Tópicos de álgebras alternativas

Marcos Munhoz

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do grau de Mestre
em
Ciências

Área de concentração: Matemática Orientador: Prof. Dr. Henrique Guzzo Junior

São Paulo, fevereiro de 2007

Tópicos de álgebras alternativas

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Marcos Munhoz e aprovada pela Comissão Julgadora.

São Paulo, 23 de fevereiro de 2007.

Banca Examinadora:

Prof. Dr. Henrique Guzzo Junior (orientador) — IME/USP

Prof. Dr. Juan Carlos Gutiérrez Fernández — IME/USP

Prof. Dr. Plamen Emilov Kochloukov - IMECC/UNICAMP

Resumo

Neste trabalho são apresentados alguns aspectos das álgebras alternativas, em especial o bar radical de uma álgebra bárica alternativa e as identidades de graus 4 e 5 nas álgebras de Cayley-Dickson. Estudamos alguns resultados importantes sobre as álgebras báricas alternativas, em particular aqueles envolvendo o radical, o bar ideal e o bar radical, fazendo uso da Decomposição de Peirce. No estudo das identidades nas álgebras de Cayley-Dickson, foram utilizadas diversas técnicas e propriedades das álgebras alternativas, onde mostramos que não existem identidades de grau 4, além das triviais e que as identidades de grau 5 são conseqüências de outras duas identidades conhecidas.

Abstract

In this work we present some aspects of alternative algebras, in special the bar radical of an alternative baric algebra and identities of degree 4 and 5 of Cayley-Dickson algebras. We studied some important results about alternative baric algebras, particularly those related with the radical, the bar-ideal and the bar radical, with the use of the Peirce decomposition. In the study of the identities in Cayley-Dickson algebras we made wide use of several techniques and properties of alternative algebras, in order to show that the only identities of degree four are the trivial ones, and the identities of degree five are consequences of other two known identities.

Sumário

Introdução				
1	Álgebras Alternativas			
	1.1	Conceitos Básicos	7	
	1.2	Álgebras Alternativas	10	
	1.3	Decomposição de Peirce	21	
	1.4	Álgebras Báricas	31	
2	Rac	dical e Semisimplicidade	36	
	2.1	O Radical	36	
	2.2	Decomposição de Peirce em álgebras báricas	50	
	2.3	O radical e o bar radical	56	
3	Álgebras de Composição			
	3.1	A descoberta dos quatérnios	71	
	3.2	As Álgebras de Composição	73	
	3.3	Processo de Duplicação de Cayley-Dickson	79	
	3.4	Exemplos de Álgebras de Composição	84	
	3.5	Hurwitz e a Soma de Quadrados	88	
4	Identidades em Álgebras de Cayley			
	4.1	Introdução	92	
	4.2	Álgebras Livres	93	
	4.3	Identidades Polinomiais	96	
	4.4	A Álgebra Exterior - Principais Resultados	101	
	4.5	Identidades nos Octônios - Grau 4	109	

Bibliografia			
4.7	Resultados Recentes	. 146	
4.6	Identidades nos Octônios - Grau 5	. 115	

Introdução

O presente trabalho é um estudo das álgebras alternativas tanto em seus aspectos gerais como em manifestações particulares, que são as álgebras báricas e as álgebras de Cayley. Nas álgebras báricas indicamos importantes resultados relacionados ao radical e ao bar-radical. Nas álgebras de Cayley fazemos uma exposição das identidades, seja na sua determinação como na verificação de propriedades usando métodos matriciais.

O Capítulo 1 trata dos conceitos básicos das álgebras alternativas, estuda a sua decomposição de Peirce tanto em relação a um idempotente quanto em relação a um conjunto de idempotentes primitivos dois a dois ortogonais. São apresentadas também as idéias preliminares referentes às álgebras báricas, em especial, as álgebras báricas alternativas.

O Capítulo 2 estabelece os conceitos de radical e semisimplicidade, demonstrando os principais teoremas relacionados. São estudados o bar(A), o bar-radical e o radical nil de A, além da semisimplicidade no sentido bárico e no sentido usual.

O Capítulo 3 é dedicado a um estudo teórico das álgebras de composição, descrevendo o processo de duplicação de Cayley-Dickson que permite obter todas as álgebras de composição. Demonstramos o Teorema de Hurwitz sobre as álgebras de composição.

O Capítulo 4 se refere às identidades nas álgebras de Cayley, em particular, as de grau 4, com resultados fundamentados nos teoremas de Amitsur-Levitzki, e as identidades de grau 5, onde mostramos que são conseqüências de outras identidades resultantes do conceito de derivações em álgebras de Jordan. Concluímos o trabalho mencionando alguns resultados recentes sobre as identidades de grau 6 nas álgebras de Cayley e de grau 7 nas álgebras alternativas, em que alguns autores utilizaram métodos computacionais na sua pesquisa.

Capítulo 1

Álgebras Alternativas

As álgebras alternativas são um importante exemplo de álgebras em que a propriedade associativa não é assumida em sua definição, mas que pode valer em casos particulares. Uma ampla gama de aplicações são conhecidas e seu estudo conduz a resultados gerais que permitem estabelecer de forma inequívoca uma série de propriedades destas álgebras. Daremos neste capítulo as definições básicas e os principais resultados, para no capítulo seguinte aprofundarmos um pouco mais este estudo.

1.1 Conceitos Básicos

Vamos trabalhar com álgebras sobre um corpo F. Uma álgebra A sobre um corpo F é um espaço vetorial onde está definido um produto de elementos de A, satisfazendo, para todos x, y, z em A e α em F:

$$(x + y)z = xz + yz$$
$$x(y + z) = xy + xz$$
$$\alpha(xy) = (\alpha x)y = x(\alpha y)$$

Definição 1.1.1. Seja A uma álgebra.

- (i) Se $(xy)z = x(yz) \quad \forall x, y, z \in A$, dizemos que A é uma álgebra associativa.
- (ii) Sejam $x, y, z \in A$. Definimos o **associador** de A por: (x, y, z) = (xy)z x(yz).
- (iii) O núcleo de uma álgebra A, denotado por Z é o conjunto dos elementos z em A que se associam com todos os elementos de A.

$$z \in Z \iff \forall x, y \in A, (x, y, z) = (x, z, y) = (z, x, y) = 0.$$

(iv) O centro de uma álgebra A, denotado por C é o conjunto dos elementos c em A que comutam e se associam com todos os elementos de A.

$$\mathcal{C} = \{ c \in Z \mid xc = cx, \ \forall x, y \in A \}.$$

Se A é associativa, então A = Z. No caso geral: $C \subseteq Z \subseteq A$.

Definição 1.1.2. Sejam A uma álgebra e X, I, B, C subconjuntos de A.

- (i) X é chamado uma **subálgebra** de A se X é um subespaço vetorial de A e X é um subanel de A. Notação: $X \leq A$, ou X < A, se $X \neq A$.
- (ii) I é chamado **ideal** de A se I é um ideal de A considerando A como anel e $\forall \alpha \in F, \forall \alpha \in A, \text{ tem-se: } \alpha \alpha \in I.$
- (iii) Indicaremos por $\langle X \rangle$ o subespaço de A gerado por X.
- (iv) De modo usual a **subálgebra de** A **gerada por** X é a intersecção de todas as subálgebras de A que contêm X. Denotamos por A(X). Quando $X = \{x_1, \ldots, x_n\}$ escrevemos $A(\{x_1, \ldots, x_n\}) = A(x_1, \ldots, x_n)$.
- (v) Indicamos por BC o seguinte subconjunto:

$$BC = \langle bc \mid b \in B, c \in C \rangle$$

Para ilustrar melhor o conjunto BC acima definido, note que:

$$u \in BC \Leftrightarrow \exists n \in \mathbb{N} \text{ e } b_1, \dots, b_n \in B, c_1, \dots, c_n \in C, \alpha_1, \dots, \alpha_n \in F \text{ tais que}$$

$$u = \sum_{i=1}^n \alpha_i b_i c_i$$

Definição 1.1.3. Sejam A e B álgebras sobre um corpo F. Uma aplicação $\phi: A \to B$ é chamada um **homomorfismo** entre A e B se valer, para todos $a, b \in A$ e $\alpha \in F$:

- (i) $\phi(a+b) = \phi(a) + \phi(b)$;
- (ii) $\phi(\alpha a) = \alpha \phi(a)$;
- (iii) $\phi(ab) = \phi(a)\phi(b)$.

As potências em uma álgebra arbitrária devem ser definidas com especial atenção, uma vez que, se A é uma álgebra associativa, a potência n-ésima de um elemento $x \in A$ é definida como:

$$x^{1} = x;$$
 $x^{n} = (x^{n-1})x,$ se $n > 1$

Esta definição traz como consequência que:

$$x^{n+m} = x^n x^m, \ \forall \ x \in A, \ \forall \ m, n \in \mathbb{N}$$

o que é válido devido à lei associativa. Mas se A é uma álgebra arbitrária, tal propriedade não vale sempre. A definição a seguir estabelece o conceito de potência no contexto mais geral.

Definição 1.1.4. Sejam A uma álgebra, $B \subset A$ subálgebra $e \ x \in A$.

(i) A potência principal à esquerda e à direita de x é dada por:

$$^{1}x = x$$
 $^{n+1}x = x(^{n}x)$ $n \in \mathbb{N}$
 $x^{1} = x$ $x^{n+1} = (x^{n})x$ $n \in \mathbb{N}$

(ii) A potência principal à esquerda e à direita de B é dada por:

$$^{1}B = B$$
 $^{n+1}B = B(^{n}B)$ $n \in \mathbb{N}$
 $B^{1} = B$ $B^{n+1} = (B^{n})B$ $n \in \mathbb{N}$

(iii) A potência principal de B é dada por:

$$B^{(1)} = B \quad B^{(n+1)} = \left\langle BB^{(n)}, B^{(n)}B \right\rangle \quad n \in \mathbb{N}$$

(iv) A potência plena de B é dada por:

$$B^{[1]} = B \quad B^{[n+1]} = B^{[n]}B^{[n]} \quad n \in \mathbb{N}$$

Definição 1.1.5. Sejam A uma álgebra não-associativa, $B \subset A$ e $x \in A$.

- (i) $x \in A$ é nilpotente à esquerda de índice k, se k = 0, mas $k-1 x \neq 0$.
- (ii) $B \subset A$, subálgebra é **nil à esquerda** se x é nilpotente à esquerda, $\forall x \in B$.
- (iii) $B \subset A$, subálgebra é **nilpotente** à **esquerda** de índice k, se ${}^kB = 0$, mas ${}^{k-1}B \neq 0$.
- (iv) $B \notin nilpotente$ de índice k, se $B^{(k)} = 0$, mas $B^{(k-1)} \neq 0$. Se k = 2, $B \notin chamada uma zero álgebra$.
- (iv) $B \subset A$ é **solúvel** de índice k se $B^{[k]} = 0$, mas $B^{[k-1]} \neq 0$.

Definição 1.1.6. Seja A uma álgebra não-associativa e $a \in A$. Definimos

(i) O operador multiplicativo à direita de A, determinado por a:

$$R_a: A \to A$$

 $x \mapsto xa$

(ii) O operador multiplicativo à esquerda de A, determinado por a:

$$L_a: A \to A$$

 $x \mapsto ax$

OBS.: R_a e L_a são operadores lineares.

1.2 Álgebras Alternativas

Uma álgebra A sobre um corpo F é chamada **alternativa** se, para todos $x, y \in A$, vale:

$$x^2y = x(xy)$$
 (Lei alternativa à esquerda)
 $yx^2 = (yx)x$ (Lei alternativa à direita)

Estas condições podem ser expressas em termos de associadores como segue:

$$(x, x, y) = (y, x, x) = 0$$

Vamos mostrar algumas propriedades simples envolvendo as álgebras alternativas, as quais serão úteis em aplicações posteriores.

Teorema 1.2.1. Em uma álgebra alternativa A, tem-se, para todos x, y, z em A:

(i)
$$L_{x^2} = L_x^2$$
, $R_{x^2} = R_x^2$;

(ii)
$$(x, y, z) = -(y, x, z) = (y, z, x);$$

(iii)
$$(x, y, x) = 0$$
 (Lei Flexível);

(iv)
$$R_x L_x = L_x R_x$$
.

Demonstração:

(i)
$$yL_{x^2} = x^2y = x(xy) = (xy)L_x = (yL_x)L_x = yL_x^2$$

 $yR_{x^2} = yx^2 = (yx)x = (yx)R_x = (yR_x)R_x = yR_x^2$

(ii) Para mostrar esta propriedade usamos a bilinearidade do associador:

$$0 = (x + y, x + y, z) = (x, x, z) + (y, x, z) + (x, y, z) + (y, y, z)$$
$$\Rightarrow 0 + (y, x, z) + (x, y, z) + 0 = 0$$

Portanto: (x, y, z) = -(y, x, z). Para a segunda igualdade temos:

$$0 = (x, y + z, y + z) = (x, y, y) + (x, y, z) + (x, z, y) + (x, z, z)$$
$$\Rightarrow (x, y, z) = -(x, z, y)$$

Fazendo x = y, y = z e z = x obtemos: (y, z, x) = -(y, x, z)

(iii)
$$0 = (x + y, y + x, x) = (x, y, x) + (x, x, x) + (y, y, x) + (y, x, x)$$

= $(x, y, x) + 0 + 0 + 0 \Rightarrow (x, y, x) = 0$

(iv) É consequência direta da lei flexível.

Teorema 1.2.2 (Identidades de Moufang). Seja A uma álgebra alternativa. Para todos $a, x, y \in A$, são válidas as sequintes identidades:

- (i) (xax)y = x(a(xy));
- (ii) (xy)(ax) = x(ya)x;
- (iii) y(xax) = ((yx)a)x.

Demonstração:

(i) (xax)y = x(a(xy))

Lembrando que, pela lei flexível, podemos escrever sem ambigüidade xax, uma vez que: 0 = (x, a, x) = (xa)x - x(ax), logo (xa)x = x(ax) = xax. Calculemos: (xax)y - x(a(xy))

$$(xax)y - x(a(xy)) = (xa, x, y) + (x, a, xy)$$

= $-(x, xa, y) - (x, xy, a)$

$$= -((x^{2}a)y - x((xa)y)) - ((x^{2}y)a - x((xy)a))$$

$$= -(x^{2}a)y - (x^{2}y)a + x((xa)y + (xy)a)$$

$$= -(x^{2}, a, y) - x^{2}(ay) - (x^{2}, y, a) - x^{2}(ya)$$

$$+ x((xa)y + (xy)a)$$

$$= x(-x(ay) - x(ya) + (xa)y + (xy)a)$$

$$= x((x, a, y) + (x, y, a)) = 0$$

(ii) (xy)(ax) = x(ya)x

$$(xy)(ax) - x(ya)x = (x, y, ax) + x(y(ax)) - x(ya)x$$

$$= (x, y, ax) + x(y(ax) - (ya)x)$$

$$= (x, y, ax) - x(y, a, x)$$

$$= -(x, ax, y) - x(y, a, x)$$

$$= x((ax)y) - (xax)y - x(y, a, x)$$

$$\stackrel{(i)}{=} x((ax)y - a(xy) - (y, a, x))$$

$$= x((a, x, y) - (y, a, x)) = 0$$

(iii) y(xax) = ((yx)a)x

$$\begin{array}{lll} y((xa)x) - ((yx)a)x & = & [(y(xa))x - (y,xa,x)] - [(y,x,a)x + (y(xa))x] \\ \\ & = & (xa,y,x) - (x,a,y)x \\ \\ & = & ((xa)y)x - (xa)(yx) - ((xa)y)x + x(ay)x \\ \\ \stackrel{(ii)}{=} & -x(ay)x + x(ay)x = 0 \end{array}$$

Corolário 1.2.3. Seja A uma álgebra alternativa. Então, para todos a, x, y, z em A, tem-se: (y, xa, z) + (y, za, x) = -(y, x, a)z - (y, z, a)x

Demonstração: A igualdade (iii) de Moufang equivale a: (y, xa, x) = -(y, x, a)x. De fato:

$$(y, xa, x) = (y(xa))x - y(xax) = (y(xa))x - ((yx)a)x = (y(xa) - (yx)a)x$$

= $-(y, x, a)x$

Linearizando a expressão (y, xa, x), temos:

$$(y, xa + za, x + z) = (y, (x + z)a, x + z)$$

$$= -(y, x + z, a)(x + z) = -(y, x + z, a)x - (y, x + z, a)z$$

$$= -(y, x, a)x - (y, z, a)x - (y, x, a)z - (y, z, a)z$$
(1)

Por outro lado, pela tri-linearidade do associador:

$$(y, xa + za, x + z) = (y, xa, x) + (y, xa, z) + (y, za, x) + (y, za, z)$$
$$= -(y, x, a)x + (y, xa, z) + (y, za, x) - (y, z, a)z$$
(2)

Igualando (1) e (2), temos:

$$-(y, x, a)x - (y, z, a)x - (y, x, a)z - (y, z, a)z$$

$$= -(y, x, a)x + (y, xa, z) + (y, za, x) - (y, z, a)z$$

$$\Rightarrow (y, xa, z) + (y, za, x) = -(y, x, a)z - (y, z, a)x$$

Definição 1.2.1. Seja A uma álgebra e $x, y \in A$. Denotamos por p = p(x, y) qualquer produto (não-associativo) de t elementos z_1, \ldots, z_t , onde cada z_i é igual a x ou y. O número t de elementos no produto é chamado de **grau** de p, o qual denotaremos por ∂p . Esta definição se aplica igualmente para um produto de qualquer número de elementos, como p = p(x, y, z), p = p(x, y, z, w), etc, onde $x, y, z, w \in A$.

Exemplos

- (a) Seja $p = x^2(yx)$. Podemos escrever: p = (xx)(yx). Portanto $\partial p = 4$.
- (b) $p = (xy^2)(z(xz^3))$. Temos então: $\partial p = 8$.

Teorema 1.2.4 (Artin). A subálgebra gerada por quaisquer dois elementos de uma álgebra alternativa A é associativa.

Demonstração: Sejam $x, y \in A$ quaisquer. Seja p = p(x, y) qualquer produto não-associativo z_1, z_2, \ldots, z_t , com alguma distribuição de parêntesis, onde $z_i = x$ ou $z_i = y$.

É suficiente provar que (p,q,r)=0 para todos os produtos não-associativos p=p(x,y), q=q(x,y) e r=r(x,y). Vamos provar por indução em $n=\partial p+\partial q+\partial r$.

O resultado é imediato para n < 3, pois, neste caso, pelo menos o grau de um dos produtos será zero.

Assumimos como hipótese de indução que (p,q,r)=0 se $\partial p+\partial q+\partial r< n$. Então, como $\partial p< n$, no produto p=p(x,y) vale a associativa. Desta forma os parêntesis não são necessários em $p(x,y)=z_1z_2\ldots z_n$ e podemos supor que p começa com z_1 .

Naturalmente este mesmo raciocínio vale para os outros produtos q e r. Desta forma, dois dos produtos p, q, r devem começar com a mesma letra. Vamos supor que q e r começam com x.

Temos 3 casos a considerar:

(1)
$$\partial q > 1$$
 e $\partial r > 1$

Temos que: q = q'x e r = r'x. Daí

$$\partial q = 1 + \partial q' \Rightarrow \partial q' = -1 + \partial q \in \partial r = 1 + \partial r' \Rightarrow \partial r' = -1 + \partial r$$

Então:
$$(p, q, r) = (p, xq', xr') = (xr', p, xq') = -(xr', xq', p)$$

Na igualdade mostrada no Corolário 1.2.3, façamos as seguintes substituições:

$$y = xr'$$
, $a = q'$, $z = p$. Resulta então:

$$(y, xa, z) + (y, za, x) = -(y, x, a)z - (y, z, a)x$$

$$\Rightarrow -(y, xa, z) = (y, za, x) + (y, x, a)z + (y, z, a)x$$

$$\Rightarrow -(xr', xq', p) = (xr', pq', x) + (xr', x, q')p + (xr', p, q')x$$

Como o segundo membro da expressão acima é igual a (p, q, r), vamos determinar o grau dessa expressão, calculando o grau de cada parcela.

