com divisão. Portanto, para mostrarmos que K é um corpo, basta provar que K é comutativo. Para isso, vamos mostrar que dado um elemento $\alpha \in K$, existe um inteiro positivo $n=n(\alpha)$ verificando $\alpha^n \in Z$. Daí decorrerá, por [5, teorema 3.2.2] que K é um corpo e que $K|_Z$ é algébrica.

Seja então $\alpha \in K$, arbitrário. Como $f \in Z\{x_1,\ldots,x_r\}$ satisfaz a condição (i), segue-se que existe um inteiro positivo k tal que

$$f(\alpha a_1,\ldots,\alpha a_d,a_{d+1},\ldots,a_r) = \alpha^k f(a_1,\ldots,a_d,a_{d+1},\ldots,a_k)$$

Por outro lado, temos que existem inteiros positivos m,n tais que

$$f(\alpha a_1,\ldots,\alpha a_d,a_{d+1},\ldots,a_r)^m \in Z \quad \text{e}$$

$$f(a_1,\ldots,a_d,a_{d+1},\ldots,a_r)^n \in Z$$

Como $\alpha \in K = C_D(a_1)\cap\ldots\cap C_D(a_r)$, obtemos:

$$\alpha^{mk} f(a_1,\ldots,a_r)^m = [\alpha^k f(a_1,\ldots,a_r)]^m =$$

$$= [f(\alpha a_1,\ldots,\alpha a_d, a_{d+1},\ldots a_r)]^m \in Z.$$

Logo, $\alpha^{mk} f(a_1,\ldots,a_r)^m \in Z$ e portanto $\alpha^{mnk} f(a_1,\ldots,a_r)^{mn} \in Z$. Mas, $f(a_1,\ldots,a_r)^{mn} \in Z$, donde $\alpha^{mnk} \in Z$.

Assim, $K|_Z$, está nas condições do teorema (11.2), do qual decorrem imediatamente as outras afirmações do lema.

$\square$

Daqui por diante passaremos a incluir nas nossas hipóteses, que <u>Z não é algébrico sobre um corpo finito</u>. Na verdade, isto não será uma restrição para o nosso teorema, pois mais tarde veremos que, a menos que D seja comutativo, esta hipótese decorre das demais.

11.4 - <u>LEMA</u> - Suponhamos que Z não seja algébrico sobre um corpo finito e que $[D:Z]=\infty$. Então, dado um elemento $u \in D$, algébrico sobre Z, temos que:

(a) O centro do $C_D(u)$ é o subcorpo de D gerado por Z e u.

(b) $[C_D(u):Z(u)] = \infty$

(c) u é puramente inseparável sobre Z.

DEMONSTRAÇÃO

(a) Seja $\alpha \in Z(u)$; então é claro que α comuta com u e portanto $\alpha \in C_D(u)$. Seja agora $x \in C_D(u)$. Queremos mostrar que $\alpha x = x\alpha$. Como $\alpha \in Z(u)$ e u é algébrico sobre Z, segue-se que $\alpha = \sum_{i=0}^{n} \alpha_i u^i$, onde $\alpha_i \in Z$, $0 \leq i \leq n$. Assim, como $x \in C_D(u)$, temos que

$$\alpha x = \left(\sum_{i=1}^{n} \alpha_i u^i\right) x = \sum_{i=0}^{n} (\alpha_i u^i x) = \sum_{i=0}^{n} (\alpha_i x u^i) =$$

$$= \sum_{i=0}^{n} x(\alpha_i u^i) = x\left(\sum_{i=0}^{n} \alpha_i u^i\right) = x\alpha.$$

Portanto, $Z(u) \subset Z(C_D(u))$, onde $Z(C_D(u))$ denota o centro do $C_D(u)$.

Para mostrarmos a outra inclusão, usaremos o Teorema do Duplo Centralizador [5, teorema 4.3.2], isto é, usaremos que $Z(u) = C_D(C_D(Z(u))$.