Ainda pelo Corolário 1.2.3, temos: (y, xa, x) = -(y, x, a)x. Daí, fazendo na primeira parcela as substituições indicadas:

$$(xr', pq', x) = -(pq', xr', x) = (pq', x, r')x$$

$$\partial(pq') = \partial p + \partial q' = 1 + (-1 + \partial q) = \partial q$$

$$\partial x = 1$$
 $\partial r' = -1 + \partial r$

Assim:
$$\partial (pq') + \partial x + \partial r' = \partial q + 1 - 1 + \partial r = \partial q + \partial r < n$$

Logo:
$$(pq', x, r') = 0$$
 e também $(pq', x, r')x = 0$

Para a segunda parcela temos:

$$(xr', x, q')p = -(xr', q', x)p = (q', xr', x)p = (q', x, r')xp$$

$$\partial q' = -1 + \partial q$$
 $\partial x = 1$ $\partial r' = -1 + \partial r$

Daí
$$\partial q' + \partial x + \partial r' = -1 + \partial q + 1 - 1 + \partial r = \partial q + \partial r - 1 < n$$

Logo:
$$(q', x, r') = 0$$
 e também $(q', x, r')xp = 0$

Agora, a terceira parcela: (xr', p, q')x Calculamos:

$$\partial(xr') = \partial r$$
 $\partial x = 1$ $\partial q' = -1 + \partial q$

Então
$$\partial(xr') + \partial p + \partial q' = \partial r + 1 - 1 + \partial q = \partial p + \partial q < n$$

Logo:
$$(xr', p, q')x = 0$$

Como cada parcela se anula, temos que: (p, q, r) = 0

(2) $\partial q > 1$ ou $\partial r > 1$

Se apenas um dos produtos q ou r tem grau > 1, digamos $\partial q > 1$, q = xq', temos, novamente pelo Corolário 1.2.3:

$$(p,q,r)=(p,xq',x)=(p,x,q')x=0$$
 pelo mesmo argumento usado acima.

(3)
$$\partial q = \partial r = 1$$

Se
$$\partial q = \partial r = 1$$
, pela lei alternativa à direita temos: $(p,q,r) = (p,x,x) = 0$

O próximo resultado irá estabelecer uma importante relação entre as álgebras nilpotentes e as nilálgebras. Pelas definições concluímos que toda álgebra nilpotente é uma nilálgebra. De fato, se A é nilpotente, então existe $n \in \mathbb{N}$ tal que $A^{(n)} = 0$. Então, para todo $x \in A$, tem-se $x^n = 0$, o que significa que x é nilpotente. Portanto A é uma nilálgebra.

A recíproca pode não ser, necessariamente, verdadeira. Mas em dimensão finita, se A é nilálgebra, então A é nilpotente. Vamos primeiro demonstrar este fato no caso associativo. Para álgebras alternativas precisaremos antes conceituar álgebra de multiplicação M(A) de uma álgebra alternativa A, e em seguida demonstrar um lema pertinente a tais álgebras.

Os operadores R_a e L_a , há pouco definidos são evidentemente lineares e, podemos considerar os conjuntos:

- R(A) de todos os operadores multiplicativos à direita de A;
- L(A) de todos os operadores multiplicativos à esquerda de A;

 ${f B}$ de todos os operadores lineares sobre A.

Claramente **B** é uma álgebra sobre F. Os conjuntos R(A) e L(A) são subespaços da álgebra associativa **B**, uma vez que R_a e L_a são transformações lineares.

Definição 1.2.2. Chama-se álgebra envolvente das multiplicações à direita e à esquerda de A, denotada por M(A) (ou simplesmente M), a subálgebra de B gerada pela reunião dos operadores multiplicativos à direita e à esquerda de A.

M é a intersecção de todas as subálgebras de \mathbf{B} que contêm R(A) e L(A). Os elementos de M são da forma $\sum S_{a_1} \dots S_{a_n}$ onde S_{a_i} é igual a R_{a_i} ou L_{a_i} .

Seja $B \subset A$, qualquer subconjunto. Consideremos a álgebra envolvente de todos os operadores multiplicativos à direita e à esquerda de A, definidos por elementos de B, que será denotada por B^* .

Note que, se A é uma álgebra e $B \subseteq A$, então, na notação acima introduzida temse: $A^* = M(A)$, mas se B é uma subálgebra própria de A, então $B^* \neq M(B)$. De fato, B^* é gerada por operadores R_{b_i}, L_{b_j} , com $b_i, b_j \in B$, calculados em elementos de A. Já M(B) compõe-se dos mesmos operadores de B^* , porém calculados em elementos de B.

Lema 1.2.5. Um ideal B de uma álgebra A é nilpotente se e somente se a subálgebra B^* de M(A) é nilpotente.

Demonstração: (\Rightarrow) Seja B ideal nilpotente de A, com índice de nilpotência n. Sejam $T_1, \ldots, T_n \in B^*$. Cada T_i pode ser escrito $T_i = f_i(S_{b_1}, \ldots, S_{b_n})$, $b_i \in B$, $i = 1, \ldots n$. Consideremos o produto: $T = T_1 \ldots T_n = f_1 \ldots f_n(S_{b_1}, \ldots, S_{b_n})$. Se cada T_i for um polinômio a apenas uma indeterminada (S_{b_i}) , T será uma soma de produtos onde cada termo tem pelo menos n operadores lineares $S_{b_i} = R_{b_i}$ ou L_{b_i} . Ao calcularmos T(x), $x \in A$, como B é ideal de A, teremos $T(x) \in B$. Logo, T(x) será uma soma em que cada parcela é o produto de pelo menos n+1 elementos. Mas qualquer produto de n ou mais elementos em B é nulo, pois B é nilpotente de índice n. Assim, T(x) = 0, para todo $x \in A$, ou seja, T = 0. Portanto B^* é nilpotente.

(\Leftarrow) Seja B subálgebra de A. Vamos verificar que qualquer produto de pelo menos 2^t elementos de B pode ser escrito como $S_1 \dots S_n(b), \ S_i \in B^*, \ b \in B$. Faremos indução em t.

Para t = 1, é fácil ver que o produto de 2 elementos de B pode ser escrito $S_{b_1}(b)$. De fato, $bb_1 = bR_{b_1}$ e $b_1b = bL_{b_1}$. Seja agora um produto de mais de 2 elementos. Podemos considerar a última multiplicação a ser feita: bc, onde c é o resultado da multiplicação dos primeiros elementos. Como ilustração, se tivermos o produto: $b_1(b_2(b_1b_3))$, fazemos $b = b_1$ e $c = b_2(b_1b_3)$.

Nossa hipótese de indução será: O produto de pelo menos 2^t elementos de B é da forma $bS_1 \dots S_t$, com $S_i \in B^*$, $b \in B$. Calculemos o produto de pelo menos 2^{t+1} elementos de B. Novamente teremos uma última multiplicação a ser feita, envolvendo dois fatores: um deles é o produto de pelo menos 2^t elementos de B e o outro é $c \in B$. Assim, pela hipótese de indução podemos escrever:

$$c(bS_1 \dots S_t) = bS_1 \dots S_t L_c = bS_1 \dots S_{t+1}$$

ou
$$(bS_1 ... S_t)c = bS_1 ... S_t R_c = bS_1 ... S_{t+1}$$

Assim, se t é o índice de nilpotência de B^* , qualquer produto de 2^t elementos de B será zero. Portanto B é nilpotente.

Lema 1.2.6. Seja $A \neq 0$ uma álgebra associativa de dimensão finita e $a \in A$. Então: Aa = A se e somente se $xa \neq 0$, para todo $x \neq 0$, $x \in A$.

Demonstração: (\Rightarrow) Seja $A = \langle u_1, \ldots, u_n \rangle$, onde $\{u_1, \ldots, u_n\}$ é uma base de A. Assim, $\{u_1a, \ldots, u_na\}$ é uma base de Aa. Seja $x \in A$ tal que xa = 0. Podemos escrever: $x = \sum_{i=1}^{n} \alpha_i x_i$, logo $0 = xa = \sum_{i=1}^{n} \alpha_i x_i a$, e daí, $\alpha_i = 0$, para todo i. Portanto x = 0.

(\Leftarrow) Basta mostrar que dim $Aa = \dim A = n$, isto \acute{e} , $\{u_1a, \ldots, u_na\}$ \acute{e} l.i. Seja dim A = n com $\{u_1, \ldots, u_n\}$ uma base de A. Claramente $\{u_1a, \ldots, u_na\}$ gera Aa. Sejam $\alpha_1, \ldots, \alpha_n \in F$ tais que $\alpha_1u_1a + \cdots + \alpha_nu_na = 0$. Então $(\alpha_1u_1 + \cdots + \alpha_nu_n)a = 0$ logo $\alpha_1u_1 + \cdots + \alpha_nu_n = 0$, por hipótese. Mas como $\{u_1, \ldots, u_n\}$ \acute{e} base de A, segue que $\alpha_i = 0$ e $\{u_1a, \ldots, u_na\}$ \acute{e} l.i. como queríamos.

Lema 1.2.7 (Albert). Qualquer nilálgebra associativa de dimensão finita sobre F é nilpotente.

Demonstração: Seja A uma nilálgebra associativa de dimensão finita. Faremos indução na dimensão de A. Seja $n = \dim A$. Se n = 1, $A = \langle u \rangle$, para algum

 $u \in A$. Assim, qualquer elemento $x \in A$ pode ser escrito $x = \alpha_1 u$, $\alpha_1 \in F$. Mas, pela tábua de multiplicação de A, existe $\alpha \in F$ tal que $u^2 = \alpha u$. Daí: $x, y \in A \Rightarrow x = \alpha_1 u$, $y = \alpha_2 u \Rightarrow xy = \alpha_1 u \alpha_2 u = \alpha_1 \alpha_2 u^2 = \alpha_1 \alpha_2 \alpha u$. Podemos ter dois casos:

- (1) $\alpha = 0$. Teremos $xy = 0, \ \forall \ x, y \in A$. Neste caso A é uma zero álgebra;
- (2) $\alpha \neq 0$. Temos $(\alpha^{-1}u)^2 = (\alpha^{-1})^2u^2 = \alpha^{-1}u$. Fazendo $\alpha^{-1}u = e$, temos que $e^2 = e \neq 0$, o que é uma contradição, pois A é uma nilálgebra. Logo A é uma zero álgebra, isto é, A é nilpotente de índice 2.

Supondo que a tese é válida para dim A < n, então todo ideal próprio I de A é nilpotente, uma vez que dim $I < \dim A = n$. Seja $a \in A$. Se Aa = 0, então xa = 0, $\forall x \in A$. Logo A é uma zero álgebra e, portanto, nilpotente. Excluído este caso, se for Aa = A, então, pelo lema anterior, $xa \neq 0$, $\forall x \in A$, $x \neq 0$. Em particular, $a^2 \neq 0$, logo $a^n \neq 0$, $\forall n$. Contradição, pois A é nilálgebra. Assim, Aa é um ideal próprio de A. Seja a0 indice de nilpotência de a0. Então a0 indice de nilpotência de a0. Então a0 indice de a1 indice de nilpotência de a3 é nilpotente. Mas a4 é nilpotente. a5 indice de nilpotente.

Lema 1.2.8. Sejam A uma álgebra alternativa e $x, y \in A$ elementos quaisquer. São válidas as seguintes igualdades dos operadores R_a e L_a :

$$R_x R_y - R_{xy} = L_{xy} - L_y L_x = L_y R_x - R_x L_y$$
$$= L_x L_y - L_{yx} = R_y L_x - L_x R_y$$
$$= R_{yx} - R_y R_x$$

Demonstração: Seja $z \in A$. Calculemos cada uma das expressões acima em z, e façamos a subtração membro a membro, usando as propriedades usuais dos operadores lineares:

$$z(R_x R_y - R_{xy}) - z(L_{xy} - L_y L_x) = zR_x R_y - zR_{xy} - zL_{xy} + zL_y L_x$$

$$= (zx)R_y - z(xy) - (xy)z + (yz)L_x$$

$$= (zx)y - z(xy) - (xy)z + x(yz)$$

$$= (z, x, y) - (x, y, z) = 0$$

$$\begin{split} z(L_{xy}-L_yL_x)-z(L_yR_x-R_xL_y) &= zL_{xy}-zL_yL_x-zL_yR_x-zR_xL_y\\ &= (xy)z-(yz)L_x-(yz)R_x-(zx)L_y\\ &= (xy)z-x(yz)-(yz)x-y(zx)\\ &= (xy,z)-(y,z,x)=0 \end{split}$$

$$z(L_yR_x-R_xL_y)-z(L_xL_y-L_yx) &= zL_yR_x-zR_xL_y-zL_xL_y+zL_yx\\ &= (yz)R_x-(zx)L_y-(xz)L_y+(yx)z\\ &= (yz)x-y(zx)-y(xz)+(yx)z\\ &= (yz)x-y(zx)-y(xz)+(yx)z\\ &= (y,z,x)+(y,x,z)=0 \end{split}$$

$$z(L_xL_y-L_yx)-z(R_yL_x-L_xR_y) &= zL_xL_y-zL_yx-zR_yL_x+zL_xR_y\\ &= (xz)L_y-(yx)z-(zy)L_x-(xz)R_y\\ &= y(xz)-(yx)z-x(zy)+(xz)y\\ &= -(y,x,z)+(x,z,y)=0 \end{split}$$

$$z(R_yL_x-L_xR_y)-z(R_yx-R_yR_x) &= zR_yL_x-zL_xR_y-zR_{yx}+zR_yR_x\\ &= (zy)L_x-(xz)R_y-x(yx)+(zy)R_x\\ &= x(zy)-(xz)y-z(yx)+(zy)x \end{split}$$

Teorema 1.2.9. Qualquer nilálgebra alternativa de dimensão finita sobre F é nilpotente.

= -(x, z, y) + (z, y, x) = 0

Demonstração: Seja B uma subálgebra própria de A, maximal em relação à propriedade que B^* é nilpotente. O Teorema 1.2.4 (Artin) garante a existência de tal álgebra. Então existe $x \in A$ tal que $x \notin B$. Definimos o conjunto das imagens de x pelos operadores de B^* , por:

$$B^*x = \{G(x) \mid G \in B^*\}.$$

Temos: $B^*x \subseteq B$. De fato:

Como B^* é nilpotente, $B^{*r}=0$, para algum $r\in\mathbb{N}$. Então $AB^{*r}=0\subseteq B$.

Seja o conjunto $K=\{m\in\mathbb{N}\mid AB^{*^m}\subseteq B\}$. Tal conjunto não é vazio, pois $r\in K$. Sendo K um conjunto de números naturais não vazio, o $Princípio\ da\ Boa\ Ordem\ garante que\ K$ tem um mínimo $m\geq 1$.

Assim, existe $m \in \mathbb{N}$ tal que $AB^{*^m} \subseteq B$ e $AB^{*^{m-1}} \nsubseteq B$. Se m = 1, tome $x \in A \setminus B$. Se m > 1, tome $x \in AB^{*^{m-1}}$, $x \notin B$. Com isto, obtemos $B^*x \subseteq B$.

Seja C = B + F[x], onde F[x] indica polinômios em x com termo independente nulo. Claramente, C é uma subálgebra de A, com $B \subset C$. Consideremos a sua álgebra envolvente $C^* = (B + F[x])^*$. Mostremos inicialmente que $(B + F[x])^* = (B + Fx)^*$.

Seja
$$c \in B + F[x]$$
. Então: $c = b + \sum_{j=1}^{n} \alpha_j x^j$, para algum n .

Se $S_c \in (B + F[x])^*$, então $S_c = L$ ou $S_c = R$, e escrevemos:

$$S_c = S_b + \sum_{j \neq 0} \alpha_j S_{x^j} = S_b + \sum_{j \neq 0} \alpha_j S_x^j \implies S_c \in (B + Fx)^*$$

$$\Rightarrow (B + F[x])^* \subseteq (B + Fx)^*.$$

Por outro lado, se $c \in B + Fx$, então $c = b + \alpha x$. Daí,

$$S_c \in (B + Fx)^* \Rightarrow S_c = S_b + \alpha S_x \Rightarrow S_c \in (B + F[x])^*.$$

 $\Rightarrow (B + Fx)^* \subseteq (B + F[x])^*.$ Portanto $(B + F[x])^* = (B + Fx)^*.$

Um elemento $T \in C^*$ pode ser escrito $T = \sum S_{c_1} \dots S_{c_k}$, onde $S_{c_i} = L_{c_i}$ ou $S_{c_i} = R_{c_i}$. Vamos procurar explicitar o elemento T em termos dos operadores de B^* e de $(Fx)^*$. Consideremos as igualdades indicadas no Lema 1.2.8, fazendo y = b, para qualquer $b \in B$. Levando em conta que $B^*x \subseteq B$, temos:

Usando a igualdade $R_x R_y - R_{xy} = R_{yx} - R_y R_x$, resulta

$$R_x R_b - R_{xb} = R_{bx} - R_b R_x \implies R_x R_b = R_{b'} + R_{b''} - R_b R_x.$$

Considerando
$$b_1 = b' + b''$$
, temos: $R_x R_b = R_{b_1} - R_b R_x$. (1)

Usando a igualdade $L_y R_x - R_x L_y = R_{yx} - R_y R_x$, vem

$$L_b R_x - R_x L_b = R_{bx} - R_b R_x \implies R_x L_b = L_b R_x + R_b R_x - R_{b2}.$$
 (2)

Da igualdade $R_y L_x - L_x R_y = L_{xy} - L_y L_x$, obtemos

$$R_b L_x - L_x R_b = L_{xb} - L_b L_x \implies L_x R_b = R_b L_x + L_b L_x - L_{b_3}.$$
 (3)

Usando, finalmente $L_xL_y - L_{yx} = L_{xy} - L_yL_x$, obtemos

$$L_x L_b - L_{bx} = L_{xb} - L_b L_x \implies L_x L_b = L_{b_1} - L_b L_x.$$
 (4)

Vemos assim que, em cada produto da multiplicação à direita e à esquerda em B^* e $(Fx)^*$, a multiplicação R_x ou L_x pode ser passada sistematicamente da esquerda para a direita de R_b ou L_b de modo que, embora possa mudar de sinal e introduzir novos termos, preserva o número de fatores de B^* , e não aumenta o número de fatores de $(Fx)^*$. Portanto, todo operador $T \in C^*$ pode ser escrito como combinação linear de termos da forma:

$$R_x^{j_1}, L_x^{j_2}, R_x^{j_3} L_x^{j_4}, B_1, B_2 R_x^{m_1}, B_3 L_x^{m_2}, B_4 R_x^{m_3} L_x^{m_4}$$
 (5)
 $B_i \in B^*, j_i > 1, m_i > 1$

Seja r o índice de nilpotência de B^* , isto é $B^{*r}=0$. E como A é nilálgebra o x que tomamos em A é nilpotente. Então existe $j\in\mathbb{N}$ tal que $x^j=0$.

Usando (1), (2), (3), (4) e (5), basta fazer $(T^r)^{2j-1} = T^{r(2j-1)}$ que teremos certamente $T^{r(2j-1)} = 0$, lembrando que R_x e L_x comutam.

Assim, todo elemento T da álgebra associativa de dimensão finita C^* é nilpotente. Logo, pelo Lema 1.2.7, C^* é nilpotente.

Mas B é maximal em relação à propriedade que B^* é nilpotente. Chegamos a esta contradição ao supormos B subálgebra própria de A. Devemos ter, então, B=A, donde A^* é nilpotente. Logo, pelo Lema 1.2.5, A é nilpotente.

Corolário 1.2.10. Seja A álgebra alternativa de dimensão finita e nilpotente à direita (esquerda). Então A é nilpotente.

Demonstração: Se A é nilpotente à direita (esquerda) então A é uma nilálgebra. De fato, para todo $x \in A$, $x^k = 0$ (k = 0), onde k é o índice de nilpotência de A. Logo A é uma nilálgebra. Portanto, pelo Teorema 1.2.9, A é nilpotente.

1.3 Decomposição de Peirce

O estudo das propriedades de uma álgebra fica facilitado se pudermos decompor esta álgebra em uma soma de álgebras mais convenientes. Uma das ferramentas mais importantes neste sentido é a decomposição de Peirce, que passamos a estudar.

Definição 1.3.1. Seja A uma álgebra alternativa. Um elemento $e \in A$ é chamado idempotente se $e \neq 0$, e $e^2 = e$.

O próximo lema, devido a Albert, juntamente com o Lema 1.2.6, permitem garantir a existência de idempotentes numa álgebra associativa de dimensão finita.

Lema 1.3.1 (Albert). Toda álgebra associativa de dimensão finita que não é uma nilálgebra possui um idempotente.

Demonstração: É imediato para álgebras de dimensão 1. Fazemos indução em $n = \dim A$. Supondo válido se dim A < n, seja $Aa \subseteq A$, subálgebra, para algum $a \in A$. Pela hipótese de indução, Aa possui um idempotente se Aa for um ideal próprio de A e o resultado está mostrado. Se Aa = A, pelo Lema 1.2.6, $xa = 0 \Rightarrow x = 0$. Em particular, a = ea para algum $e \in A$. Logo $ea = e^2a \Rightarrow (e^2 - e)a = 0 \Rightarrow e^2 - e = 0 \Rightarrow e^2 = e$. Portanto $e \in A$ é idempotente.

Os dois próximos lemas garantem a existência de idempotentes numa álgebra de potências associativas e numa álgebra alternativa, respectivamente.

Lema 1.3.2. Toda álgebra A de potências associativas e de dimensão finita que não é uma nilálgebra, contém um idempotente e.

Demonstração: Como A não é uma nilálgebra, existe $x \in A$ que não é nilpotente. Pelo Teorema 1.2.4 (Artin), a subálgebra A(x) de A é uma álgebra associativa de dimensão finita (pois dim $A < \infty$), que não é uma nilálgebra ($x \in A(x)$ e x não é nilpotente). Logo, pelo Lema 1.3.1 (Albert), A(x) contém um idempotente. \Box

Lema 1.3.3. Toda álgebra alternativa A de dimensão finita que não é uma nilálgebra, contém um idempotente e.

Demonstração: É fácil ver que toda álgebra alternativa é de potências associativas. Logo, pelo lema anterior, toda álgebra alternativa de dimensão finita que não é uma nilálgebra possui um idempotente. □

Seja A uma álgebra alternativa, e $e \in A$ um idempotente. A pode ser decomposta numa soma direta de subespaços vetoriais:

$$A = A_{11} \oplus A_{10} \oplus A_{01} \oplus A_{00}$$
, onde
 $A_{ij} = \{x_{ij} \mid ex_{ij} = ix_{ij}, x_{ij}e = jx_{ij}\}$ $i, j = 0, 1$

A seguinte decomposição de um elemento x qualquer de uma álgebra alternativa A em relação a um idempotente e é bastante útil:

$$x = \underbrace{exe}_{(1)} + \underbrace{(ex - exe)}_{(2)} + \underbrace{(xe - exe)}_{(3)} + \underbrace{(x - ex - xe + exe)}_{(4)}$$

Mostremos que cada uma das parcelas indicadas está em um dos subespaços A_{ij} da decomposição de Peirce.

(1) $exe \in A_{11}$.

De fato, usando as propriedades usuais das álgebras alternativas, temos:

$$e(exe) = -(e, e, xe) + e^{2}(xe) = 0 + e(xe) = exe = 1exe$$

 $(exe)e = (ex, e, e) + (ex)e^{2} = 0 + exe = exe = 1exe$

(2) $(ex - exe) \in A_{10}$.

Seja y = ex - exe. Mostremos que ey = y e que ye = 0:

$$ey = e(ex - exe) = e(ex) - e(exe) = ex - exe = y$$

 $ye = (ex - exe)e = exe - (exe)e = exe - exe^2 = exe - exe = 0$

(3) $(xe - exe) \in A_{01}$.

Fazendo
$$y = xe - exe$$
, mostremos que $ey = 0$ e que $ye = y$:
 $ey = e(xe - exe) = exe - e(exe) = exe - e^2xe = exe - exe = 0$
 $ye = (xe - exe)e = (xe)e - (exe)e = xe^2 - exe^2 = xe - exe = y$

(4) $(x - ex - xe + exe) \in A_{00}$

Basta mostrar que ey = ye = 0, onde y = x - ex - xe + exe

$$ey = e(x - ex - xe + exe) = ex - e(ex) - e(xe) + e(exe)$$
$$= ex - e^2x - exe + e^2xe$$
$$= ex - ex - exe + exe = 0$$

Definição 1.3.2. Em uma álgebra alternativa A, os idempotentes e_1, e_2, \ldots, e_t são chamados **dois a dois ortogonais** se $e_i e_j = 0$, $i \neq j$.

Lema 1.3.4. Em uma álgebra alternativa A, com e_1, e_2, \ldots, e_t idempotentes dois a dois ortogonais, tem-se:

(i)
$$e = e_1 + e_2 + \cdots + e_t \ \acute{e} \ um \ idempotente$$

(ii)
$$ee_i = e_i e = e_i$$
, $\forall i$

(iii)
$$(x, e_i, e_j) = (x, e_i, e) = 0, \forall x \in A$$

Demonstração:

(i) Calculemos $e^2 = (e_1 + e_2 + \dots + e_t)(e_1 + e_2 + \dots + e_t) = e_1^2 + \dots + e_t^2 + \sum_{i \neq j} e_i e_j$ Como os e_i são idempotentes, $e_i e_j = 0$ se $i \neq j$. Resulta então: $e^2 = e_1^2 + \dots + e_t^2 = e_1 + e_2 + \dots + e_t = e$

(ii)
$$ee_i = (e_1 + e_2 + \dots + e_t)e_i = e_i^2 = e_i, \forall i$$

(iii) Se i = j resulta imediatamente que $(x, e_i, e_i) = 0$. Seja $i \neq j$:

$$(x, e_1, e_j) = (xe_i)e_j - x(e_ie_j) = (xe_i)e_j$$
, pois $e_ie_j = 0$.
 $(xe_i)e_j = (xe_i)e_j^2 = (x, e_i, e_j)e_j = -(x, e_j, e_i)e_j = -((xe_j)e_i)e_j$

$$\stackrel{(*)}{=} -x(e_je_ie_j) = 0$$

(*) Moufang, identidade (iii)

Definição 1.3.3. Um idempotente e de uma álgebra A é chamado **primitivo** se não existem idempotentes ortogonais u e v em A tais que e = u + v.

Lema 1.3.5. Em uma álgebra A de dimensão finita, qualquer idempotente e pode ser escrito como $e = e_1 + \cdots + e_t$, com e_i $(i = 1, \ldots, t)$ idempotentes primitivos dois a dois ortogonais.

Demonstração: Se e é primitivo nada temos a mostrar. Se e não é primitivo, existem u e v tais que e = u + v. Se u e v forem primitivos, está demonstrado. Caso contrário, teremos $e = u_1 + \cdots + u_r$. Os idempotentes u_i geram um subespaço de dimensão r, que é uma subálgebra associativa e comutativa, com $r \leq \dim A$. Se ainda algum u_i não for primitivo, podemos decompô-lo em uma soma. Como A tem dimensão finita, o processo deve se encerrar e chegamos a $e = e_1 + \cdots + e_t$, com os e_i idempotentes primitivos dois a dois ortogonais.

Pode-se obter uma decomposição de Peirce mais refinada considerando-se os idempotentes dois a dois ortogonais e_1, \ldots, e_t . Tal decomposição é dada por:

$$A = \sum_{i,j} A_{ij} \qquad i, j = 0, 1, \dots t$$

onde, usando o δ de Kronecker, definimos:

$$A_{ij} = \{ x_{ij} \mid e_k x_{ij} = \delta_{ki} x_{ij}, \quad x_{ij} e_k = \delta_{jk} x_{ij}, \quad k = 0, 1, \dots, t \}$$
$$i, j = 0, 1, \dots t$$

Apresentamos a seguir uma série de propriedades da decomposição de Peirce, as quais terão grande utilidade no próximo capítulo quando trataremos do radical de uma álgebra.

Proposição 1.3.6 (Existência e Unicidade da Decomposição de Peirce). Seja A uma álgebra alternativa, e e_1, \ldots, e_t idempotentes dois a dois ortogonais. Então: $A = \sum_{i,j} A_{ij}, \quad i, j = 0, 1, \ldots, t, \quad onde$:

$$A_{ij} = \{x_{ij} \mid e_k x_{ij} = \delta_{ki} x_{ij}, x_{ij} e_k = \delta_{jk} x_{ij}, k = 0, 1, \dots, t\}$$

 $i, j = 0, 1, \dots t.$

Tal decomposição é única.

Demonstração: Seja $x \in \sum A_{ij}$, então $x = \sum_{k,l=0}^{t} x_{kl}$

Comecemos calculando $e_i x e_j$, para $i = 1, \ldots, t$.

$$e_i x e_j = e_i \left(\sum_{k,l=0}^t x_{kl} \right) e_j = \sum_{k,l=0}^t e_i x_{kl} e_j = \sum_{kl}^t \delta_{ik} x_{kl} e_j = \sum_{kl}^t \delta_{ik} \delta_{lj} x_{kl} = x_{ij}$$

Observação: Podemos escrever e_ixe_j , pois $(e_ix)e_j=e_i(xe_j)$, já que $(x,e_i,e_j)=0$, conforme Lema 1.3.4.

Encontramos, então:

$$e_i x e_i = x_{ij}$$

Calculemos agora $e_i x$ e $e_i x e$, para $i = 1, \dots, t$.

$$e_i x = e_i \sum_{k,l=0}^{t} x_{kl} = \sum_{k,l=0}^{t} e_i x_{kl} = \sum_{k,l=0}^{t} \delta_{ik} x_{kl} = \sum_{l=0}^{t} x_{il}$$

$$e_i x e = e_i x \sum_{k=1}^t e_k = \sum_{l=0}^t x_{il} \sum_{k=1}^t e_k = \sum_{l=0}^t \sum_{k=1}^t x_{il} e_k = \sum_{l=0}^t \sum_{k=1}^t \delta_{lk} x_{il} = \sum_{l=1}^t x_{il}$$

Observação: Note que este último somatório começa mesmo em l=1, pois para $l=0,\ \delta_{0k}=0$, para todo $k=1,\ldots,t$.

Podemos escrever, então:

$$e_i x - e_i x e = x_{i0}$$

De maneira análoga, calculando xe_j , e exe_j , obtemos:

$$xe_{j} = \left(\sum_{k,l=0}^{t} x_{kl}\right) e_{j} = \sum_{k,l=0}^{t} x_{kl} e_{j} = \sum_{k,l=0}^{t} \delta_{lj} x_{kl} = \sum_{k=0}^{t} \sum_{l=0}^{t} \delta_{lj} x_{kl}$$

$$= \sum_{k=0}^{t} \left(\delta_{0j} x_{k0} + \delta_{1j} x_{k1} + \dots + \delta_{jj} x_{kj} + \dots + \delta_{lj} x_{kl}\right)$$

$$= \sum_{k=0}^{t} \delta_{jj} x_{kj} = \sum_{k=0}^{t} x_{kj}$$

$$exe_{j} = \left(\sum_{l=1}^{t} e_{l}\right) \left(\sum_{k=0}^{t} x_{kj}\right) = \sum_{l=1}^{t} e_{l} \sum_{k=0}^{t} e_{l} x_{kj} = \sum_{l=1}^{t} e_{l} \sum_{k=0}^{t} \delta_{lk} x_{kj}$$

$$= \sum_{k=0}^{t} \sum_{l=1}^{t} \delta_{lk} x_{kj} = \sum_{k=0}^{t} \left(\delta_{1k} x_{kj} + \dots + \delta_{kk} x_{kj} + \dots + \delta_{kt} x_{kj}\right) = \sum_{k=1}^{t} x_{kj}$$

Temos assim:

$$xe_j - exe_j = x_{0j}$$

Falta encontrar uma expressão para x_{00} , que podemos escrever em função das parcelas já calculadas, como:

$$x_{00} = x - \sum_{i,j=1}^{t} x_{ij} - \sum_{i=1}^{t} x_{i0} - \sum_{j=1}^{t} x_{0j}$$

$$= x - \sum_{i,j=1}^{t} e_i x e_j - \sum_{i=1}^{t} (e_i x - e_i x e) - \sum_{j=1}^{t} (x e_j - e_j x e_j)$$

$$= x - e_j x e_j - (e_j x - e_j x e) - (e_j x - e_j x e) - (e_j x - e_j x e) - (e_j x - e_j x e)$$

Resulta, finalmente:

$$x_{00} = x - ex - xe + exe$$

Dado $x \in A$, então:

$$x = \sum_{i,j=1}^{t} x_{ij} + \sum_{i=1}^{t} x_{i0} + \sum_{j=1}^{t} x_{0j} + x_{00} \in \sum A_{ij}$$
, onde $x_{ij} = e_i x e_j$,

$$x_{i0}=e_ix-e_ixe, \quad x_{0j}=xe_j-exe_j \quad \text{e} \quad x_{00}=x-ex-xe+exe$$

Portanto: $A\subset\sum_{i,j=0}^tA_{ij}$. Como, claramente $\sum_{i,j=0}^tA_{ij}\subset A$, segue que: $A=\sum_{i,j=0}^tA_{ij}$. Mostremos que a decomposição é única. Vimos que:

$$x_{ij} = e_i x e_i, i, j = 1, \dots, t$$

donde $x = \sum x_{ij}$

Se houvesse outra decomposição: $x = \sum y_{ij}$, então:

$$y_{ij} = e_i x e_j = x_{ij}, i, j = 1, \dots, t$$

Analogamente para os outros casos.

Proposição 1.3.7 (Propriedades da Decomposição de Peirce). A decomposição de Peirce, conforme indicada na proposição acima, satisfaz as seguintes propriedades:

1.
$$A_{ij}A_{jk} \subseteq A_{ik}$$
 $(i, j, k = 0, 1, ..., t)$

2.
$$A_{ij}A_{ij} \subseteq A_{ji}$$
 $(i, j = 0, 1, ..., t)$

3.
$$A_{ij}A_{kl} = 0$$
 $j \neq k$, $(i,j) \neq (k,l)$ $(i,j,k,l=0,1,\ldots,t)$

4.
$$x_{ij}^2 = 0$$
 $\forall x_{ij} \in A_{ij} \ (i \neq j)$

5.
$$x_{ij}y_{ij} = -y_{ij}x_{ij}$$
 $\forall x_{ij}, y_{ij} \in A_{ij} \ (i \neq j)$

6.
$$(x_{ij}, y_{jk}, z_{ki}) = 0$$
 se $(i, j, k) \neq (i, i, i), \forall x_{ij} \in A_{ij}, y_{jk} \in A_{jk}, z_{ki} \in A_{ki}$

7.
$$(x_{ii}, y_{ij}z_{ji}, t_{ii}) = 0 \text{ se } i \neq j, \ \forall x_{ii}, t_{ii} \in A_{ii}, \ y_{ij} \in A_{ij}, \ z_{ji} \in A_{ji}$$

8.
$$(x_{ij}y_{ij})z_{ij} = (y_{ij}z_{ij})x_{ij} = (z_{ij}x_{ij})y_{ij} \text{ se } i \neq j, \ \forall x_{ij}, y_{ij}, z_{ij} \in A_{ij}$$

9.
$$x_{ij}(y_{ij}z_{jj}) = (x_{ij}z_{jj})y_{ij} = z_{jj}(x_{ij}y_{ij}) \text{ se } i \neq j, \ \forall x_{ij}, \ y_{ij} \in A_{ij}, \ z_{jj} \in A_{jj}$$

10.
$$x_{ij}(z_{ii}y_{ij}) = (z_{ii}x_{ij})y_{ij} = (x_{ij}y_{ij})z_{ii} \text{ se } i \neq j, \ \forall \ x_{ij}, \ y_{ij} \in A_{ij}, \ z_{ii} \in A_{ii}$$

11.
$$(x_{ii}a)^m = (x_{ii}a_{ii})^{m-1} \sum_{k=0}^t x_{ii}a_{ik}$$

12.
$$(x_{ij}a)^m = (x_{ij}a_{ji})^{m-1} \sum_{k=0}^t x_{ij}a_{jk} + (x_{ij}a_{ji})(x_{ij}a_{ji})^{m-1}$$
, se $i \neq j$

13.
$$e_i(x_{ij}a)^m e_i = (x_{ij}a_{ji})^m (i, j = 0, 1, ..., t)$$

Demonstração: Omitiremos algumas demonstrações, já que os procedimentos são análogos para todas as propriedades.

1.
$$A_{ij}A_{jk} \subseteq A_{ik}$$
 $(i, j, k = 0, 1, ..., t)$

Seja $z \in A_{ij}A_{jk}$, isto é, $z = x_{ij}y_{jk}$. Calculemos e_lz e ze_l :

$$e_{l}z = e_{l}(x_{ij}y_{jk}) = -(e_{l}, x_{ij}, y_{jk}) + (e_{l}x_{ij})y_{jk} = (x_{ij}, e_{j}, y_{jk}) + \delta_{li}x_{ij}y_{jk}$$

$$= (x_{ij}e_{l})y_{jk} - x_{ij}(e_{l}y_{jk}) + \delta_{li}x_{ij}y_{jk} = \delta_{jl}y_{jk} - \delta_{lj}x_{ij}y_{jk} + \delta_{li}x_{ij}y_{jk}$$

$$= \delta_{li}x_{ij}y_{jk} = \delta_{li}z$$

$$ze_{l} = (x_{ij}y_{jk}e_{l} = (x_{ij}, y_{jk}, e_{l}) + x_{ij}(y_{jk}e_{l} = -(x_{ij}, e_{l}, y_{jk}) + \delta_{kl}x_{ij}y_{jk})$$

$$= (x_{ij}(e_{l}y_{jk}) - (x_{ij}e_{l})y_{jk} + \delta_{kl}x_{ij}y_{jk} = \delta_{lj}x_{ij}y_{jk} - \delta_{jl}x_{ij}y_{jk} + \delta_{kl}x_{ij}y_{jk})$$

$$= \delta_{kl}x_{ij}y_{ik} = \delta_{kl}z$$

$$\Rightarrow z \in A_{ik}$$

3.
$$A_{ij}A_{kl} = 0$$
 $j \neq k$, $(i,j) \neq (k,l)$ $(i,j,k,l=0,1,\ldots,t)$

Sejam $x_{ij} \in A_{ij}$ e $y_{kl} \in A_{kl}$. Basta mostrar que $x_{ij}y_{kl} = 0$. Devemos considerar 3 casos:

(i)
$$l, k \neq 0$$
, $l \neq k$, $l \neq j$

Pelo Corolário 1.2.3, temos:

$$(y, xa, z) + (y, za, x) = -(y, x, a)z - (y, z, a)x$$
 (I)

Expandindo os associadores de (I):

$$(y(xa))z - y((xa)z) + (y(za))x - y((za)x) = (y(xa) - (yx)a)z + (y(za) - (yz)a)x$$

$$= (y(xa))z - ((yx)a)z + (y(za))x - ((yz)a)x$$

$$\Rightarrow y((xa)z) + y((za)x) = ((yx)a)z + ((yz)a)x$$
(II)

Fazendo em (II) as seguintes substituições: $y=x_{ij}, x=e_k, a=y_{kl}$ e $z=e_l$ obtemos:

$$\underbrace{x_{ij}(e_k y_{kl} e_l)}_{(1)} + \underbrace{x_{ij}(e_l y_{kl} e_k)}_{(2)} = \underbrace{((x_{ij} e_k) y_{kl}) e_l}_{(3)} + \underbrace{((x_{ij} e_l) y_{kl}) e_k}_{(4)}$$
(III)

$$(1) \rightarrow x_{ij}(e_k y_{kl}e_l) = x_{ij}(e_k y_{kl})e_l = x_{ij}(\delta_{kk} y_{kl}e_l) = x_{ij}(\delta_{kk}\delta_{ll}y_{kl}) = x_{ij}y_{kl}$$

$$(2) \rightarrow x_{ij}(e_l y_{kl} e_k) = x_{ij}(e_l y_{kl}) e_k = \delta_{lk} y_{kl} e_k = 0$$

$$(3) \rightarrow ((x_{ij}e_k)y_{kl})e_l = (\delta_{jk}x_{ij}y_{kl})e_l = 0$$

$$(4) \rightarrow ((x_{ij}e_l)y_{kl})e_k = (\delta_{il}x_{ij}y_{kl})e_k = 0$$

Portanto $x_{ij}y_{kl}=0$.

(ii)
$$l \neq k$$
, $l = j$

A expressão (III) se reduz a:

$$x_{ij}y_{kj} = (\delta_{ll}x_{ij}y_{kj})e_k = (x_{ij}y_{kj})e_k = (x_{ij}, y_{kj}, e_k) + x_{ij}(y_{kj}e_k)$$

$$= (y_{kj}, e_k, x_{ij}) + \delta_{jk}x_{ij}y_{kl} = (y_{kj}, e_k, x_{ij})$$

$$= (y_{kj}e_kx_{ij} - y_{kj}(e_kx_{ij}) = \delta_{jk}y_{kj}x_{ij} - \delta_{ki}y_{kj}x_{ij} = 0$$

pois $\delta_{jk} = 0$, já que $j \neq k$. Também $\delta_{ki} = 0$, pois como l = j, devemos ter, necessariamente, $i \neq k$, pois $(i, j) \neq (k, l)$.

(iii)
$$l = k$$

Incluímos dois subcasos bem simples, e ficamos com:

(a)
$$j=l$$

$$x_{ij}y_{jj}+x_{ij}y_{jj}=(x_{ij}y_{jj})e_j \Rightarrow 2x_{ij}y_{jj}=x_{ij}y_{jj} \Rightarrow x_{ij}y_{jj}=0$$
 Usamos que, $x_{ij}y_{jj}e_j=z_{ij}e_j=\delta_{jj}z_{ij}=z_{ij}$, pois, pela propriedade 1, $x_{ij}y_{jj}\in A_{ij}$.