Seja então $\alpha \in Z(C_D(u))$. Devemos mostrar que $\alpha \in C_D(C_D(Z(u))$, ou seja, devemos mostrar que α comuta com todo elemento de $C_D(Z(u))$.

Seja $x \in C_D(Z(u))$. Então x comuta com todo elemento de $Z(u)$ e portanto x comuta, em particular, com u. Logo $x \in C_D(u)$. Como $\alpha \in Z(C_D(u))$, segue-se que α comuta com x.

Portanto, $Z(C_D(u)) \subset Z(u)$ com o que concluímos a demonstração de (a).

(b) Suponhamos por absurdo que $[C_D(u):Z(u)]<\infty$ e consideremos K um subcorpo maximal de $C_D(u)$. Então, $[K:Z(u)]<\infty$ e portanto $[K:Z]<\infty$.

Vamos mostrar que K é, na verdade, um subcorpo maximal de D; com isto chegaremos a uma contradição pois neste caso teríamos $[D:Z]=[K:Z]^2<\infty$.

Seja L um subcorpo de D tal que $K\subset L\subset D$. Então $Z(u)\subset L$ e portanto $u\in L$. Consideremos um elemento $x\in L$ qualquer. Como L é comutativo, segue-se que x comuta com u; logo $x\in C_D(u)$. Assim,

$$K\subset L\subset C_D(u)$$

e portanto K=L.

(c) Pela parte (b), sabemos que $[C_D(u):Z(u)]=\infty$; logo f não é uma identidade polinomial para $C_D(u)$; assim existem $a_1,\ldots,a_r \in C_D(u)$ tais que $f(a_1,\ldots,a_r) \neq 0$.

Como $u \in C_D(a_1)\cap\ldots\cap C_D(a_r)$ e Z não é algébrico sobre um corpo finito, segue-se pelo lema (11.3) que u é puramente inseparável sobre Z.

$\square$

Seja D um anel com divisão de centro Z e $f\in Z\{x_1,\ldots,x_r\}$ um polinômio nas variáveis não comutativas $\{x_1,\ldots,x_r\}$, satis

fazendo as condições (i) (ii) e (iii) do Teorema. Nessas condições, vale o seguinte

11.5 - LEMA - Se Z não é algébrico sobre um corpo finito, então $[D:Z]<\infty$.

DEMONSTRAÇÃO

Suponhamos por absurdo que $[D:Z] = \infty$. Dividiremos a prova em dois casos:

1º CASO: $car(Z) = 0$

Sejam $a_1,\ldots,a_r$ elementos quaisquer de D. Então, como f satisfaz a condição (ii), temos que $f(a_1,\ldots,a_r)$ é algébrico sobre Z, e portanto pelo lema (11.4,c) segue-se que $f(a_1,\ldots,a_r)$ é puramente inseparável sobre Z. Como $car(Z)=0$, decorre que $f(a_1,\ldots,a_r)\in Z$, para toda r-upla $(a_1,\ldots,a_r)$ de elementos de D. Assim $(fy-yf)$ é uma identidade polinomial para D; pelo teorema de Kaplansky ([5,teorema 6.3.1]), temos que $[D:Z] < \infty$, contradição.

2º CASO: $car(Z) = p>0$

Se f fosse um polinômio central para D, então, como antes, teríamos que $(f.y-y.f)$ seria uma identidade polinomial para D e portanto $[D:Z] <\infty$.

Logo, podemos supor que existem $b_1,\ldots,b_r \in D$ tais

que $\alpha = f(b_1,\ldots,b_r) \notin Z$. Como α é algébrico sobre Z, novamente pelo lema (11.4,c), temos que α é puramente inseparável sobre Z; logo existe um elemento $u \in D$, $u \notin Z$ tal que $u^p \in Z$. Nosso objetivo será mostrar que $u=0$, o que acarretará uma contradição.

Para isso, separaremos a demonstração em vários passos.

<u>1º PASSO</u> - Existe um elemento $y \in D$ tal que $v=[y,u]=yu-uy \neq 0$ e $[v,u]=0$.