(b)
$$j \neq l$$

 $x_{ij}y_{ll} + x_{ij}y_{ll} = 0 \implies x_{ij}y_{ll} = 0$

4.
$$x_{ij}^2 = 0$$
 $\forall x_{ij} \in A_{ij} \ (i \neq j)$

Pela propriedade 2, $x_{ij}^2 \in A_{ji}$. Como $i \neq j \ (\Rightarrow i \neq 0 \text{ ou } j \neq 0)$, podemos supor $i \neq 0$. Então:

$$x_{ij}^2 = x_{ij}^2 e_i = (x_{ij}x_{ij})e_i = x_{ij}(x_{ij}e_i) = x_{ij}(\delta_{ji}x_{ij}) = 0$$

5.
$$x_{ij}y_{ij} = -y_{ij}x_{ij}$$
 $\forall x_{ij}, y_{ij} \in A_{ij} \ (i \neq j)$

$$0 = (x_{ij} + y_{ij})^2 = x_{ij}^2 + x_{ij}y_{ij} + y_{ij}x_{ij} + y_{ij}^2 \Rightarrow x_{ij}y_{ij} + y_{ij}x_{ij} = 0$$

$$\Rightarrow x_{ij}y_{ij} = -y_{ij}x_{ij}$$

6.
$$(x_{ij}, y_{jk}, z_{ki}) = 0$$
 se $(i, j, k) \neq (i, i, i), \forall x_{ij} \in A_{ij}, y_{jk} \in A_{jk}, z_{ki} \in A_{ki}$

$$(x_{ij}, y_{jk}, z_{ki}) = -(y_{jk}, x_{ij}, z_{ki}) = -\underbrace{(y_{jk}x_{ij}z_{ki})}_{(1)} + \underbrace{y_{jk}(x_{ij}z_{ki})}_{(2)}$$

(1) \rightarrow Se $k \neq i$, $y_{jk}x_{ij} = 0$, pela propriedade 3.

Se k=i, devemos ter $i\neq j$, logo $y_{jk}x_{ij}=y_{ji}x_{ij}\in A_{jj}$. Assim, $y_{jk}x_{ij}=w_{jj}$. Daí, $(y_{jk}x_{ij})z_{ki}=w_{jj}z_{ki}=0$, pela prop. 3, já que $i\neq j$ e $j\neq k$.

(2) \rightarrow Se $j \neq k$, $x_{ij}zki = 0$, pela propriedade 3.

Se j=k ambos devem ser $\neq i$, logo $x_{ij}z_{ki}=x_{ij}z_{ji}\in A_{ii}$, e $x_{ij}z_{ki}=w_{ii}$. Daí, $y_{jk}w_{ii}=y_{jj}w_{ii}=0$, pela prop. 3.

7. $(x_{ii}, y_{ij}z_{ji}, t_{ii}) = 0 \text{ se } i \neq j, \ \forall x_{ii}, t_{ii} \in A_{ii}, \ y_{ij} \in A_{ij}, \ z_{ji} \in A_{ji}$

$$(x_{ii}, y_{ij}z_{ji}, t_{ii}) = (x_{ii}(y_{ij}z_{ji}))t_{ii} - x_{ii}((y_{ij}z_{ji})t_{ii})$$

$$= (-(x_{ii}, y_{ij}, z_{ji}) + (x_{ii}y_{ij})z_{ji})t_{ii} - x_{ii}((y_{ij}, z_{ji}, t_{ii}) + y_{ij}(z_{ji}, t_{ii}))$$

Pela propriedade 6, $(x_{ii}, y_{ij}z_{ji}) = 0$ e $(y_{ij}, z_{ji}, t_{ii}) = 0$, logo:

$$(x_{ii}, y_{ij}z_{ji}, t_{ii}) = ((x_{ii}y_{ij})z_{ji})t_{ii} - x_{ii}(y_{ij}(z_{ji}t_{ii}))$$

$$= (x_{ii}y_{ij}, z_{ji}, t_{ii}) + (x_{ii}y_{ij})(z_{ji}t_{ii}) + (x_{ii}, y_{ij}, z_{ji}t_{ii}) - (x_{ii}y_{ij})(z_{ji}, t_{ii})$$

$$= (w_{ij}, z_{ji}, t_{ii}) + (x_{ii}, y_{ij}u_{ji}) = 0$$

Usei que: $x_{ii}y_{ij} \in A_{ij}$, logo $x_{ii}y_{ij} = w_{ij}$ e $z_{ji}t_{ii} \in A_{ji}$, logo $z_{ji}t_{ii} = u_{ji}$, de acordo com a propriedade 1.

Pela prop. 6, os dois associadores no final da igualdade acima são iguais a zero.

8.
$$(x_{ij}y_{ij})z_{ij} = (y_{ij}z_{ij})x_{ij} = (z_{ij}x_{ij})y_{ij} \text{ se } i \neq j, \ \forall x_{ij}, y_{ij}, z_{ij} \in A_{ij}$$

$$(x_{ij}y_{ij})z_{ij} = (x_{ij}, y_{ij}, z_{ij}) + x_{ij}(y_{ij}z_{ij}) = -(x_{ij}, z_{ij})y_{ij} + x_{ij}(y_{ij}z_{ij})$$

$$= x_{ij}(z_{ij}y_{ij}) - (x_{ij}z_{ij})y_{ij} + x_{ij}(y_{ij}z_{ij})$$

$$- x_{ij}(y_{ij}z_{ij}) + (z_{ij}x_{ij})y_{ij} + x_{ij}(y_{ij}z_{ij})$$

$$\Rightarrow (x_{ij}y_{ij})z_{ij} = (z_{ij}x_{ij})y_{ij}$$

A outra igualdade se demonstra de forma inteiramente análoga.

11.
$$(x_{ii}a)^m = (x_{ii}a_{ii})^{m-1} \sum_{k=0}^t x_{ii}a_{ik}$$

Demonstramos por indução em m.

Para m=1: $x_{ii}a=x_{ii}\sum_{j,k}x_{ii}a_{jk}=\sum_kx_{ii}a_{ik}$, pois $x_{ii}a_{jk}=0$ se $i\neq j$ pela prop. 3.

Supondo válido para m, calculamos:

$$(x_{ii}a)^{m+1} = (x_{ii}a)^m (x_{ii}a) = (x_{ii}a_{ii})^{m-1} \left(\sum_{k=0}^t x_{ii}a_{ik}\right) (x_{ii}a)$$

$$= (x_{ii}a_{ii})^{m-1} \sum_{k=0}^t (x_{ii}a_{ik}) (x_{ii}a)$$

$$= (x_{ii}a_{ii})^{m-1} \left(\sum_{k=0}^t (x_{ii}a_{ik}) \sum_{j=0}^t (x_{ii}a_{ij})\right)$$

$$= (x_{ii}a_{ii})^{m-1} \left(\sum_{k=0}^t \sum_{j=0}^t (x_{ii}a_{ik}) (x_{ii}a_{ij}) \sum_{(2)}^t (x_{ii}a_{ij})\right)$$

$$= (x_{ii}a_{ii})^{m-1} \sum_{j=0}^t (x_{ii}a_{ii}) (x_{ii}a_{ij}) = (x_{ii}a_{ii})^m \sum_{j=0}^t (x_{ii}a_{ij})$$

$$(1) \rightarrow x_{ii}a_{ik} \in A_{ik}, \quad e \quad (2) \rightarrow x_{ii}a_{ij} \in A_{ij} \quad \Rightarrow (x_{ii}a_{ik})(x_{ii}a_{ij}) = 0$$

se $k \neq i$, portanto o somatório em k se anula para todo $k \neq i$, ficando apenas o termo $x_{ii}a_{ii}$.

1.4 Álgebras Báricas

As álgebras báricas têm sua origem nos estudos da Genética, e são caracterizadas por uma função peso relacionada às características genéticas transmitidas entre os indivíduos. Nosso estudo aqui visa somente os aspectos algébricos desta aplicação, caracterizando suas estruturas fundamentais em termos dos conceitos usualmente encontrados em Álgebra, como homomorfismos, radical, semisimplicidade, etc. Consideraremos também somente álgebras de dimensão finita.

Definição 1.4.1. Uma álgebra A sobre um corpo F é chamada de **álgebra bárica** se admitir um homomorfismo de álgebras não trivial $w:A \to F$, chamado homo-

morfismo peso. Denotamos por (A, w). Para cada $x \in A$, w(x) será chamado de **peso** de x.

Dado $x \in A$ tal que $w(x) \neq 0$, então temos a seguinte decomposição para A:

$$A = Fx \oplus Ker(w)$$

De fato, sendo $w(x) \neq 0$, podemos escrever, para todo $a \in A$:

$$a = \frac{w(a)}{w(x)}x + \left(a - \frac{w(a)}{w(x)}x\right)$$

A primeira parcela está, evidentemente, em Fx. Quanto à segunda, temos:

$$w\left(a - \frac{w(a)}{w(x)}x\right) = w(a) - w\left(\frac{w(a)}{w(x)}x\right) = w(a) - \frac{w(a)}{w(x)}w(x) = w(a) - w(a) = 0$$

o que indica que $\left(a - \frac{w(a)}{w(x)}x\right) \in Ker(w)$. A soma é direta, pois tomando $\alpha x \in Fx$, se $\alpha x \in Ker(w)$, então $w(\alpha x) = 0$, logo $\alpha w(x) = 0$, e como $w(x) \neq 0$, segue que $\alpha = 0$, portanto $\alpha x = 0$.

Consideraremos as álgebras báricas alternativas de dimensão finita sobre um corpo F de característica $\neq 2$. Nosso principal objetivo nesta seção é mostrar que toda álgebra bárica alternativa possui um idempotente de peso 1. Vamos começar mostrando tal resultado para uma álgebra associativa. Para isto precisaremos dos três lemas seguintes.

Lema 1.4.1. Toda álgebra bárica associativa (A,w) possui um idempotente.

Demonstração: Como A é álgebra bárica, existe $x \in A$ tal que $w(x) \neq 0$. Então, x não é nilpotente, pois se fosse teríamos:

$$x^{n} = 0 \implies w(x^{n}) = 0 \implies (w(x))^{n} = 0 \implies w(x) = 0$$

uma contradição. Como existe $x \in A$ tal que x não é nilpotente, então A é uma álgebra associativa que não é uma nilálgebra. Logo, pelo Lema 1.2.6, A possui um idempotente. \Box

Definição 1.4.2. Seja (A, w) uma álgebra bárica. Chamamos de bar(A) ao conjunto $bar(A) = \{x \in A \mid w(x) = 0\}.$

Em vista da definição acima, se B é uma subálgebra de A e $B \nsubseteq bar(A)$, dizemos que B é uma subálgebra bárica de A. Neste caso dizemos que $(B, w \mid_B)$ é uma álgebra bárica. Em outras palavras, uma subálgebra bárica é aquela que possui pelo menos um elemento de peso não nulo.

Lema 1.4.2. Se (A, w) é uma álgebra bárica associativa $a \in A$, tal que w(a) = 1, então Aa é uma subálgebra bárica de A.

Demonstração: Sempre existe em uma álgebra bárica um elemento a de peso 1. Como sabemos, existe $x \in A$ tal que $w(x) \neq 0$. Seja $a = \frac{x}{w(x)}$. Então:

$$w(a) = w\left(\frac{x}{w(x)}\right) = w\left(\frac{1}{w(x)}x\right) = \frac{1}{w(x)}w(x) = 1$$

Mostremos que Aa é uma subálgebra de A. Tomando $b, c \in A$, temos $ba \in Aa$ e $ca \in Aa$. Daí, $(ba)(ca) = (bac)a \in Aa$. Logo, Aa é subálgebra. Para provar que Aa é uma subálgebra bárica de A, basta mostrar que existe $y \in Aa$ tal que $w(y) \neq 0$. Tomando $y = a^2 \in Aa$, temos: $w(a^2) = w(a)w(a) = 1$. Logo y é um elemento de peso 1 em Aa.

Lema 1.4.3. Se (A, w) é uma álgebra bárica associativa e, para algum $a \in A$, com w(a) = 1, tivermos Aa = A, então (A, w) possui um idempotente de peso 1.

Demonstração: Pelo Lema 1.2.6 podemos escrever: Aa = A se e somente se $xa \neq 0$, para todo $x \neq 0$, $x \in A$. Assim, xa = 0 se e somente se x = 0 (pois $a \neq 0$, uma vez que w(a) = 1). Por hipótese, Aa = A. Assim, $a \in A$ e também $a \in Aa$, logo a = ea para algum $e \in A$. Multiplicando ambos os membros por e:

$$ea = e^2 a \implies (e - e^2)a = 0 \implies e - e^2 = 0 \implies e = e^2.$$

Provamos assim que e é idempotente. Mas

$$1 = w(a) = w(ea) = w(e)w(a) = w(e)1 = w(e) \implies w(e) = 1.$$

Teorema 1.4.4. Toda álgebra bárica associativa (A, w) possui um idempotente de peso 1.

Demonstração: Seja $a \in A$ tal que w(a) = 1. Faremos indução em dim A. Se dim A = 1, então $A \cong Fa$, onde w(a) = 1. Pelo Lema 1.4.3, Fa possui um idempotente, isto é, $\exists \alpha \in F$, $\alpha \neq 0$ tal que αa é idempotente. Então

$$(\alpha a)^2 = \alpha a \implies \alpha^2 a^2 = \alpha a \implies \alpha a^2 = a \implies w(\alpha a^2) = w(a) = 1$$

$$\implies \alpha w(a^2) = 1 \implies \alpha w(a)w(a) = 1 \implies \alpha.1.1 = 1 \implies \alpha = 1.$$

Então $\alpha a=1.a=a$ é um idempotente de peso 1. Suponhamos agora, por hipótese de indução, que o teorema é válido se dim A< n. Seja dim A=n. Consideraremos dois casos:

Caso 1:
$$A = Aa$$

Podemos aplicar o Lema 1.3.3, uma vez que w(a)=1. Assim, A possui um idempotente de peso 1.

Caso 2:
$$A \neq Aa$$

Neste caso, dim $Aa < \dim A$, logo pela hipótese de indução, Aa possui um idempotente de peso 1. Mas $Aa \subseteq A$, logo, pelo Lema 1.4.2, Aa é uma subálgebra bárica de A. Portanto este mesmo idempotente de peso 1 de Aa é idempotente de peso 1 de A. Logo A possui um idempotente de peso 1.

Corolário 1.4.5. Se (A, w) é uma álgebra bárica de potências associativas, então A possui um idempotente de peso 1.

Demonstração: Seja $x \in A$ tal que w(x) = 1. A subálgebra B = A(x) é bárica e associativa. Logo B possui um idempotente de peso 1. Segue que A possui um idempotente de peso 1.

Corolário 1.4.6. Se (A, w) é uma álgebra bárica alternativa, então A possui um idempotente de peso 1.

Demonstração: Como A é alternativa, então A é de potências associativas (consequência do Teorema 1.2.4 (Artin)). Logo, pelo corolário anterior, A possui um idempotente de peso 1.

A seguir apresentamos uma caracterização para álgebras báricas alternativas em termos de elementos do bar(A).

Proposição 1.4.7. Seja (A, w) uma álgebra bárica com um idempotente e de peso 1. Então (A, w) é alternativa se e somente se, para quaisquer $u, v \in bar(A)$ são válidas as seguintes condições:

(i)
$$(e, e, u) = (u, e, e) = (e, u, e) = 0;$$

(ii)
$$(e, u, u) = (u, u, e) = (u, e, u) = 0;$$

(iii)
$$(u, u, v) = (v, u, u) = 0;$$

(iv)
$$(e, u, v) + (u, e, v) = 0$$
;

(v)
$$(v, e, u) + (v, u, e) = 0$$
.

Demonstração: Se A é alternativa, então as cinco condições acima são obviamente válidas. Precisamos provar apenas a recíproca. Seja então (A, w) álgebra bárica na qual são válidas as igualdades indicadas. Tomamos $x = \alpha e + u \in A$ e $y = \beta e + v \in A$, com $\alpha, \beta \in F$. Temos:

$$(x, x, y) = (\alpha e + u, \alpha e + u, \beta e + v)$$

$$= (\alpha e, \alpha e, \beta e) + (\alpha e, \alpha e, v) + (\alpha e, u, \beta e) + (\alpha e, u, v)$$

$$+ (u, \alpha e, \beta e) + (u, \alpha e, v) + (u, u, \beta e) + (u, u, v)$$

$$= \alpha^{2} \beta(e, e, e) + \alpha^{2}(e, e, v) + \alpha \beta(e, u, e) + \alpha(e, u, v)$$

$$+ \alpha \beta(u, e, e) + \alpha(u, e, v) + \beta(u, u, e) + (u, u, v) = 0$$

De maneira análoga provamos que (y, x, x) = 0, resultando que A é alternativa.

Capítulo 2

Radical e Semisimplicidade

Neste capítulo trabalharemos com o importante conceito de radical, aplicado às álgebras alternativas e alternativas báricas. Trata-se de um conceito intimamente relacionado à estrutura de uma álgebra. Portanto iremos retomar tais idéias para refiná-las um pouco mais e estabelecer uma caracterização do radical nestes termos, visando em seguida estudar alguns resultados envolvendo a semisimplicidade das álgebras alternativas e báricas.

2.1 O Radical

Voltemos a considerar as álgebras nilpotentes. Lembrando, uma álgebra A é chamada nilpotente se $A^{(n)}=0$, para algum $n\in\mathbb{N},\ n>1$.

Vamos verificar que toda álgebra A possui alguma subálgebra nilpotente. Em particular A possui um ideal nilpotente. Mais ainda, veremos que em toda álgebra existe um ideal nilpotente que contém todos os outros ideais nilpotentes da referida álgebra.

Proposição 2.1.1. Toda álgebra A de dimensão finita possui um único ideal nilpotente R que contém todo ideal nilpotente N de A.

Demonstração: Se o único ideal nilpotente de A é 0 o teorema está provado. Seja então R um ideal nilpotente não nulo tal que dim R seja máxima. Seja N um ideal nilpotente não nulo, $N \neq R$. Claro que $R \cap N$ também é um ideal nilpotente. Calculemos:

$$(R+N)^m = (R+N)^{m-1}(R+N)$$
, onde

 $m = max\{r, n\}, r =$ índice de nilpotência de R e n =índice de nilpotência de N.

Provaremos que: $(R+N)^m=R^m+f(R,N)+N^m$, onde f(X,Y) é um polinômio não associativo em X e Y. Faremos indução em m.

A expressão é válida para m=2, pois:

$$(R+N)^2 = (R+N)(R+N) = R^2 + RN + NR + N^2.$$

Supondo agora válida para m, calculemos:

$$(R+N)^{m+1} = (R+N)^m (R+N) = (R^m + f(R,N) + N^m)(R+N)$$
$$= R^{m+1} + R^m N + f(R,N)R + f(R,N)N + N^m R + N^{m+1}$$
$$= R^{m+1} + g(R,N) + N^{m+1}$$

onde $g(R,N) = R^m N + f(R,N) R + f(R,N) N + N^m R$ é um polinômio nas condições desejadas.

Sendo $m \ge r$ e $m \ge n$, conforme indicado acima, resulta que $(R+N)^m = g(R,N)$, e portanto, $(R+N)^m \subseteq R \cap N$, logo $(R+N)^m$ é nilpotente à direita.

Mostremos que R+N é nilpotente. De fato, se $(R+N)^m$ é nilpotente, existe $k \in \mathbb{N}$ tal que $((R+N)^m)^k = 0$. Assim, para todo $x \in (R+N)$, temos que $x^m \in (R+N)^m$, logo $(x^m)^k = 0 \implies x^{mk} = 0 \implies (R+N)$ é nilpotente à direita. Logo, pelo Corolário 1.2.10, (R+N) é nilpotente de índice mk.

Mas $\dim R \geq \dim (R+N),$ devido à maximalidade da dimR. Portanto $N \subseteq R.$ \Box

Definição 2.1.1. Seja A uma álgebra alternativa. Chama-se **radical** de A ao ideal nilpotente maximal de A. Notação: R(A).

Convém notar que, embora o radical seja nilpotente e portanto uma nilálgebra, ou seja, todos os seus elementos são nilpotentes, o radical não é igual ao conjunto de todos os elementos nilpotentes. Vejamos, através de um exemplo simples, que pode haver elementos nilpotentes não nulos que não pertençam ao radical.

Contra-exemplo

Na álgebra das matrizes reais $M_2(\mathbb{R})$, temos que $a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ é nilpotente de índice 2. Seja $z = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$. Então $az = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$ e $(az)^2 = \begin{bmatrix} c^2 & cd \\ 0 & 0 \end{bmatrix}$. Assim $(az)^r \neq 0$, se $c, d \neq 0$, para todo $r \in \mathbb{N}$.

Pode-se obter uma caracterização do radical usando o conceito de nilpotência, considerando-se uma noção levemente modificada deste conceito, conforme definição a seguir.

Definição 2.1.2. Seja A uma álgebra alternativa. Um elemento $z \in A$ é chamado **propriamente nilpotente** se za é nilpotente, para todo $a \in A$.

Lema 2.1.2. Seja A álgebra alternativa. Um elemento $z \in A$ é propriamente nilpotente se e somente se az é nilpotente, para todo $a \in A$.

Demonstração: (\Rightarrow) z é propriamente nilpotente, então za é nilpotente, logo $(za)^m = 0$ para algum m. Pelo Teorema 1.2.4 (Artin), a subálgebra gerada por quaisquer dois elementos de uma álgebra alternativa A é associativa. Então:

$$(az)^{m+1} = (az)(az)\dots(az) = a(za)\dots(za)z = a(za)^mz = a0z = 0$$

o que prova que az é nilpotente.

 (\Leftarrow) Analogamente, se az é nilpotente, temos:

$$(za)^{m+1} = (za)(za)\dots(za) = z(az)\dots(az)a = z(az)^mz = z0a = 0$$

provando que za é nilpotente. Portanto z é propriamente nilpotente.

Lema 2.1.3. Seja A álgebra alternativa. Se $z \in A$ é propriamente nilpotente então z é nilpotente.

Demonstração: Fazendo a=z, temos que: $za=zz=z^2$ é nilpotente. Então:

$$0 = (z^2)^r = z^2 \dots z^2 = z^{2r}$$

pois a subálgebra gerada por z^2 é de potências associativas (pois A é alternativa e, toda álgebra alternativa é de potências associativas, como conseqüência do Teorema 1.2.4 (Artin)).

Designaremos por \mathcal{B} o conjunto dos elementos propriamente nilpotentes de A.

Definição 2.1.3. Seja A uma álgebra. Um elemento $u \in A$ é chamado **unidade** de A se xu = ux = x, $\forall x \in A$. Neste caso dizemos que A é uma **álgebra com unidade**. Denotamos a unidade de A por 1.

Definição 2.1.4. Seja A uma álgebra com unidade. Dizemos que um elemento $x \in A$ tem **inverso**, denotado por x^{-1} , se $xx^{-1} = x^{-1}x = 1$. Dizemos também que o elemento x é **invertível**.

Lema 2.1.4. Seja A álgebra alternativa com unidade e $x \in A$ invertível. Então $(x, x^{-1}, y) = 0$, para todo $y \in A$.

Demonstração: A seguinte identidade

$$a(x, y, z) + (a, x, y)z = (ax, y, z) - (a, xy, z) + (a, x, yz)$$

é trivialmente verificada. Basta apenas desenvolver os associadores. Fazendo as seguintes substituições: $a=x^{-1},\ y=x,\ z=x^{-1}y,$ obtemos:

$$x^{-1}\overbrace{(x,x,x^{-1}y)}^{=0} + \overbrace{(x^{-1},x,x)}^{=0} x^{-1}y = (x^{-1}x,x,x^{-1}y) - (x^{-1},x^2,x^{-1}y) + (x^{-1},x,x(x^{-1}y))$$

$$+ (x^{-1},x,x(x^{-1}y))$$

$$\Rightarrow (x^{-1},x^2,x^{-1}y) - (x^{-1},x,x(x^{-1}y)) = 0$$

Desenvolvendo os associadores e aplicando a identidade (i) de Moufang (i) (Teorema 1.2.2), (xax)y = x(a(xy)), obtemos:

$$(x^{-1}x^{2})(x^{-1}y) - x^{-1}(x^{2}(x^{-1}y)) + (xx^{-1})(x(x^{-1}y)) - x(x^{-1}(x(x^{-1}y))) = 0$$

$$\Rightarrow (x^{-1}x^{2})(x^{-1}y) - (x^{-1}x^{2}x^{-1})y + x(x^{-1}y) - x((x^{-1}xx^{-1})y) = 0$$

$$\Rightarrow (x^{-1}x^{2})(x^{-1}y) - (x^{-1}x^{2}x^{-1})y + x(x^{-1}y) - x(x^{-1}y) = 0$$

$$\Rightarrow (x^{-1}x^{2})(x^{-1}y) - (x^{-1}x^{2}x^{-1})y = 0$$

Note que: $x^{-1}x^2 = x$. De fato:

$$0 = (x^{-1}, x, x) = (x^{-1}x)x - x^{-1}x^2 = x - x^{-1}x^2 \implies x^{-1}x^2 = x$$

A última igualdade obtida acima fica, portanto:

$$x(x^{-1}y) - (xx^{-1})y = 0 \implies -(x, x^{-1}, y) = 0$$

Lema 2.1.5. O inverso, em uma álgebra alternativa A, é único.

Demonstração: Se x' é outro inverso de x (xx' = 1), então

$$x' = 1x' = (x^{-1}x)x' = x^{-1}(xx') = x^{-1}.1 = x^{-1},$$

usando que $(x, x^{-1}, x') = 0$, pelo lema anterior.

Lema 2.1.6. Seja A álgebra alternativa de dimensão finita, com 1, sendo 1 o único idempotente de A. Então para todo $z \in A$, ou z tem inverso, $z^{-1} \in A$, ou z é propriamente nilpotente.

Demonstração: Seja $z \in A$ não nilpotente. A(z) é uma subálgebra de A, associativa de dimensão finita que não é uma nilálgebra. Logo, segundo o Lema 1.3.1 (Albert), A(z) contém um idempotente. Mas $A(z) \subset A$ e o único idempotente de A é 1. Logo

$$1 = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \dots + \alpha_1 z \qquad \alpha_i \in F$$

$$\Rightarrow 1 = z(\alpha_n z^{n-1} + \alpha_{n-1} z^{n-2} + \dots + \alpha_1)$$

Portanto z é invertível.

Suponhamos agora z nilpotente. Mostremos que z é propriamente nilpotente. Se z não for propriamente nilpotente, então existe $a \in A$ tal que za não é nilpotente. Logo, pela primeira parte deste lema, za tem inverso $(za)^{-1}$.

Como z é nilpotente, existe m tal que $z^m=0$ e $z^{m-1}\neq 0$. Então:

$$0 \neq z^{m-1} = z^{m-1}((za)(za)^{-1}) \stackrel{*}{=} (z^{m-1}(za))(za^{-1})$$
$$= ((z^{m-1}z)a)(za^{-1}) = (z^ma)(za^{-1}) = 0$$

contradição. Portanto z é propriamente nilpotente.

(*) A subálgebra gerada por dois elementos de uma álgebra alternativa, é associativa. \Box

Lema 2.1.7. Seja A álgebra alternativa de dimensão finita, com 1, sendo 1 o único idempotente de A. O conjunto $\mathcal B$ dos elementos propriamente nilpotentes de A é um ideal de A.

Demonstração: Para mostrar que \mathcal{B} é um ideal de A devemos mostrar três coisas:

(i) $z + z' \in \mathcal{B}$, para todos $z, z' \in \mathcal{B}$

Sejam $z, z' \in \mathcal{B}$. Se $z + z' \notin \mathcal{B}$, z + z' não é propriamente nilpotente, logo, pelo lema anterior, z + z' não é nilpotente. Então, ainda pelo lema anterior, z + z' tem um inverso y e escrevemos:

$$(z+z')y = 1 \Rightarrow zy + z'y = 1 \Rightarrow z'y = 1 - zy$$

Mas zy é propriamente nilpotente, pois $z \in \mathcal{B}$ e $y \in A$, logo zy é nilpotente. Podemos escrever:

$$(zy)^{m} = 0 \implies 1 - (zy)^{m} = 1$$

$$= (1 - zy)((zy)^{m-1} + (zy)^{m-2} + \dots + (zy)^{2} + zy + 1)$$

$$\implies (1 - zy)^{-1} = 1 + zy + (zy)^{2} + \dots$$

Assim, 1-zy tem inverso. Mas 1-zy=z'y e z'y é nilpotente, pois $z'\in\mathcal{B}$ e $y\in A$. Mas z'y não pode ser ao mesmo tempo nilpotente e invertível. Chegamos a esta contradição, ao afirmarmos que z+z' não é propriamente nilpotente. Devemos ter, portanto, z+z' propriamente nilpotente, ou seja, $z+z'\in\mathcal{B}$.

(ii) $\alpha z \in \mathcal{B}$, para todo $\alpha \in F$, e todo $z \in \mathcal{B}$

Sejam $\alpha \in F$ e $z \in \mathcal{B}$. Como z é propriamente nilpotente, isto é, za é nilpotente, $\forall a \in A$, temos:

$$\alpha(za) = z(\alpha a) = (\alpha z)a$$

Mas $z(\alpha a)$ é nilpotente, uma vez que $\alpha a \in A$. Daí, $(\alpha z)a$ é nilpotente. Portanto αz é propriamente nilpotente, isto é, $\alpha z \in \mathcal{B}$.

(iii) $az \in \mathcal{B}$, para todo $a \in A$, e todo $z \in \mathcal{B}$

Sejam $a \in A$, $z \in \mathcal{B}$. Como z é propriamente nilpotente, az é nilpotente, $\forall a \in A$. Mas, nesta álgebra, como vimos no lema anterior, todo elemento nilpotente é também propriamente nilpotente. Então az é propriamente nilpotente, isto é, $az \in \mathcal{B}$.

Definição 2.1.5. Em qualquer álgebra A, um idempotente e é chamado **principal** se não existir idempotente $u \in A$, não nulo, ortogonal a e.

A proposição a seguir dá uma caracterização para o idempotente principal em termos da subálgebra A_{00} da decomposição de Peirce.

Proposição 2.1.8. Sejam A uma álgebra alternativa de dimensão finita $e \in A$. Então e é um idempotente principal de A se e somente se a subálgebra A_{00} na decomposição de Peirce relativa a e, é uma nilálgebra. **Demonstração:** (\Rightarrow) Seja $e \in A$ idempotente principal. Dado $x \in A_{00}$, então xe = ex = 0. Logo x é ortogonal a e. Então x não é idempotente, pois se fosse, e não seria principal. Então A_{00} não tem idempotentes não nulos. Assim, de acordo com o Lema 1.3.3, A_{00} é uma nilálgebra.

(\Leftarrow) Seja A_{00} uma nilálgebra. Então $\forall x \in A_{00}$, x é nilpotente. Seja $u \in A$ um idempotente ortogonal a e. Então ue = eu = 0, o que significa que $u \in A_{00}$, ou seja u é nilpotente. Mas isto é uma contradição, pois se u é nilpotente não pode ser idempotente. Então não podem existir idempotentes não nulos ortogonais a e. Logo e é principal.

O próximo resultado garante a existência de idempotentes principais em qualquer álgebra alternativa de dimensão finita que não é uma nilálgebra.

Proposição 2.1.9. Qualquer álgebra alternativa A de dimensão finita que não é uma nilálgebra contém um idempotente principal.

Demonstração: Pelo Lema 1.3.3, A contém um idempotente e. Se e não é principal, existe um idempotente u em A, ortogonal a e, isto é, $u^2 = u, u \neq 0$ e ue = eu = 0. Mas isto significa que $u \in A_{00}$. Além disso, e' = e + u é um idempotente e a subálgebra $A_{11,e'}$ contém propriamente $A_{11} = A_{11,e}$. De fato, seja $x_{11} \in A_{11}$. Então:

$$x_{11}e' = x_{11}e + x_{11}u = x_{11}e = x_{11}$$

$$e'x_{11} = ex_{11} + ux_{11} = ex_{11} = x_{11}$$

Logo, $x_{11} \in A_{11,e'}$. E como $u \in A_{11,e'}$ e $u \notin A_{11,e}$, segue que dim $A_{11,e} < \dim A_{11,e'}$. Se e' é principal, está demonstrado. Caso contrário repetimos o procedimento acima para um idempotente $u' \in A$ ortogonal a e'. O novo idempotente e'' = e' + u' deve gerar uma subálgebra $A_{11,e''}$ com dimensão maior que a dimensão de $A_{11,e'}$. Como A é de dimensão finita este processo deve acabar em algum momento, resultando então em um idempotente principal.

Os resultados a seguir permitirão conhecer com mais detalhes como são os elementos propriamente nilpotentes de uma álgebra A. A partir deste conhecimento ficará mais natural a relação destes elementos com o radical R(A).

Consideremos inicialmente a decomposição de Peirce de A relativa a um idempotente principal e, a ser usada no próximo lema.

Lema 2.1.10. Seja A álgebra alternativa de dimensão finita $e = e_1 + \cdots + e_t$ um idempotente principal de A, onde os e_i são idempotentes primitivos dois a dois ortogonais. Seja a decomposição de Peirce de A em relação aos idempotentes e_1, \ldots, e_t . Então, para todo $i = 1, \ldots, t$:

- (i) e_i é a unidade de A_{ii} ;
- (ii) e_i é o único idempotente de A_{ii} ;
- (iii) Se $x_{ii} \in A_{ii}$ é propriamente nilpotente em A_{ii} , então x_{ii} é propriamente nilpotente em A.

Demonstração: Temos: $A_{ii} = \{x_{ii} \in A \mid e_k x_{ii} = \delta_{ki} x_{ii}, x_{ii} e_k = \delta_{ik} x_{ii}\}$. Se k = i, então $e_i x_{ii} = x_{ii} e_i = x_{ii}$, o que prova (i).

Se $u \in A_{ii}$ é um idempotente, então $e_i = u + (e_i - u)$. Mas $u(e_i - u) = ue_i - u^2 = u - u = 0$, logo u e $(e_i - u)$ são ortogonais. Escrevemos então e_i como soma de dois idempotentes ortogonais, o que contraria o fato de e_i ser primitivo. Logo, e_i é o único idempotente em A_{ii} , provando (ii).

Se x_{ii} é propriamente nilpotente em A_{ii} , isto é $x_{ii}a_{ii}$ é nilpotente $\forall a_{ii} \in A_{ii}$, existe $r \in \mathbb{N}$ tal que $(x_{ii}a_{ii})^r = 0$

A Propriedade 11 da decomposição de Peirce estabelece que

$$(x_{ii}a)^m = (x_{ii}a_{ii})^{m-1} \sum_{k=0}^t x_{ii}a_{ik}.$$

Fazendo r = m - 1, temos que $(x_{ii}a)^{r+1} = 0$. Assim $x_{ii}a$ é nilpotente $\forall a \in A$. Logo x_{ii} é propriamente nilpotente em A e, (iii) está provado.

Lema 2.1.11. Nas hipóteses do lema anterior, seja o conjunto

 $G_{ij} = \{s_{ij} \in A_{ij} \mid todos \ os \ elementos \ de \ s_{ij}A_{ji} \ s\~ao \ nilpotentes \}.$

Cada G_{ij} é um subespaço vetorial de A e $G_{ij} \subseteq \mathcal{B}$, o conjunto dos elementos propriamente nilpotentes de A.

Demonstração: Vamos mostrar primeiro que $G_{ij} \subseteq \mathcal{B}, i, j = 0, \dots, t$.

Pela Proposição 2.1.8, A_{00} é uma nilálgebra. Assim, pela Propriedade 11 (Peirce), todo elemento em A_{00} é propriamente nilpotente em A. Podemos concluir então que: $G_{00} = A_{00} \subseteq \mathcal{B}$.

É fácil ver que $G_{0j} = A_{0j}$, j = 1, ..., t. Vamos mostrar agora que os elementos de G_{0j} são propriamente nilpotentes, o que significa que $G_{0j} \subseteq \mathcal{B}$. Usando a Propriedade 12 (Peirce), fazendo i = 0, temos:

$$(x_{0j}a)^m = (x_{0j}a_{j0})^{m-1} \sum_{k=0}^t x_{0j}a_{jk} + (x_{0j}a_{0j})(x_{0j}a_{j0})^{m-1}$$

Mas $x_{0j}a_{j0} \in A_{00}$, logo é um elemento nilpotente. Fazendo m-1=r (r= índice de nilpotência de $x_{0j}a_{j0}$), temos que: $(x_{0j}a_{j0})^r=0$, e daí: $(x_{0j}a)^{r+1}=0$. Isto mostra que $(x_{00}a)$ é nilpotente, ou seja x_{0j} é propriamente nilpotente. Portanto $G_{0j} \subseteq \mathcal{B}$.

De maneira análoga provamos que $G_{i0} = A_{i0}$, i = 1, ..., t. Para provar que $G_{i0} \subseteq \mathcal{B}$ usamos novamente a propriedade 12 da decomposição de Peirce, mas com uma leve adaptação, conforme indicamos a seguir. Fazendo j = 0 na referida propriedade, vem:

$$(x_{i0}a)^m = (x_{i0}a_{0i})^{m-1} \sum_{k=0}^t x_{i0}a_{0k} + (x_{i0}a_{i0})(x_{i0}a_{0i})^{m-1}$$

O termo $(x_{i0}a_{0i}) \in A_{ii}$ não é necessariamente nilpotente. Aí fazemos:

$$(x_{i0}a_{0i})^{m-1} = (x_{i0}a_{0i})(x_{i0}a_{0i})\dots(x_{i0}a_{0i}) = x_{i0}(a_{0i}x_{i0})\dots(a_{0i}x_{i0})a_{0i}$$
$$= x_{i0}(a_{0i}x_{i0})^{m-2}a_{0i}$$

Assim, o termo $(a_{0i}x_{i0}) \in A_{00}$, sendo portanto nilpotente. Daí $(x_{i0}a)^m = 0$ para algum m, o que significa que x_{i0} é propriamente nilpotente. Portanto $G_{i0} \subseteq \mathcal{B}$.

Resta provar que $G_{ij} \subseteq \mathcal{B}$, para $i, j \neq 0$. Com o mesmo argumento utilizado para mostrar que $G_{i0} \subseteq \mathcal{B}$, usando j no lugar de 0 na propriedade 12 (Peirce), temos que se $x_{ij} \in G_{ij}$, então $(x_{ij}a_{ji})$ é nilpotente. Logo, pela propriedade 12, $x_{ij}a$ é nilpotente $\forall a \in A$. Mas isto quer dizer que x_{ij} é propriamente nilpotente, ou seja $x_{ij} \in \mathcal{B}$. Portanto $G_{ij} \subseteq \mathcal{B}$.

Mostremos agora que cada G_{ij} é um subespaço de A. Sejam $s_{ij}, s'_{ij} \in G_{ij}$. Para que G_{ij} seja subespaço de A, devemos ter:

(i)
$$\alpha s_{ij} \in G_{ij}$$
, para todo $\alpha \in F$;

(ii)
$$s_{ij} + s'_{ij} \in G_{ij}$$
.

Para provar (i) basta mostrar que $\alpha s_{ij}a_{ji}$ é nilpotente. Mas $s_{ij}a_{ji}$ é nilpotente, logo, $(s_{ij}a_{ji})^m = 0$, para algum m. Então:

$$(\alpha s_{ij}a_{ji})^m = \alpha^m (s_{ij}a_{ji})^m = \alpha^m.0 = 0$$

Quanto a (ii), devemos mostrar que $(s_{ij} + s'_{ij})a_{ji}$ é nilpotente, para todo $a_{ji} \in A_{ji}$. Pelo Lema 2.1.10 e_i é o único idempotente de A_{ii} . Agora, usando o Lema 2.1.7 o conjunto dos elementos propriamente nilpotentes de A_{ii} é um ideal. Assim, $(s_{ij} + s' + ij)a_{ji} = s_{ij}a_{ji} + s'_{ij}a_{ji}$ é propriamente nilpotente em A_{ii} .

O próximo teorema estabelece uma relação importante entre o conjunto dos elementos propriamente nilpotentes e o radical.

Teorema 2.1.12 (Zorn). O radical R de qualquer álgebra alternativa A de dimensão finita é o conjunto \mathcal{B} dos elementos propriamente nilpotentes de A.

Demonstração: Seja $G = \sum G_{ij}$. De acordo com o lema anterior cada $G_{ij} \subseteq \mathcal{B}$. Assim $G \subseteq \langle \mathcal{B} \rangle$. Mostremos que $G = \mathcal{B}$ e que G é um ideal de A. Vamos dividir esta demonstração nos seguintes passos, onde mostraremos que:

(i) $\mathcal{B} \subseteq G$

Supondo por absurdo que \mathcal{B} não está contido em G, existe $x \in \mathcal{B}$ tal que $x \notin G = \sum G_{ij}$. Mas $x = \sum x_{ij}$, e $x_{ij} \in A_{ij}$, com pelo menos um $x_{ij} \notin G_{ij}$. Mas, pelo lema anterior (2.1.11), $G_{ij} = A_{ij}$ se i = 0 ou j = 0. Logo $x_{ij} \notin G_{ij}$ requer necessariamente que $i, j \neq 0$.