De fato, como $u \notin Z$, existe $x \in D$ tal que $[x,u]=xu-ux \neq 0$. Consideremos então:

$$x_1=[x,u], \quad x_2=[x_1,u],\ldots,x_k=[x_{k-1},u].$$

Como $u^p \in Z$ e $car(Z)=p>0$, segue-se que $x_p=0$. Logo

$$\{k \in \mathbb{N} \mid x_k = 0\} \neq \phi$$

Seja $t = \min\{k \in \mathbb{N} \mid x_k = 0\}$.

Se $t=2$, consideremos $y=x$. Então $v=[x,u] = x_1 \neq 0$ e

$$[v,u] = [x_1,u] = x_2 = 0.$$

Se $t>2$, consideremos $y = x_{t-2}$. Então

$$v = [y,u] = x_{t-1} \neq 0 \qquad e$$

$$[v,u] = [x_{t-1},u] = x_t = 0$$

<u>2º PASSO</u> - Existe um elemento $w \in D$ tal que $u=[w,u]=[w^{p^n},u]$, para todo $n \in \mathbb{N}$.

Seja $v \in D$, como no 1º passo. Então $v \in C_D(u)$; logo $v=a.u$, onde $a \in C_D(u)$. Temos então:

$$u = a^{-1}v = a^{-1}(yu-uy) = a^{-1}yu-a^{-1}uy$$

Mas $a \in C_D(u)$; logo $u=a^{-1}yu-ua^{-1}y = [a^{-1}y,u]$.

Seja então $w = a^{-1}y$. Por construção, $u = [w,u]$.

Comutando esta igualdade p^n vezes com w e observando que $car(Z) = p$, obtemos

$$u = [w^{p^n},u] = [w,u], \quad \text{para todo } n \in N.$$

Em particular, $(w^p-w)u=u(w^p-w)$ donde, $w^p-w \in C_D(u)$.

Seja agora D_o a Z-álgebra gerada por u e w e seja L o centro de D_o. Então D_o é álgebra com divisão, e $(w^p-w) \in L$, pois (w^p-w) comuta com w e u.

Se $w^p-w=0$ então w pertence a $\mathbb{F}_p$, o corpo primo de L. Logo, $w\in Z$ e teríamos que $u=0$. Assim, podemos supor que

$$(w^p-w) \in L - \{0\}$$

<u>3º PASSO</u> - $[D_o:L] = p^2$.

Pela observação acima temos que $w^p-w\in L-\{0\}$. Logo w satisfaz um polinômio com coeficientes em L, da forma:

$$g(X) = X^p - X - \alpha, \qquad \text{com} \quad \alpha \neq 0.$$

Um tal polinômio ou é irredutível sobre L ou se decompõe completamente em L. Logo, se g(X) não for irredutível, teremos que $w\in L$. Novamente, isto implica que w comuta com u e portanto $u=0$.

Portanto, podemos supor que g(X) é irredutível sobre L e donde segue que $[L(w):L]=p$.

Mostraremos agora que $[D_o:L(w)]=p$.

De fato, como $u.w=w.u-u$, os elementos $(1,u,\ldots,u^{p-1})$ geram D_o como espaço vetorial à esquerda sobre L(w). Como $[D_o:L]$ é um quadrado perfeito, e $[L(w):L] = p$ segue-se que $[D_o:L] = p^2$.

<u>4º PASSO</u> - f não é uma identidade polinomial para D_o.

Suponhamos, por absurdo, que f seja uma identidade polinomial para D_o. Consideremos um corpo de decomposição E para D_o. Então

$$D_o \otimes_L E \simeq M_p(E).$$

Como L é um corpo infinito, segue-se por [14, teorema 3.16] que f é uma identidade para $M_p(E)$, o que contraria a hipótese.

Logo f não é identidade polinomial para D_o.

<u>5º PASSO</u> - u=0.

Pelo 4º passo, sabemos que existem elementos $a_1,\ldots,a_r \in D_o$, tais que $f(a_1,\ldots,a_r) \neq 0$.

Por outro lado, como $(w^p-w) \in L = Z(D_o)$, segue-se que

$$(w^p-w) \in C_D(a_1) \cap \ldots \cap C_D(a_r).$$

Assim, pelo lema (11.3), temos que (w^p-w) é puramente inseparável sobre Z. Em particular, w é algébrico sobre Z e portanto pelo lema (11.4), w é puramente inseparável sobre Z. Consequentemente, existe um inteiro positivo n tal que $w^{p^n} \in Z$. Mas então temos que

$$u = [w^{p^n}, u] = 0,$$

com o que concluimos a demonstração.

$\square$

O lema anterior mostra que nas hipóteses do teorema, se Z não é algébrico sobre um corpo finito então $[D:Z]<\infty$.

Nosso objetivo agora será demonstrar que, nas hipóteses do teorema, Z não é algébrico sobre um corpo finito, a menos que D seja comutativo.

11.6 - PROPOSIÇÃO - Seja D um anel com divisão de centro Z, não comutativo, e $f \in Z\{x_1,\ldots,x_r\}$ satisfazendo as condições do teorema. Então Z não é algébrico sobre um corpo finito.

DEMONSTRAÇÃO

Suponhamos, por absurdo, que Z seja algébrico sobre um corpo finito. Então $car(Z) = p>0$.

Vamos mostrar que isto implica que D é comutativo.

REDUÇÃO - Podemos supor que existe um elemento $\alpha \in D$, algébrico sobre Z, de grau $n>1$.

É claro que existem elementos em D algébricos sobre Z, pois todo elemento da forma $\alpha=f(a_1,\ldots,a_r)$ é algébrico sobre Z, pela hipótese (ii) do teorema.

Logo, se os únicos elementos de D, algébricos sobre Z, são os elementos de Z, então ou f é uma identidade po

linomial para D ou f é um polinômio central para D.

De toda forma, pelo teorema de Kaplansky [5, teorema 6.3.1], teríamos que $[D:Z] < \infty$.

Como Z é algébrico sobre um corpo finito, Z é algébrico sobre seu corpo primo $\mathbb{F}_p$. Logo D é algébrico sobre $\mathbb{F}_p$. Consequentemente, dado um elemento qualquer $x \in D$, existe um inteiro positivo $n=n(x)$ tal que $x^{p^n}=x$. Portanto, por [5, lema 3.1.3], segue-se que D é comutativo, com o que concluiríamos a demonstração.

Logo, podemos supor que D possui elementos algébricos sobre Z, de grau $n>1$.

Vamos mostrar agora que dado um elemento $\alpha \in D$, algébrico sobre Z de grau $n>1$, então $n \leq \frac{1}{2}(\partial f+2)$.

Para provarmos essa afirmação, construiremos, em primeiro lugar, um anel com divisão $D_o \subset D$, de dimensão finita n^2 sobre seu centro Z_o, que satisfaz todas as hipóteses do Teorema de Herstein-Procesi-Schacher.

Consideremos a extensão $Z(\alpha)$ de Z. Como Z é algébrico sobre seu corpo primo $\mathbb{F}_p$, segue-se que a extensão $Z(\alpha)|Z$ é galoisiana, com grupo de Galois cíclico, gerado por um elemento σ, onde $o(\sigma)=n$.

Aplicando o teorema de Skolem-Nöether ao Z-automorfismo σ de $Z(\alpha)$, temos que existe um elemento não nulo $u \in D$

tal que

$$\sigma(x) = u\,x\,u^{-1} \quad , \quad \text{para todo } x \in Z(\alpha).$$

Seja $D_o = Z(\alpha,u)$, o anel com divisão gerado por α e u e denotemos por Z_o o centro de D_o.

Como $[Z(\alpha):Z] = n$ e $u\alpha=\sigma(\alpha)u$, o conjunto $\{u^i\alpha^j \mid 0\leq i,j\leq n-1\}$ gera D_o sobre Z_o.