Se i = j, $x_{ij} \in A_{jj}$, que é uma álgebra com 1, logo, pelo Lema 2.1.6, x_{ij} tem inverso ou é propriamente nilpotente. Mas estamos supondo $x_{ij} \notin G_{ij} \subseteq \mathcal{B}$, logo x_{ij} não é propriamente nilpotente. Então x_{ij} tem inverso b_{ji} em U_{jj} e podemos escrever

$$b_{ii}x_{ij}=e_i$$

Vamos mostrar que se $i \neq j$, temos a mesma equação para algum $b_{ji} \in A_{ji}$. Como $x_{ij} \notin G_{ij}$, existe $a_{ji} \in A_{ji}$ tal que $a_{ji}x_{ij} \in A_{jj}$ não é nilpotente. Logo $a_{ji}x_{ij}$ tem inverso $z_{jj} \in A_{jj}$ e temos:

$$z_{jj}(a_{ji}x_{ij}) = e_j$$

Mas, pela propriedade 6 (Peirce), $(z_{jj}, a_{ji}, x_{ij}) = 0$, $i \neq j$. Então posso associar, o que resulta:

$$(z_{jj}a_{ji})x_{ij} = e_j$$

O elemento $z_{jj}a_{ji} \in A_{ji}$ é o inverso de x_{ij} . Assim, podemos considerar a mesma equação $b_{ji}x_{ij} = e_j$, tanto para i = j como para $i \neq j$.

Pela propriedade 13 (Peirce):

$$e_i(x_{ij}a)^m = (x_{ij}a_{ji})^m \quad i, j = 0, 1, \dots, t$$

Fazendo as seguintes substituições: i = j, j = i, $x_{ij} = b_{ji}$ e a = x, temos:

$$e_j(b_{ji}x)^m e_j = (b_{ji}x_{ij})^m = e_j^m = e_j \neq 0$$

Logo $b_{ji}x$ não é nilpotente, o que significa que x não é propriamente nilpotente, isto é, $x \notin \mathcal{B}$, uma contradição.

Portanto, se $x \in \mathcal{B}$, devemos ter $x \in G$, e assim $\mathcal{B} \subseteq G$, como queríamos.

(ii) $G = \langle \mathcal{B} \rangle$

Como G é subespaço de A, claro que $\langle \mathcal{B} \rangle \subseteq G$. E como, pelo Lema 2.1.11, $G \subseteq \langle \mathcal{B} \rangle$, segue que $G = \langle \mathcal{B} \rangle$.

(iii) G é um ideal de A

Mostraremos inicialmente as seguintes inclusões:

(iii.1)
$$G_{ij}A_{ik} \subseteq G_{ik}$$
 $i, j, k = 0, 1, \dots, t$

(iii.2)
$$G_{ij}A_{ij} \subseteq G_{ji}$$
 $i \neq j$, $i, j = 1, \dots, t$

Se i = k, seja $s_{ij} \in G_{ij}$. Então $s_{ij}A_{ji}$ é nilpotente e $s_{ij}A_{ji} \in A_{ii}$. Mas, notando que:

$$G_{ii} = \{s_{ii} \in A_{ii} \mid \text{todos os elementos de } s_{ii}A_{ii} \text{ são nilpotentes}\}$$

temos que $s_{ij}A_{ji} \subseteq G_{ii}$, $\forall s_{ij} \in G_{ij}$. Então $G_{ij}A_{ji} \subseteq G_{ii}$. Se $i \neq k$, usamos a propriedade 6 (Peirce), fazendo:

$$(G_{ij}A_{ik})A_{ki} = G_{ij}(A_{ik}A_{ki}) \subseteq G_{ij}A_{ii} \subseteq G_{ii}$$

Isto indica que $x_{ik}A_{ki}$ é nilpotente, onde $x_{ik} \in G_{ij}A_{jk}$. Mas, notando que:

 $G_{ik} = \{s_{ik} \in A_{ik} \mid \text{todos os elementos de } s_{ik} A_{ki} \text{ são nilpotentes}\}$

temos que $x_{ik}A_{ki} \in G_{ik}$, para todo $x_{ik} \in G_{ik}A_{ki}$. Então: $G_{ij}A_{jk} \in G_{ik}$. Provamos, assim, a inclusão (iii.1).

Aplicando a propriedade 8 (Peirce), podemos escrever:

$$(G_{ij}A_{ij})A_{ij} = (A_{ij}A_{ij})G_{ij} \subseteq A_{ji}G_{ij}$$

Vamos mostrar que $A_{ji}G_{ij} \subseteq G_{jj}$.

Seja $s_{ij} \in G_{ij}$. Então $A_{ji}s_{ij}$ é nilpotente e $A_{ji}s_{ij} \subseteq A_{jj}$. Mas notando que:

$$G_{jj} = \{s_{jj} \in A_{jj} \mid \text{todos os elementos de } A_{jj}s_{jj} \text{ são nilpotentes}\}$$

segue que $A_{ji}s_{ij} \subseteq G_{jj}$, para todo $s_{ij} \in G_{ij}$. Logo $A_{ji}G_{ij} \subseteq G_{jj}$. Assim, os elementos de $(G_{ij}A_{ij})A_{ij}$ são nilpotentes, logo $x_{ji} \in G_{ij}A_{ij} \implies x_{ji} \in G_{ji}$. Portanto $G_{ij}A_{ij} \subseteq G_{ji}$, concluindo a prova de (iii.2).

Podemos então escrever:

$$GA = (\sum G_{ij})(\sum A_{kl}) = \sum G_{ij}A_{jk} + \sum_{i \neq j} G_{ij}A_{ij} \subseteq G$$

Esta última inclusão ocorre porque cada parcela está em G, de acordo com (iii.1) e (iii.2).

(iv) $\langle \mathcal{B} \rangle$ é nilpotente (logo $\langle \mathcal{B} \rangle \subseteq R$)

Já mostramos que $G = \langle \mathcal{B} \rangle$ é um ideal de A. Provemos agora que $\langle \mathcal{B} \rangle$ é um ideal nilpotente. Supondo que $\langle \mathcal{B} \rangle$ não seja nilpotente, por estarmos em dimensão finita, $\langle \mathcal{B} \rangle$ não é nilálgebra. Então, pelo Lema 1.3.3, $\langle \mathcal{B} \rangle$ possui um idempotente $e = e_1 + \cdots + e_r$.

Mas $\langle \mathcal{B} \rangle = G = \sum G_{ij}$, logo $e_1 \in G_{11}$ é nilpotente, contradição. Então $\langle \mathcal{B} \rangle$ é nilpotente, logo $\langle \mathcal{B} \rangle \subseteq R$. Mas $R \subseteq \mathcal{B}$, logo $\langle \mathcal{B} \rangle = \mathcal{B}$ e, portanto $R = \mathcal{B}$.

Corolário 2.1.13. Seja e um idempotente em uma álgebra alternativa A de dimensão finita e R radical de A. Seja a decomposição de Peirce de A em relação a e, dada por $A = A_{11} + A_{10} + A_{01} + A_{00}$. Se R_i é o radical de A_{ii} , então $R_i = R \cap A_{ii}$, (i = 0, 1).

Demonstração: Seja $x_{ii} \in R_i$. Claro que $x_{ii} \in A_{ii}$ e x_{ii} é propriamente nilpotente em A_{ii} . Então, pelo Lema 2.1.10, segue que x_{ii} é propriamente nilpotente em A, logo $x_{ii} \in R$. Então $x_{ii} \in R \cap A_{ii}$ e portanto $R_i \subseteq R \cap A_{ii}$.

Reciprocamente, seja $x_{ii} \in R \cap A_{ii}$. Temos que x_{ii} é propriamente nilpotente em A (pois $x_{ii} \in R$). Mas como $x_{ii} \in A_{ii}$, x_{ii} é propriamente nilpotente em A_{ii} , isto é, $x_{ii} \in R_i$. Logo $R \cap A_{ii} \subseteq R_i$. Daí, temos a igualdade desejada.

Corolário 2.1.14. Seja e um idempotente principal em uma álgebra alternativa A de dimensão finita. Então $A_{10} + A_{01} + A_{00} \subseteq R$.

Demonstração: Pelo Lema 1.3.3 podemos escrever $e = e_1 + \cdots + e_t$, com os e_i idempotentes primitivos dois a dois ortogonais. Vamos provar que

$$A_{10} = \sum_{i=1}^{t} G_{i0}, \quad A_{01} = \sum_{j=1}^{t} G_{0j}, \quad e \quad A_{00} = G_{00}.$$

Esta última igualdade já foi provada no Lema 2.1.11, onde também foi provado que $G_{i0} = A_{i0}$ e $G_{0j} = A_{0j}$, i, j = 1, ..., t. Considerando a decomposição de Peirce de A em relação aos e_i , temos, pela própria maneira como tal decomposição é definida, que $A_{10} = \sum_{i=1}^t A_{i0}$, o que é equivalente a $A_{10} = \sum_{i=1}^t G_{i0}$. Analogamente provamos que $A_{01} = \sum_{j=1}^t G_{0j}$. Como, pelo mesmo lema os G_{ij} são subespaços de A e $G_{ij} \subseteq \mathcal{B} = R$, segue que $\sum_{i=1}^t G_{i0} + \sum_{j=1}^t G_{0j} + G_{00} \subseteq R$, ou $A_{10} + A_{01} + A_{00} \subseteq R$, conforme foi afirmado. \square

Definição 2.1.6. Uma álgebra alternativa A é chamada **semisimples** se R(A)=0.

Teorema 2.1.15. Toda álgebra alternativa semisimples A não nula, de dimensão finita possui unidade.

Demonstração: Como A é semisimples, seu radical R é nulo. Como $A \neq 0$, A não é uma nilálgebra. De fato, se A fosse nilálgebra, todo $x \in A$ seria nilpotente. Como A é de dimensão finita, A seria nilpotente. Mas R é o ideal nilpotente maximal de A, logo A = R = 0, contradição.

Pelo Lema 1.3.3, se A não é nilálgebra, A possui um elemento idempotente. Nestas condições, A possui um idempotente principal e, de acordo com a Proposição 2.1.9.

Daí, pelo corolário anterior (2.1.14), considerando a decomposição de Peirce de A relativa a e, temos:

$$A_{10} + A_{01} + A_{00} \subseteq R = 0 \implies A = A_{11} = eAe \implies e = 1$$

Definição 2.1.7. Uma álgebra A é chamada simples se A não é uma zero álgebra e os seus únicos ideais são 0 e A.

O teorema a seguir, devido a Zorn, estabelece a estrutura das álgebras semisimples, como soma direta de ideais simples. Sua demonstração será omitida, podendo ser encontrada em [22].

Teorema 2.1.16 (Zorn). Uma álgebra alternativa A não nula de dimensão finita é semisimples se e somente se $A = G_1 \oplus \cdots \oplus G_t$, com G_i ideais simples $(i = 1, \ldots, t)$.

Exemplos de álgebras semisimples

- Toda álgebra simples é semisimples.
 É uma conseqüência direta do teorema anterior (2.1.16).
- finita é uma álgebra semisimples. Sejam A_1, \ldots, A_n álgebras simples. Formamos o produto cartesiano $A = A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i, \ 1 \leq i \leq n\}$. Tal produto é uma álgebra se definirmos as operações componente a componente. Assim, se $a = (a_1, \ldots, a_n), \ b = (b_1, \ldots, b_n) \in A$, temos: $a + b = (a_1 + b_1, \ldots, a_n + b_n)$ e $ab = (a_1b_1, \ldots, a_nb_n)$. Para $i = 1, \ldots, n$, seja $I_i = 0 \times \cdots \times 0 \times A_i \times 0 \times \cdots \times 0$. I_i é um ideal simples de A, pois A_i é simples. Como $A = I_1 \oplus \cdots \oplus I_n$, então A é semisimples.

2) O produto cartesiano de uma família finita de álgebras simples de dimensão

- 3) A/R(A) é semisimples. A verificação de que o radical de A/R(A) é nulo será feita no lema a seguir.
- 4) Seja G um grupo finito e F corpo. A álgebra de grupo FG é definida por: $FG = \{ \sum_{g \in G} \alpha_g g, \ \alpha_g \in F \}. \ FG \text{ é semisimples se e somente se } carF = 0 \text{ ou } carF$ não divide a ordem de G. Este é o Teorema de Maschke, cuja demonstração pode ser encontrada em [5].

Lema 2.1.17. Seja (A, w) álgebra bárica alternativa. Então R(A/R(A)) = 0

Demonstração: $x \in R(A/R(A)) \Rightarrow x = a + R(A)$, com $a \in A$ e x é propriamente nilpotente. Seja n índice de nilpotência de R(A). Então, dado $y \in A/R(A)$, y = b + R(A). Daí: $0 = (yx)^n = ((b + R(A))(a + R(A)))^n = (ba)^n + (R(A))^n = (ba)^n + R(A) \Rightarrow (ba)^n \in R(A)$. Assim, ba é nilpotente, o que significa que a é propriamente nilpotente. Logo $a \in R(A)$ e a + R(A) = x = 0.

2.2 Decomposição de Peirce em álgebras báricas

Vimos que uma álgebra bárica alternativa (A, w) pode ser decomposta como $A = Fx \oplus Ker(w)$, para algum $x \in A$, com $w(x) \neq 0$.

Vimos também que (A, w) (bárica alternativa) possui um idempotente de peso 1. Seja e este idempotente. Podemos fazer a decomposição acima com e no lugar de x e ficamos com:

$$A = Fe \oplus Ker(w)$$
 ou, equivalentemente $A = Fe \oplus bar(A)$

Além disso, temos a decomposição de Peirce de A em relação à e, dada por:

$$A = A_{11} \oplus A_{10} \oplus A_{01} \oplus A_{00}$$
, onde
 $A_{ij} = \{x_{ij} \in A \mid ex_{ij} = ix_{ij}, x_{ij}e = jx_{ij}, i, j = 0, 1\}$

A proposição seguinte relaciona estas duas decomposições.

Proposição 2.2.1. Tendo em vista as duas decomposições da álgebra bárica alternativa (A, w), temos:

$$A_{11} = Fe \oplus bar(A)_{11}$$
 $A_{10} = bar(A)_{10}$ $A_{01} = bar(A)_{01}$ $A_{00} = bar(A)_{00}$

Demonstração: Explicitando a decomposição de bar(A) em termos de seus elementos, temos:

$$bar(A)_{11} = \{x \in bar(A) \mid ex = x, xe = x\}$$

$$bar(A)_{10} = \{x \in bar(A) \mid ex = x, xe = 0\}$$

$$bar(A)_{01} = \{x \in bar(A) \mid ex = 0, xe = x\}$$

$$bar(A)_{00} = \{x \in bar(A) \mid ex = 0, xe = 0\}$$

Mostremos primeiro que $A_{11} = Fe \oplus bar(A)_{11}$. Seja $x \in Fe \oplus bar(A)_{11}$. Então $x = \alpha e + u, \ \alpha \in F, \ u \in bar(A)_{11}$. Daí:

$$xe = (\alpha e + u)e = (\alpha e)e + ue = \alpha e^2 + u = \alpha e + u = x$$
$$ex = e(\alpha e + u) = e\alpha e + eu = \alpha e^2 + u = \alpha e + u = x$$

Como xe = x = ex, segue que $Fe \oplus bar(A)_{11} \subseteq A_{11}$.

Seja agora $x \in A_{11}$. Considerando a decomposição original de A como $A = Fe \oplus bar(A)$, podemos escrever $x = \alpha e + u$, com $\alpha \in F$, e $u \in bar(A)$. Mas $x \in A_{11}$, então:

$$xe = x \implies (\alpha e + u)e = \alpha e + u \implies \alpha e^2 + ue = \alpha e + u$$

 $\Rightarrow \alpha e + ue = \alpha e + u \implies ue = u$
 $ex = x \implies e(\alpha e + u) = \alpha e + u \implies e\alpha e + eu = \alpha e + u$
 $\Rightarrow \alpha e^2 + eu = \alpha e + u \implies \alpha e + eu = \alpha e + u \implies eu = u$

Então, ue = u = eu, logo $u \in bar(A)_{11}$ e, assim, $x \in Fe \oplus bar(A)_{11}$, logo $A_{11} \subseteq Fe \oplus bar(A)_{11}$. Com isto, provamos que $A_{11} = Fe \oplus bar(A)_{11}$.

Mostremos agora que $A_{10} = bar(A)_{10}$. Evidentemente $bar(A)_{10} \subseteq A_{10}$. Resta provar que $A_{10} \subseteq bar(A)_{10}$. Seja $x \in A_{10}$. Então ex = x e xe = 0, e calculamos:

$$w(x) = w(ex) = w(e)w(x) = w(x)w(e) = w(xe) = w(0) = 0$$

Daí, $x \in bar(A)$. E como ex = x e xe = 0, segue que $x \in bar(A)_{10}$. Logo $A_{10} \subseteq bar(A)_{10}$, resultando então que $A_{10} = bar(A)_{10}$.

De maneira inteiramente análoga se prova que $A_{01} = bar(A)_{01}$

Mostremos finalmente que $A_{00} = bar(A)_{00}$. É claro que $bar(A)_{00} \subseteq A_{00}$. Basta mostrar que $A_{00} \subseteq bar(A)_{00}$. Para tanto, seja $x \in A_{00}$. Então xe = ex = 0. Afirmamos que $x \in bar(A)$. De fato:

$$w(x) = 1.w(x) = w(e).w(x) = w(ex) = w(0) = 0$$

E como xe = ex = 0, temos que $x \in bar(A)_{00}$, logo $A_{00} \subseteq bar(A)_{00}$ e, portanto $A_{00} = bar(A)_{00}$.

Observações

• A decomposição de Peirce de A em relação a e fica:

$$A = Fe \oplus bar(A)_{11} \oplus bar(A)_{10} \oplus bar(A)_{01} \oplus bar(A)_{00}$$

• $Fe \oplus bar(A)_{11}$ é uma subálgebra bárica de A. De fato, se $x \in Fe \oplus bar(A)_{11}$, então existe $\alpha \in F$ e $u \in bar(A)_{11}$ tal que

$$x = \alpha e + u$$
 e $w(x) = w(\alpha e + u) = \alpha w(e) + w(u) = \alpha .1 + 0 = \alpha$.

E como α é arbitrário, o peso de x não é zero. Assim, $Fe \oplus bar(A)_{11}$ é uma subálgebra bárica de A.

• $bar(A)_{00}$ é uma subálgebra de bar(A) que não é bárica.

A proposição a seguir estabelece as condições para que um idempotente e em uma álgebra bárica alternativa seja principal.

Proposição 2.2.2. Em uma álgebra bárica alternativa (A, w), um elemento e é um idempotente principal se e somente se $bar(A)_{00}$ é uma nilálgebra.

Demonstração: (\Rightarrow) Se e é um idempotente principal e $x \in bar(A)_{00}$, então ex = xe = 0. Isto significa que x é ortogonal a e. Logo x não pode ser idempotente, pois, se fosse, e não seria principal. Então, $bar(A)_{00}$ não possui idempotentes. Como $bar(A)_{00}$ é subálgebra de A, segue que $bar(A)_{00}$ é uma nilálgebra.

(\Leftarrow) Se $bar(A)_{00}$ é uma nilálgebra, $bar(A)_{00}$ não possui idempotentes, pois todo elemento de $bar(A)_{00}$ é nilpotente. Se e não fosse principal, existiria um idempotente $x \in A$ ortogonal a e, isto é, ex = xe = 0, logo $x \in bar(A)_{00}$, contradição. Portanto e é principal.

Seja $e \in (A, w)$ um idempotente de peso 1. Sabemos que $e = e_1 + \cdots + e_n$, com os e_i idempotentes primitivos dois a dois ortogonais. Se e é um idempotente, devemos ter w(e) = 0 ou w(e) = 1. De fato, se $w(e) \neq 0$, então $w(e) = w(e^2) = w(e)w(e) \Rightarrow w(e) = 1$. Assim, na decomposição acima, supondo w(e) = 1, temos: $1 = w(e) = w(e_1 + \cdots + e_n) = w(e_1) + \cdots + w(e_n)$. Então, um dos e_i tem peso 1 e os demais, peso 0. Vamos considerar: $w(e_1) = \ldots = w(e_{n-1}) = 0$ e $w(e_n) = 1$. Desta forma, escrevemos:

$$A = Fe \oplus bar(A)$$
.