Além disso, o conjunto $\{u^i \mid 0\leq i\leq n-1\}$ é linearmente independente sobre $Z(\alpha)$ e gera D_o sobre $Z(\alpha)$. Logo, $[D_o:Z_o]=n^2$.

Consideremos então $(e_1,\ldots,e_{n^2})$ uma base de D_o sobre Z_o. Temos:

$$e_i\,e_j = \sum_{k=1}^{n^2} a_{ijk}\,e_k \ ,$$

onde $a_{ijk} \in Z_o$, $1\leq i,j,k\leq n^2$.

Sejam ainda L o menor subcorpo de D_o que contém $\mathbb{F}_p$, os coeficientes de f e os a_{ijk}, $1\leq i,j,k\leq n^2$ e D_1 a álgebra com divisão de centro L gerada pelos $(e_i)_{1\leq i\leq n^2}$.

Observemos que $f \in L\{x_1,\ldots,x_r\}$. Além disso, se $a_1,\ldots,a_r$ são elementos de D_1 então é claro que $f(a_1,\ldots,a_r)\in D_1$. Por hipótese, existe $m=m(a_1,\ldots,a_r)\in\mathbb{N}$ tal que $f(a_1,\ldots,a_r)^m \in Z$. Logo, $f(a_1,\ldots,a_r)^m$ comuta com todo elemento de D e, em particular, comuta com todo elemento de D_1. Assim, $f(a_1,\ldots,a_r)^m \in L$.

Portanto, mostramos que dados $a_1,\ldots,a_r \in D_1$, existe $m=m(a_1,\ldots,a_r)\in\mathbb{N}$ tal que $f(a_1,\ldots,a_r)^m\in L$.

Como L é finitamente gerado sobre seu corpo primo $\mathbb{F}_p$, segue-se pela proposição (11.1), que existe um inteiro positivo N tal que f^N é um polinômio central em D_1.

Voltemos agora à álgebra D_o. Observemos inicialmente que $D_o = D_1 \otimes_L Z_o$. Além disso, L é um corpo infinito pois, caso contrário, teríamos $D_1=L$ e portanto n=1, o que não ocorre.

Como f^N é um polinômio central em D_1 e L é um corpo infinito, segue-se que f^N é um polinômio central em D_o. Agora, por [14, pág. 172], segue-se que f^N é uma identidade para $M_{n-1}(Z)$ e portanto por [14, pág. 64] temos que f é uma identidade em $M_{n-1}(Z)$; logo $2(n-1)\leq\partial f$, donde $n\leq \frac{1}{2}(\partial f+2)$, com o que concluímos a demonstração da nossa afirmação.

Vamos mostrar agora que D possui um subcorpo maximal de dimensão finita sobre Z.

Para isso, consideremos K um subcorpo maximal de D, com relação à propriedade de ser algébrico sobre Z. Como todo elemento de D, que é algébrico sobre Z, tem grau menor ou igual a $\frac{1}{2}(\partial f+2)$, segue-se que $[K:Z]<\infty$. Vamos demonstrar que K é um subcorpo maximal de D, provando que $C_D(K) = K$.

Seja então $\Delta = C_D(K)$. Pelo teorema do duplo Centra-

lizador, [5, teorema 4.3.2], segue-se que $K = Z(\Delta)$, o centro de Δ. Logo, Δ é anel com divisão de centro K. Além disso, dados $a_1,\ldots,a_r \in \Delta$, temos que $f(a_1,\ldots,a_r)$ é algébrico sobre Z, e portanto $f(a_1,\ldots,a_r) \in K$. Assim, $f.y-y.f$ é uma identidade polinomial para Δ; logo, pelo teorema de Kaplansky, $[\Delta:K]<\infty$.

Por outro lado, como Z é algébrico sobre $\mathbb{F}_p$, temos que Δ é algébrico sobre $\mathbb{F}_p$. Novamente, por [5, lema 3.1.3], temos que Δ é comutativo e portanto $\Delta = K = C_D(K)$.