Obtemos também uma decomposição mais refinada de A

$$A = \bigoplus_{i,j=1}^{n} A_{ij}$$
, onde

$$A_{ij} = \{x_{ij} \in A \mid e_k x_{ij} = \delta_{ki} x_{ij} \in x_{ij} e_k = \delta_{jk} x_{ij} \}$$

 $i, j = 0, \dots, n; \quad k = 1, \dots, n$

Proposição 2.2.3. Tendo em vista as duas decomposições da álgebra bárica alternativa (A, w), temos:

$$A_{nn} = Fe_n \oplus bar(A)_{nn}, \quad A_{ij} = bar(A)_{ij}, \quad (i,j) \neq (n,n)$$

Demonstração: É inteiramente análoga à Proposição 2.2.1

Com a notação da proposição anterior, escrevemos:

$$A = Fe_n \oplus (\bigoplus_{i,j=0}^n bar(A)_{ij})$$

Consideremos agora a decomposição de Peirce de bar(A) em relação a

$$u = e_1 + \dots + e_{n-1}.$$

Para isto usaremos a notação $(bar(A))_{ij}$ para diferenciar de $bar(A)_{ij}$ (que se refere à decomposição em relação a e). Assim, temos:

$$bar(A) = \bigoplus_{i,j=0}^{n-1} (bar(A))_{ij}$$

A proposição a seguir relaciona as decomposições de bar(A) em relação a e e a u.

Proposição 2.2.4. Na notação indicada acima, tem-se:

(i)
$$(bar(A))_{00} = bar(A)_{00} \oplus bar(A)_{0n} \oplus bar(A)_{n0} \oplus bar(A)_{nn}$$

(ii)
$$\bigoplus_{j=1}^{n-1} (bar(A))_{0j} = \bigoplus_{j=1}^{n-1} (bar(A)_{0j} \oplus bar(A)_{nj})$$

(iii)
$$\bigoplus_{i=1}^{n-1} (bar(A))_{i0} = \bigoplus_{i=1}^{n-1} (bar(A)_{i0} \oplus bar(A)_{in})$$

(iv)
$$\bigoplus_{i,j=1}^{n-1} (bar(A))_{ij} = \bigoplus_{i,j=1}^{n-1} bar(A)_{ij}$$

Demonstração:

(i)
$$(bar(A))_{00} = \{x_{ij} \in bar(A) \mid e_k x_{ij} = 0, x_{ij} e_k = 0\}$$

 $(i, j = 0, \dots, n; k = 1, \dots, n-1)$

Como $e_k x_{ij} = \delta_{ki} x_{ij}$, para que um elemento x_{ij} pertença a $(bar(A))_{00}$, devemos ter $\delta_{ki} = 0$, ou seja $k \neq i$. Portanto, i = 0 e i = n.

Da mesma forma, sendo $x_{ij}e_k = \delta_{jk}x_{ij}$, para que $x_{ij} \in (bar(A))_{00}$, devemos ter $\delta_{jk} = 0$, para todos $j = 1, \ldots, n$. Portanto j = 0 e j = n.

Assim, os elementos de $(bar(A))_{00}$ são todos da forma x_{00} , x_{0n} , x_{n0} , x_{nn} . Mas $x_{00} \in bar(A)_{00}$, $x_{0n} \in bar(A)_{0n}$, $x_{n0} \in bar(A)_{n0}$ e $x_{nn} \in bar(A)_{nn}$. Logo

$$(bar(A))_{00} \subseteq bar(A)_{00} \oplus bar(A)_{0n} \oplus bar(A)_{n0} \oplus bar(A)_{nn}$$

Mas como a inclusão contrária é claramente verdadeira, segue a igualdade.

(ii)
$$(bar(A))_{0j} = \{x_{ij} \in bar(A) \mid e_k x_{ij} = 0, x_{ij} e_k = x_{ij}\}$$

 $(i, j = 0, \dots, n; k = 1, \dots, n - 1)$

Para que $e_k x_{ij} = 0$ devemos ter $k \neq i$, então i = 0 e i = n.

Para que $x_{ij}e_k = x_{ij}$ devemos ter k = j, então $j = 1, \dots, n-1$. Portanto

$$x_{ij} \in (bar(A))_{0j} \Rightarrow x_{ij} = x_{01} + \ldots + x_{0,n-1} + x_{n1} + \ldots + x_{n,n-1}$$

Assim
$$(bar(A))_{0j} \subseteq \bigoplus_{j=1}^{n-1} (bar(A)_{0j}) \oplus bar(A)_{nj}$$

Como a outra inclusão é clara, segue a igualdade.

(iii)
$$(bar(A))_{i0} = \{x_{ij} \in bar(A) \mid e_k x_{ij} = x_{ij}, \ x_{ij} e_k = 0\}$$

 $(i, j = 0, \dots, n; \ k = 1, \dots, n - 1)$

Para que $e_k x_{ij} = x_{ij}$ devemos ter k = i, então $i = 1, \dots, n-1$.

Para que $x_{ij}e_k=0$ devemos ter $k\neq j$, então j=1 e j=n. Portanto

$$x_{ij} \in (bar(A))_{i0} \Rightarrow x_{ij} = x_{10} + \ldots + x_{n-1,0} + x_{1n} + \ldots + x_{n-1,n}$$

Assim
$$(bar(A))_{i0} \subseteq \bigoplus_{i=1}^{n-1} (bar(A)_{i0} \oplus bar(A)_{in})$$

Também a outra inclusão é imediata, e temos então a igualdade.

(iv)
$$(bar(A))_{ij} = \{x_{ij} \in bar(A) \mid e_k x_{ij} = x_{ij}, x_{ij} e_k = x_{ij}\}$$

 $i, j = 0, \dots, n; k = 1, \dots, n-1$

Para que $e_k x_{ij} = x_{ij}$ devemos ter k = i, então $i = 1, \dots, n-1$.

Para que $x_{ij}e_k=x_{ij}$ devemos ter k=j, então $j=1,\ldots,n-1.$

Os elementos de $(bar(A))_{ij}$ $(i,j) \neq (n,n)$ devem ser da forma:

$$x_{ij} = x_{11} + \dots + x_{1n} + \dots + x_{n-1,1} + \dots + x_{n-1,n-1}$$

Analogamente aos casos anteriores, obtemos:

$$(bar(A))_{ij} = \bigoplus_{i,j=1}^{n-1} bar(A)_{ij}$$

Proposição 2.2.5. Sejam (A, w) álgebra bárica alternativa, e idempotente principal em (A, w), com $e = e_1 + \cdots + e_n$, $w(e) = w(e_n) = 1$, e_i idempotentes primitivos dois a dois ortogonais. Então $u = e_1 + \cdots + e_{n-1}$ é um idempotente principal em bar(A).

Demonstração: Considerando a decomposição de Peirce de bar(A) em relação a u, temos, na notação da proposição anterior:

$$bar(A) = (bar(A))_{00} \oplus (\bigoplus_{j=1}^{n-1} (bar(A))_{0j} \oplus (\bigoplus_{i=1}^{n-1} (bar(A))_{i0} \oplus (\bigoplus_{i,j=1}^{n-1} (bar(A))_{ij})$$

Para que u seja principal, $(bar(A))_{00}$ deve ser uma nilálgebra (de acordo com a Proposição 2.2.2). Sabemos, da proposição anterior (2.2.4), que:

$$(bar(A))_{00} = bar(A)_{00} \oplus bar(A)_{0n} \oplus bar(A)_{n0} \oplus bar(A)_{nn}$$

Seja $x \in (bar(A))_{00}$. Podemos escrever $x = b + x_{nn}$, com

$$b \in bar(A)_{00} \oplus bar(A)_{0n} \oplus bar(A)_{n0} \subseteq R(A) \in x_{nn} \in bar(A)_{nn}$$
.

Como $A_{nn} = Fe_n \oplus bar(A)_{nn}$, pelo Lema 2.1.10 e_n é o único idempotente em A_{nn} , logo $bar(A)_{nn}$ não possui idempotentes. Então, a Proposição 2.1.9 garante que $bar(A)_{nn}$ é uma nilálgebra. Assim, x_{nn} é nilpotente. Sendo e_n o único idempotente em A_{nn} , estamos nas condições do Lema 2.1.6, em cuja demonstração ficou provado que todo elemento nilpotente em A_{nn} é também propriamente nilpotente. Temos então, x_{nn} propriamente nilpotente, logo $x_{nn} \in R(A)$.

Assim $x = b + x_{nn} \in R(A)$ (pois R(A) é ideal de $A, b \in R(A), x_{nn} \in R(A)$), logo x é propriamente nilpotente, o que significa (Lema 2.1.3) que x é nilpotente. Sendo

 $x \in (bar(A))_{00}$ arbitrário, segue que $(bar(A))_{00}$ é uma nilálgebra. Portanto u é um idempotente principal em bar(A).

Proposição 2.2.6. Seja (A, w) uma álgebra bárica alternativa $e \in A$ um idempotente de peso 1. Então bar(A) é uma nilálgebra se e somente se e é um idempotente primitivo e principal.

Demonstração: (\Rightarrow) Se e não é primitivo, então e = u + v, com u e v idempotentes ortogonais não nulos, isto é, uv = vu = 0, $u^2 = u$, $v^2 = v$ Como w(e) = 1, então se w(u) = 1, deveríamos ter $v \in bar(A)$, contradição, pois bar(A) é uma nilálgebra. Então e tem que ser primitivo. Se e não é principal, então existe $u \in A$ tal que eu = ue = 0 e $u^2 = u$. logo $u \in bar(A)$, pois 0 = w(eu) = w(e)w(u) = w(u). Contradição. Logo e deve ser principal.

 (\Leftarrow) Seja a decomposição de A em relação a e, dada por

$$A = Fe \oplus bar(A)_{11} \oplus bar(A)_{10} \oplus bar(A)_{01} \oplus bar(A)_{00}$$

que também pode ser escrita: $A = Fe \oplus bar(A)$.

Pela Proposição 2.2.5 $bar(A)_{11}$ é uma nilálgebra e, além disso, e é o único idempotente de $A_{11} = Fe \oplus bar(A)_{11}$. Assim, o Lema 2.1.6 pode ser aplicado, e todo elemento nilpotente de $bar(A)_{nn}$ é também propriamente nilpotente. Daí $bar(A)_{nn} \subseteq R(A)$. Mas, sabemos que $bar(A)_{10} \oplus bar(A)_{01} \oplus bar(A)_{00} \subseteq R(A)$, (Corolário 2.1.14) logo $bar(A) \subseteq R(A)$. Portanto bar(A) é nilpotente e, consequentemente, bar(A) é uma nilálgebra.

2.3 O radical e o bar radical

Nesta seção vamos definir o $bar\ radical$ de uma álgebra bárica. Começaremos com uma proposição que relaciona o radical de A com o radical de bar(A).

Proposição 2.3.1. Sejam (A, w) álgebra bárica alternativa, R(A) o radical de A e R(bar(A)) o radical de bar(A). Então R(A) = R(bar(A)).

Demonstração: Como R(A) é uma nilálgebra, então $R(A) \subset bar(A)$.

$$(x \in R(A) \Rightarrow x^n = 0 \Rightarrow w(x^n) = (w(x))^n = 0 \Rightarrow w(x) = 0)$$

Sendo R(A) um ideal de A, e $R(A) \subset bar(A) \subseteq A$, temos que R(A) também é um ideal (nilpotente) de bar(A). Logo $R(A) \subseteq R(bar(A))$. Resta mostrar que $R(bar(A)) \subseteq R(A)$. Para isto, é suficiente mostrar que R(bar(A)) é um ideal de A.

Considerando a decomposição de Peirce de bar(A) em relação a $u=e_1+\cdots+e_{n-1}$ dada na Proposição 2.2.5:

$$bar(A) = (bar(A))_{00} \oplus (\bigoplus_{j=1}^{n-1} (bar(A))_{0j} \oplus (\bigoplus_{i=1}^{n-1} (bar(A))_{i0} \oplus (\bigoplus_{i,j=1}^{n-1} (bar(A))_{ij})$$

Temos, pelo Corolário 2.1.14, que:

$$(bar(A))_{00} \oplus (\bigoplus_{j=1}^{n-1} (bar(A))_{0j} \oplus (\bigoplus_{j=1}^{n-1} (bar(A))_{i0} \subseteq R(bar(A))$$

Agora, usando a decomposição de Peirce de A em relação ao idempotente principal e, temos que, de acordo com a Proposição 2.2.4, um elemento $b \in R(bar(A))$ pode ser escrito de maneira única como:

$$b = (b_{00} + b_{0n} + b_{n0} + b_{nn}) + \sum_{j=1}^{n-1} (b_{0j} + b_{nj}) + \sum_{i=1}^{n-1} (b_{i0} + b_{in}) + \sum_{i,j=1}^{n-1} b_{ij}$$

Para mostrar que R(bar(A)) é um ideal de A, precisamos mostrar que $e_nb \in A$ e que $be_n \in A$, pois $w(e_n) = 1$ e $w(e_i) = 0$ para todo i = 1, ..., n - 1.

$$e_n b = e_n b_{00} + e_n b_{0n} + e_n b_{n0} + e_n b_{nn} + \sum_{j=1}^{n-1} (e_n b_{0j} + e_n b_{nj})$$

$$+ \sum_{i=1}^{n-1} (e_n b_{i0} + e_n b_{in}) + \sum_{i,j=1}^{n-1} e_n b_{ij}$$

$$\Rightarrow e_n b = b_{n0} + b_{nn} + \sum_{j=1}^{n-1} b_{nj} \in (bar(A))_{00} \oplus (\bigoplus_{j=1}^{n-1} (bar(A))_{0j}) \subseteq R(bar(A))$$

$$be_n = b_{00}e_n + b_{0n}e_n + b_{n0}e_n + b_{nn}e_n + \sum_{j=1}^{n-1} (b_{0j}e_n + b_{nj}e_n)$$

$$+ \sum_{i=1}^{n-1} (b_{i0}e_n + b_{in}e_n) + \sum_{i,j=1}^{n-1} b_{ij}e_n$$

$$\Rightarrow be_n = b_{0n} + b_{nn} + \sum_{i=1}^{n-1} b_{in} \in (bar(A))_{00} \oplus (\bigoplus_{i=1}^{n-1} (bar(A))_{i0}) \subseteq R(bar(A))$$

Provamos assim, que R(bar(A)) é um ideal de A, logo $R(bar(A)) \subseteq R(A)$. Das duas inclusões resulta que R(bar(A)) = R(A), como queríamos.

Para avançarmos em nosso objetivo precisaremos estudar algumas propriedades válidas para as álgebras báricas arbitrárias (não necessariamente alternativas). Tais propriedades permitirão caracterizar o conceito essencial desta seção, o bar radical, que definiremos em breve.

Definição 2.3.1. Sejam (A, w), (B, γ) álgebras báricas $e \varphi: A \to B$ homomorfismo de álgebras tal que $\gamma \circ \varphi = w$.

- (i) φ é chamado homomorfismo bárico.
- (ii) Se φ for sobrejetor será chamado **epimorfismo bárico**.
- (iii) Se φ for bijetor dizemos que φ é um **isomorfismo bárico**. Neste caso, as álgebras báricas (A, w) e (B, γ) são ditas **isomorfas** e denotamos $(A, w) \cong_b (B, \gamma)$.

Definição 2.3.2. Um ideal I de uma álgebra bárica alternativa (A, w) é chamado ideal bárico de A se $I \subseteq bar(A)$

Definição 2.3.3. Sejam (A, w) uma álgebra bárica e B subálgebra de A tal que bar(B) é um ideal bilateral de A. Então B é chamada **subálgebra bárica normal**. Notação: $B \leq A$ ou $B \triangleleft A$, se $B \neq A$.

Lema 2.3.2. Sejam (A, w), (B, γ) álgebras báricas e $\varphi : A \to B$ um homomorfismo bárico. Então tem-se:

- (i) $ker \varphi \acute{e} um ideal b\'{a}rico de A;$
- (ii) Se $C \leq A$, então $\varphi(C) \leq B$ e $bar(\varphi(C)) = \varphi(bar(C))$;
- (iii) Se $C \triangleleft D \leq A$, então $\varphi(C) \triangleleft \varphi(D) \leq B$.

Demonstração:

(i) Basta mostrar que $\ker \varphi \subseteq bar(A)$. Seja $x \in \ker \varphi$. Então $\varphi(x) = 0$. Mas $w = \gamma \circ \varphi$, logo $w(x) = (\gamma \circ \varphi)(x) = \gamma(\varphi(x)) = \gamma(0) = 0 \implies x \in bar(A)$. Portanto $\ker \varphi \subseteq bar(A)$.

- (ii) É imediato que $\varphi(C) \leq B$. Mostremos que $bar(\varphi(C)) = \varphi(bar(C))$. Seja $x \in bar(\varphi(C))$. Então, como $\varphi(C)$ é subálgebra de B, temos $\gamma(x) = 0$, e ainda $x \in \varphi(C)$, donde $x = \varphi(c)$ para algum $c \in C$. Assim $0 = \gamma(x) = \gamma(\varphi(c)) = (\gamma \circ \varphi)(x) = w(c)$. Então $c \in bar(A)$ e $x = \varphi(c) \in \varphi(bar(C))$. Logo $bar(\varphi(C)) \subseteq \varphi(bar(C))$. Seja agora $x \in \varphi(bar(C))$. Existe $c \in bar(C)$ tal que $x = \varphi(c)$. Daí, $x \in \varphi(C)$ e $\gamma(x) = \gamma(\varphi(c)) = (\gamma \circ \varphi)(x) = w(c) = 0 \Rightarrow x \in bar(\varphi(C))$. Logo $\varphi(bar(C)) \subseteq bar(\varphi(C))$.
- (iii) Basta provar que $bar(\varphi(C))$ é um ideal bilateral de $bar(\varphi(D))$. Sejam $x \in bar(\varphi(D))$ e $y \in bar(\varphi(C))$. Então, por (ii), $x \in \varphi(bar(D))$ e $y \in \varphi(bar(C))$, e podemos escrever $x = \varphi(D)$, com $d \in bar(D)$ e $y = \varphi(C)$, com $c \in bar(C)$. Daí, $xy = \varphi(d)\varphi(c) = \varphi(dc)$. Mas como $C \leq D$, bar(C) é um ideal bilateral de bar(D), então $dc \in bar(C)$, logo $xy = \varphi(dc) \in \varphi(bar(C)) = bar(\varphi(C))$. Portanto $bar(\varphi(C))$ é ideal bilateral de $bar(\varphi(D))$.

Definição 2.3.4. Sejam (A, w) uma álgebra bárica $e B \subseteq A$.

- (i) $B \notin uma \ subálgebra \ bárica \ maximal \ (subálgebra \ bárica \ maximal \ normal)$ $de \ (A, w) \ se \ B < A \ (B \triangleleft A) \ e \ se \ C \le A \ (C \unlhd A) \ tal \ que \ B \subseteq C, \ então \ C = B$ $ou \ C = A$.
- (ii) $B \notin um \ ideal \ b\'{arico} \ maximal \ de \ (A, w) \ se \ B \notin um \ ideal \ b\'{arico} \ de \ (A, w), B \neq bar(A) \ e \ se \ J \notin um \ ideal \ b\'{arico} \ de \ (A, w) \ tal \ que \ B \subseteq J, \ ent\~{ao} \ J = B \ ou \ J = bar(A).$

Lema 2.3.3. Sejam (A, w) e (B, γ) álgebras báricas e $\varphi: A \to B$ um epimorfismo bárico. Então as seguintes condições são válidas:

- $\text{(i)} \ \ Se \ C \leq B, \ ent \tilde{ao} \ \varphi^{-1}(C) \leq A \ \ e \ bar(\varphi^{-1}(C)) = \varphi^{-1}(bar(C));$
- (ii) Se $C \le D \le B$, então $\varphi^{-1}(C) \le \varphi^{-1}(D) \le A$;
- (iii) Se $C \leq A$ ($C \leq A$) é maximal e $ker \varphi \subseteq C$, então $\varphi(C) \leq B$ ($\varphi(C) \leq B$) é maximal;
- (iv) Se C < B ($C \triangleleft B$) é maximal, então $\varphi^{-1}(C) < A$ ($\varphi^{-1}(C) \triangleleft A$) é maximal.