Logo, K é um subcorpo maximal de D e $[K:Z]<\infty$. Consequentemente, $[D:Z] = [K:Z]^2 < \infty$, o que implica, como antes, que D é comutativo; contradição.

□

Finalmente estamos em condições de demonstrar o teorema de Herstein-Procesi-Schacher, que reenunciamos abaixo.

11.7 - <u>TEOREMA</u> - Sejam D um anel com divisão de centro Z e $f \in Z\{x_1,\ldots,x_r\}$ um polinômio nas variáveis não comutativas $\{x_1,\ldots,x_r\}$ verificando as seguintes condições:

(i) f é homogêneo em $\{x_1,\ldots,x_d\}$, para algum inteiro d, $1 \leq d \leq r$.

(ii) Dados $a_1,\ldots,a_r \in D$, existe um inteiro positivo $m=m(a_1,\ldots,a_r)$ tal que $f(a_1,\ldots,a_r)^m \in Z$.

Se $car(Z)=p>0$, assumiremos ainda que f não é uma i-

dentidade polinomial para matrizes p×p em característica p.

Nessas condições, temos:

(1) $[D:Z] = n^2$, onde $n \leq \frac{1}{2}(\partial f+2)$

(2) Se $n>1$, f é uma identidade polinomial em $M_{n-1}(Z)$

(3) f^n é um polinômio central em $M_n(Z)$ e dados $a_1,\ldots,a_r \in D$ podemos tomar $m=m(a_1,\ldots,a_r) = n$.

DEMONSTRAÇÃO

Separaremos a demonstração em dois casos:

1º CASO - Z é algébrico sobre um corpo finito.

Nessa situação, pela proposição (11.6), temos que D é comutativo. Logo $[D:Z] = 1$ e as afirmações decorrem trivialmente.

2º CASO - Z não é algébrico sobre um corpo finito.

Nessa situação, pelo lema (11.5), temos que $[D:Z]=n^2<\infty$.

Consideremos então $\{e_1,\ldots,e_{n^2}\}$ uma base de D sobre Z. Temos que

$$e_i e_j = \sum_{k=1}^{n^2} a_{ij}^k e_k ,$$

onde $a_{ij}^k \in Z$, $1 \leq i,j,k \leq n^2$.

Seja P o corpo primo de Z e consideremos L o subcorpo de D gerado por P, pelos coeficientes de f e pelo conjunto $\{a_{ij}^k \in Z \mid 1 \leq i,j,k \leq n^2\}$. Então L é finitamente gerado sobre seu corpo primo P. Além disso, $L \subset Z$ e portanto o conjunto $\{e_i \mid 1 \leq i \leq n^2\}$ é linearmente independente sobre L.

Seja D_o o anel com divisão de centro L, gerado pelo conjunto $\{e_i \mid 1 \leq i \leq n^2\}$. Então $[D_o:L] = n^2$ e ainda $f \in L\{x_1,\ldots,x_r\}$.

Além disso, D_o satisfaz a condição (ii). Logo, pela proposição (11.1), existe um inteiro positivo N tal que f^N é um polinômio central em D_o.

Por outro lado, podemos supor que L é um corpo infinito, pois, caso contrário, teríamos que D_o é comutativo. Como $D = D_o \otimes_Z L$, teríamos que D é também comutativo e nesse caso, o teorema segue trivialmente.

Assim, como $L \subset Z$, temos que Z é um corpo infinito, e como $(f^N y - y f^N)$ é uma identidade para D_o, segue-se então que $(f^N y - y f^N)$ é uma identidade para D. Logo, f^N é um polinômio central em D.

Consideremos agora F um corpo de decomposição para D. Então $D \otimes_Z F \simeq M_n(F)$.

Como F é infinito, temos que $(f^N y - y f^N)$ é uma identidade em $M_n(F)$ e portanto em $M_n(Z)$. Consequentemente, f^N é um polinômio central em $M_n(Z)$. Por [14, pag. 172] , segue-se que

f^N é uma identidade em $M_{n-1}(Z)$.

Novamente, como Z é um corpo infinito, temos por [14, pág. 64] que f é uma identidade em $M_{n-1}(Z)$. Logo, $2(n-1) \leq \partial f$, donde $n \leq \frac{1}{2}(\partial f+2)$.

Resta, portanto, provar a afirmação (3) do teorema.

Já sabemos que f^N é central em $M_n(Z)$. Logo, por [8, lema 3.6], segue-se que f^n é central em $M_n(Z)$. Por outro lado,

$$D \underset{Z}{\otimes} M_n(Z) \simeq M_n(D)$$

Como f^n é central em $M_n(Z)$ e Z é um corpo infinito, temos que f^n é central em $M_n(D)$ e portanto é central em D.

Assim, dados $a_1,\ldots,a_r$ elementos de D, podemos tomar $m = m(a_1,\ldots,a_r) = n$.

Com isto o teorema está demonstrado.

$\square$

BIBLIOGRAFIA

[1] ALBERT, A.A. *Structure of algebras*. New York, AMS, 1939. 210p. (American Mathematical Society Colloquium Publications, 24)

[2] AMITSUR, S.A. & SALTMAN, D. Generic Abelian crossed products and p-algebras. *Journal of Algebra*, 51(1): 76-87, 1978.

[3] AMITSUR, S.A.; ROWEN, L.H.; TIGNOL, J.P. Division algebras of degree 4 and 8 with involution. *Israel Journal of Mathematics*, 33(2):133-148, 1979.

[4] FELZENSZWALB, B. *Algebras de dimensão finitas*. Rio de Janeiro, IMPA, 1979. 105p. Trab. apres. ao 12º Coloquio Brasileiro de Matemática, Poços de Caldas, 1979.

[5] HERSTEIN, I.N. *Noncommutative rings*. S.l.p., MAA, 1968. 199p. (The Carus Mathematical Monographs, 15)

[6] HERSTEIN, I.N. *Topics in ring theory*. Chicago, University Press, 1969. 132p.

[7] HERSTEIN, I.N. *Rings with involution*. Chicago, University Press, 1976. 247p. (Chicago Lectures in Mathematics).

[8] HERSTEIN, I.N.; PROCESI, C.; SCHACHER, M. Algebraic valued functions on noncommutative rings. *Journal of Algebra*, *36*(1):128-150, 1975.

[9] HOFFMAN, K. & KUNZE, R.A. *Algebra linear*. 2.ed. São Paulo, Livros Técnicos e Científicos, 1979. 514p.

[10] JACOBSON, N. *Structure of rings*. Providence, AMS, 1956. 299p. (American Mathematical Society Colloquium Publications, 37).

[11] JACOBSON, N. *Structure and representations of Jordan algebras*. Providence, AMS, 1968. 453p. (American Mathematical Society Colloquium Publications, 39).

[12] KAPLANSKY, I. *Fields and rings*. 2.ed. Chicago, University Press, 1972. 206p. (Chicago Lectures in Mathematics).

[13] KLEIN, A.A. A new proof of a result of Levitzki. *Proceedings of the American Mathematical Society*, *81*(1):8, 1981.

[14] PROCESI, C. *Rings with polynomial identities*. New York, Marcel Dekker, 1973. 109p. (Pure and Applied Mathematics, 17).

[15] ROWEN, L.H. Central simple algebras. *Israel Journal of Mathematics*, 29(2-3):285-301, 1978.

[16] SMITH, K.C. *Algebraic characterizations of quaternions algebras: a survey.*

[17] SMITH, K.C. A characterization of quaternion division algebras. *Rocky Mountain Journal of Mathematics*, 9(2):371-375, 1979.

[18] VAN PRAAG, P. Une caractérisation des corps de quaternions. *Bulletin de la Société Mathématique de Belgique*, 20:283-285, 1968.