Demonstração:

- (i) É fácil ver que $\varphi^{-1}(C)$ é subálgebra de A. Agora, seja $x \in bar(\varphi^{-1}(C))$. Temos que $x \in \varphi^{-1}(C)$, logo $\varphi(x) \in C$. Além disso, w(x) = 0. Escrevemos então: $0 = w(x) = (\gamma \circ \varphi)(x) = \gamma(\varphi(x)) \implies \varphi(x) \in bar(C)$ e $x \in \varphi^{-1}(bar(C))$. Logo $bar(\varphi^{-1}(C)) \subseteq \varphi^{-1}(bar(C))$. Seja agora $x \in \varphi^{-1}(bar(C))$. Então existe $c \in bar(C)$ tal que $\varphi(x) = c$. Mas se $c \in bar(C)$, então $\gamma(c) = 0$ e escrevemos: $0 = \gamma(c) = \gamma(\varphi(x)) = (\gamma \circ \varphi)(x) = w(x)$. Assim, $x \in bar(\varphi^{-1}(bar(C)))$. Logo, pela primeira inclusão, $x \in \varphi^{-1}(bar(bar(C))) = \varphi^{-1}(bar(C))$.
- (ii) Devemos mostrar que $bar(\varphi^{-1}(C))$ é ideal bilateral de $bar(\varphi^{-1}(D))$. Tomemos $a \in bar(\varphi^{-1}(C))$ e $b \in bar(\varphi^{-1}(D))$. Então, por (i), $a \in \varphi^{-1}(bar(C))$ e $b \in \varphi^{-1}(bar(D))$, donde $\varphi(a) \in bar(C)$, $\varphi(b) \in bar(D) \Rightarrow \varphi(a)\varphi(b) = \varphi(ab) \in bar(D)$, pois $C \leq D$. Logo $ab \in \varphi^{-1}(bar(D)) \stackrel{(i)}{=} bar(\varphi^{-1}(D))$. De maneira análoga chegamos a $ba \in bar(\varphi^{-1}(D))$.
- (iii) Por 2.3.2 (ii) temos que $\varphi(C) \leq B$. Devemos mostrar que $\varphi(C) < B$, isto é, $\varphi(C) \neq B$. Supondo que $\varphi(C) = B$, teremos $C = \varphi^{-1}(\varphi(C)) = \varphi^{-1}(B) = A$, contradição, pois C < A. Para mostrar que $\varphi(C)$ é maximal, seja $D \leq A$ tal que $\varphi(C) \subseteq D$. Então, por (ii), $\varphi^{-1}(\varphi(C)) \leq \varphi^{-1}(D) \leq A$ ou $C \leq \varphi^{-1}(D) \leq A$. Mas como C é maximal, devemos ter $\varphi^{-1}(D) = C$ ou $\varphi^{-1}(D) = A$. Daí, $D = \varphi(C)$ ou $D = \varphi(A) = B$. Portanto $\varphi(C)$ é maximal. O caso $C \leq A \Rightarrow \varphi(C) \leq B$ é maximal, se prova de modo análogo.
- (iv) Por 2.3.2 (ii) temos que $\varphi(C) \leq A$. Se $\varphi^{-1}(C) = A$, então $C = \varphi(\varphi^{-1}(C)) = \varphi(A) = B$, contradição, pois C < B. Seja agora $D \leq A$ tal que $\varphi^{-1}(C) \subseteq D$. Então $C \subseteq \varphi(D)$ e por 2.3.2 (ii), $\varphi(D) \leq B$. Daí, $C \subseteq \varphi(D) \leq B$, mas sendo C maximal, segue que $\varphi(D) = C$ ou $\varphi(D) = B$. Logo, $D = \varphi^{-1}(C)$ ou $D = \varphi^{-1}(B) = A$, o que significa que $\varphi^{-1}(C)$ é maximal. O caso $C \leq B \Rightarrow \varphi^{-1}(C) \leq A$ é maximal, se prova de modo análogo. \square

Lema 2.3.4. Sejam A_1 e A_2 subálgebras báricas de uma álgebra bárica (A, w). Então $A_1 = A_2$ se e somente se $A_1 \subseteq A_2$ e $bar(A_1) \supseteq bar(A_2)$

Demonstração: A parte somente se é imediata. Agora, note que $A_1 \subseteq A_2 \Rightarrow bar(A_1) \subseteq bar(A_2)$ e como, por hipótese, $bar(A_1) \supseteq bar(A_2)$, resulta $bar(A_1) = bar(A_2)$. Daí: $A_1 = Fa \oplus bar(A_1) = Fa \oplus bar(A_2) = A_2$, $\forall a \in A, w(a) = 1$.

A próxima proposição corresponde a um dos conhecidos teoremas do homomorfismo de álgebras, válidos naturalmente para álgebras báricas. A demonstração se faz do modo usual e será aqui omitida.

Proposição 2.3.5. Sejam B uma subálgebra de uma álgebra bárica (A, w) e I um ideal bárico de A. Então $B+I \leq A$, I é um ideal bárico de B+I e $\frac{B+I}{I} \cong_b \frac{B}{I \cap B}$.

Lema 2.3.6. Sejam (A, w) uma álgebra bárica e $B \leq A$. Então B é maximal se e somente se bar(B) é um ideal bárico maximal de (A, w).

Demonstração: (\Rightarrow) Seja $B \triangleleft A$ maximal $(B \neq A)$. Quero mostrar que bar(B) é um ideal bárico maximal de A. Seja então D um ideal bárico de A tal que $bar(D) \subseteq D \subseteq bar(A)$. Seja $b \in B$ tal que w(b) = 1. Sabemos que $B = Fb \oplus bar(A)$. Fazendo $C = Fb \oplus D$, segue que D = bar(C), que é ideal bárico de A, donde $C \unlhd A$. Temos ainda: $B \subseteq C \subseteq A$, e como B é maximal, C = B ou C = A. Daí, bar(C) = bar(B) ou bar(C) = bar(A) e portanto D = bar(B) ou D = bar(A).

(⇐) Suponhamos agora que bar(B) é um ideal bárico maximal de A. Seja $C \le A$ tal que $B \subseteq C$. Assim: $bar(B) \subseteq bar(C) \subseteq bar(A)$, e como bar(B) é maximal, resulta que bar(C) = bar(B) ou bar(C) = bar(A). Então, por 2.3.4 devemos ter C = B ou C = A, o que indica que B é maximal.

Definição 2.3.5. Uma álgebra bárica (A, w) é **simples** se para todas $B \subseteq A$, tivermos bar(B) = 0 ou bar(B) = bar(A).

Lema 2.3.7. Sejam (A, w) uma álgebra bárica e $B \leq A$. Então B é maximal se e somente se A/bar(B) é simples.

Demonstração: Seja $\varphi: A \to A/bar(B)$ o epimorfismo bárico dado por $\varphi(a) = a + bar(B)$. Seja $B \triangleleft A$ maximal. Então, se $C \unlhd A/bar(B)$, por 2.3.3, temos:

$$\varphi^{-1}(C) \leq \varphi^{-1}(A/bar(B)) = A. \quad \text{E tamb\'em } bar(B) \subseteq bar(\varphi^{-1}(C)). \quad \text{De fato,}$$

$$b \in bar(B) \ \Rightarrow \ \varphi(B) = b + bar(B) = 0 \in C \ \Rightarrow \ b \in \varphi^{-1}(C) \stackrel{w(b)=0}{\Rightarrow} b \in bar(\varphi^{-1}(C)).$$

$$\Rightarrow bar(B) \subseteq bar(\varphi^{-1}(C))$$

Mas, pelo Lema 2.3.6, sendo $B \triangleleft A$ maximal, bar(B) é um ideal bárico maximal de bar(A). Portanto:

$$bar(\varphi^{-1}(C)) = bar(B)$$
 ou $bar(\varphi^{-1}(C)) = bar(A)$ (I)

Mas, podemos escrever $C = \varphi^{-1}(C)/bar(B)$. Então:

$$bar(C) = bar(\varphi^{-1}(C)/bar(B)) \Rightarrow bar(C) = bar(\varphi^{-1}(C))/bar(B)$$

Por (I) temos:
$$bar(C) = bar(B)/bar(B) = 0$$
 ou $bar(C) = bar(A)/bar(B) = bar(A/bar(B))$

Reciprocamente, seja A/bar(B) simples. Se existe $C \leq A$ tal que $B \subseteq C$ então, pelo Lema 2.3.2, $\varphi(C) \leq A/bar(B)$. Mas, sendo A/bar(B) simples, devemos ter $bar(\varphi(C)) = 0$ ou $bar(\varphi(C)) = bar(A/bar(B))$. Novamente, por 2.3.2, $bar(\varphi(C)) = \varphi(bar(C))$. Logo:

$$bar(B) = \varphi^{-1}(0) = bar(C)$$
 ou
$$bar(C) = \varphi^{-1}(bar(A/bar(B))) = bar(\varphi^{-1}(A/bar(B))) = bar(A).$$

Definição 2.3.6. O bar radical de uma álgebra bárica alternativa (A, w) é a intersecção de todos bar(B), onde $B \triangleleft A$ é maximal. Notação: $R_B(A)$.

Lema 2.3.8. Sejam (A, w) uma álgebra bárica e I um ideal bárico de A. Então são válidas:

- (i) $R_B(A/I) = \bigcap bar(B)/I$, onde $B \triangleleft A$ é maximal e $I \subseteq B$;
- (ii) $(R_B(A) + I)/I \subseteq R_B(A/I)$;
- (iii) Se $I \subseteq R_B(A)$, então $R_B(A/I) = R_B(A)/I$.

Demonstração:

- (i) Seja $\varphi: A \to A/I$, $\varphi(a) = a + I$, epimorfismo bárico. Por definição, $R_B(A/I)$ é a intersecção de bar(C), onde $C \subseteq A/I$ é maximal. Seja $B \triangleleft A$, maximal e com $I \subseteq B$. Podemos fazer o quociente B/I e, é claro que $\varphi(B) = B/I$. Pelo Lema 2.3.3, $\varphi(B) = B/I \subseteq A/I$ e é maximal. Portanto $R_B(A/I) \subseteq \bigcap bar(B/I)$. Seja agora, $B' \triangleleft A/I$ maximal. Então, pelo Lema 2.3.3, $\varphi^{-1}(B') \subseteq \varphi^{-1}(A/I) = A$.
- (ii) Se $B \triangleleft A$ é maximal e $I \subseteq B$, então $R_B(A) + I \subseteq B$. Logo $R_B(A) + I \subseteq A$ for $A \in A$ is maximal e $A \in A$. Logo $A \in A$ is maximal e $A \in A$. Log

(iii) Se
$$I \subseteq R_B(A)$$
, então $I \subseteq B$, $\forall B \triangleleft A$ maximal. Então, por (i), $R_B(A/I) = R_B(A)/I$.

Lema 2.3.9. Sejam (A, w) uma álgebra bárica e $B \subseteq A$. Então $R_B(B) \subseteq R_B(A) \cap B$.

Demonstração: Tomemos $C \triangleleft A$ maximal. Se $bar(B) \subseteq bar(C)$, então $R_B(B) \subseteq B \cap bar(C)$. De fato, $R_B(B) \subseteq bar(B) = B \cap bar(B) \subseteq B \cap bar(C)$.

Agora, se $bar(B) \nsubseteq bar(C)$, então $bar(B) \nsubseteq C$, logo $C \subset C + bar(B)$. Mas C é maximal, portanto A = C + bar(B).

Seja $x \in B$. Como $B \subseteq A$, $x \in A$. Logo posso escrever x = c + b, onde $c \in C$ e $b \in bar(B)$. Daí, $c = x - b \Rightarrow c \in B \Rightarrow c \in B \cap C$. Com isto $x \in B \cap C + bar(B)$, o que resulta em: $B \subseteq B \cap C + bar(B)$. Como a inclusão contrária é óbvia, obtemos: $B = B \cap C + bar(B)$.

Tomamos agora $b \in B \cap C$ tal que w(b) = 1 e escrevemos: C = Fb + bar(C) e também B = Fb + bar(B). Mas

$$A = C + bar(B) = Fb + bar(C) + bar(B) \Rightarrow A = B + bar(C)$$
. Então:

$$\frac{A}{bar(C)} = \frac{B + bar(C)}{barC} \stackrel{(*)}{\approx}_{b} \frac{B}{bar(C) \cap B} = \frac{B}{bar(C \cap B)}$$

(*) Prop. 2.3.5

Como $C \triangleleft A$ é maximal, pelo Lema 2.3.7, A/bar(C) é simples, daí, pelo isomorfismo indicado acima, também $B \cap C \triangleleft B$ é maximal. Temos ainda: $R_B(B) \subseteq bar(B \cap C) = B \cap bar(C)$. Como C é arbitrária, esta inclusão vale para toda subálgebra maximal de A. Então:

$$R_B(B) \subseteq \bigcap_{C \triangleleft A} (B \cap bar(C)) = B \cap \left(\bigcap_{C \triangleleft A} bar(C)\right) = B \cap R_B(A)$$

Proposição 2.3.10. Sejam (A, w) álgebra bárica e B, subálgebra bárica normal de A tal que $R_B(A/bar(B)) = 0$. Então $R_B(B) \subseteq R_B(A) \subseteq B$.

Demonstração: Lembrando que bar(B) é um ideal bárico de A, podemos aplicar o Lema 2.3.8 (ii), obtendo:

$$(R_B(A) + bar(B))/bar(B) \subseteq R_B(A/bar(B)) = 0 \Rightarrow R_B(A) \subseteq bar(B) \subseteq B.$$

Assim,
$$R_B(A) \cap B = R_B(A)$$
 e, pelo Lema 2.3.9, $R_B(B) \subseteq R_B(A)$

Definição 2.3.7. Seja (A, w) uma álgebra bárica alternativa tal que $R_B(A) = 0$. Dizemos que (A, w) é semisimples no sentido bárico ou b-semisimples.

Definição 2.3.8. Seja (A, w) uma álgebra bárica alternativa e I um ideal bárico de A. Se I for simples, dizemos que I é um **ideal b-simples**.

A estrutura das álgebras báricas b-semisimples, semelhantemente às álgebras semisimples, é dada como uma soma direta de ideais b-simples. O teorema a seguir explicita tal resultado. Omitiremos sua demonstração, que pode ser encontrada em [7].

Teorema 2.3.11. Seja (A, w) álgebra bárica de dimensão finita. Então A é b-semisimples se e somente se bar(A) é soma direta de ideais b-simples.

Lema 2.3.12. Seja (A, w) álgebra bárica alternativa e R(A) o radical de A. Se R(A) = 0, então $R_B(A) = 0$.

Demonstração: Se R(A)=0, sabemos que $A=G_1\oplus\cdots\oplus G_k$, com os G_i ideais simples. Cada G_i tem um elemento identidade e_i e $G_i=e_iA$. Para cada e_i tem-se $w(e_i)=0$ ou $w(e_i)=1$. Mas necessariamente, para algum $i,w(e_i)=1$, caso contrário $G_i\subseteq bar(A)$ e A não seria uma álgebra bárica. Supondo sem perda de generalidade que $w(e_1)=1$, temos que $w(e_j)=0$ para $1< j\leq k$. Assim $G_j\subseteq bar(A)$, se $1< j\leq k$. Já vimos que $G_1=Fe_1\oplus bar(G_1)$. Mas $bar(G_1)$ é um ideal de A, e $bar(G_1)\subseteq G_1$. Como G_1 é simples, segue que $bar(G_1)=0$. Assim: $A=Fe_1\oplus G_2\oplus\cdots\oplus G_k$ ou $A=Fe_1\oplus bar(A)$. Portanto, pelo Teorema 2.3.11, $R_B(A)=0$.

Teorema 2.3.13. Seja (A, w) álgebra bárica alternativa. Então $R_B(A) \subseteq R(A)$.

Demonstração: Por definição, $R_B(A) = \bigcap_{B \triangleleft A} bar(B)$. Claramente, $R_B(A) \subseteq bar(A)$. Se bar(A) = R(A), então $R_B(A) \subseteq R(A)$. Se $bar(A) \neq R(A)$, consideramos a subálgebra P dada por $P = Fe \oplus R(A)$, onde e é um idempotente de peso 1 de A (existe e pelo Corolário 1.4.6). P é normal, pois bar(P) = R(A) é ideal de A. Como, pelo Lema 2.1.17, R(A/R(A)) = 0 segue, pelo Lema 2.3.12, que $R_B(A/R(A)) = 0$. Podemos então aplicar a Proposição 2.3.10, com R(A) no lugar de R0, e chegamos a $R_B(A) \subseteq R(A)$.

Proposição 2.3.14. Seja (A, w) álgebra bárica, com $bar(A) = I_1 \oplus \cdots \oplus I_k$, com os I_i ideais báricos simples. Se J é qualquer ideal bárico de A, então: J = 0 ou $J = I_{j_1} \oplus \cdots \oplus I_{j_l}$, $1 \leq j_i \leq k$.

Demonstração: Seja J ideal bárico de A. Então $J \subseteq bar(A)$ e, se $j \in J$ podemos escrever $j = i_1 + \cdots + i_k$, com $i_l \in I_l$, $1 \le l \le k$ (podendo algum i_l ser zero). Consideremos o seguinte conjunto:

$$J_l = \{i_l \in I_l \text{ tal que } i_l \text{ \'e somando de algum } j \in J\}$$

Mostremos que J_l é um ideal de A. Seja $x \in A$. Provemos que $i_l x, xi_l \in J_l, \forall i_l \in J_l$. Tomemos $i_l \in J_l$ arbitrário. Então existe $j \in J$ tal que i_l é um somando de j. Como J é ideal, $xj, jx \in J$. E como I_l é ideal, $xi_l, i_lx \in I_l$. Mas $xi_l \in I_l$ e é somando de $xj \in J$. Logo $xi_l \in I_l$. Analogamente temos $i_l \in J_l$. Portanto J_l é um ideal de A. Cada $J_l \subseteq I_l$, logo $J_l = 0$ ou $J_l = I_l$, pois I_l é um ideal simples. E como $J \subseteq J_1 \oplus \cdots \oplus J_j, 1 \leq j \leq k$, segue que $J = I_1 \oplus \cdots \oplus I_j$.

Proposição 2.3.15. Sejam (A, w) álgebra bárica alternativa e I um ideal b-simples de A. Então $I^2 = I$ ou $I^2 = 0$.

Demonstração: Como $I^2 \subseteq I$, e I é um ideal simples, basta provar que I^2 é um ideal de A. Tomamos $x \in A$ e $y = ab \in I^2$ $(a, b \in I)$

$$x(ab) = (xa)b - (x, a, b) = (xa)b = (b, x, a) = (xa)b - (bx)a + b(xa) \in I^2$$

$$(ab)x = (a,b,x) + a(bx) = -(a,x,b) + a(bx) = a(xb) - (ax)b + a(bx) \in I^2$$

Portanto, I^2 é um ideal de A.

Lema 2.3.16. Seja (A, w) uma álgebra bárica alternativa b-semisimples. Então A pode ser escrita:

$$A = Fe \oplus R_1 \oplus \cdots \oplus R_m \oplus I_1 \oplus \cdots \oplus I_p$$

onde os ideais b-simples R_i e I_j satisfazem $R_i^2 = 0$ e $I_j^2 = I_j$, $1 \le i \le m$ e $1 \le j \le p$.

Demonstração: É conseqüência direta do Teorema 2.3.11 e da Proposição 2.3.15.

Proposição 2.3.17. Com as mesmas hipóteses do lema anterior, a subálgebra bárica alternativa $A' = Fe \oplus I_1 \oplus \cdots \oplus I_p$ é semisimples, isto é, R(A') = 0 e existe um idempotente $e_1 \in A$ com $w(e_1) = 1$ e tal que $e_1I_l = I_le_1 = 0$, $1 \le l \le p$.

Demonstração: Seja $x \in R(A')$. Então x é propriamente nilpotente em A'. Então, para todo $y \in R(A) = R_1 \oplus \cdots \oplus R_m$, xy = 0. Assim, x é propriamente nilpotente em A, pois $A = A' \oplus R(A)$. Logo $R(A') \subset R(A)$, daí $R(A') \subset R(A) \cap A' = \{0\}$. Portanto A' é semisimples.

Pelo Teorema 2.1.16, A' pode ser escrita como soma direta de ideais simples: $A' = G_1 \oplus \cdots \oplus G_r$, onde cada G_i é ideal simples (i = 1, ..., r). O idempotente $e \in A'$ pode ser escrito: $e = e_1 + \cdots + e_r$, onde cada $e_i \in G_i$ é idempotente. Como e tem peso 1, somente um dos e_i tem peso 1, e os outros têm peso 0. Suponhamos que $w(e_1) = 1$.

 $bar(G_1)$ é um ideal de G_1 , logo é também ideal de A. Como G_1 é simples, então $bar(G_1) = G_1$ ou $bar(G_1) = 0$. Mas $e_1 \in G_1$ tem peso 1, logo $bar(G_1) = 0$. Assim $G_1 = Fe_1$. Escrevemos então:

 $A'=Fe_1\oplus G_2\oplus \cdots \oplus G_r$. Como a soma é direta, temos que $e_1G_i=G_ie_1=0$, para $2\leq i\leq r$.

Por hipótese, $A' = Fe_1 \oplus I_1 \oplus \cdots \oplus I_p$. Comparando as duas decomposições de A' temos:

$$G_2 \oplus \cdots \oplus G_r = I_1 \oplus \cdots \oplus I_p$$

Cada G_i é um ideal bárico de A', pois $G_i \subseteq bar(A')$, logo, de acordo com a Proposição 2.3.14, G_i é uma soma dos ideais I_l . Mas os ideais I_l são simples, logo cada G_i é igual a um certo I_l . Portanto $e_1I_l = I_le_1 = 0$.

Vamos procurar uma relação mais explícita entre $R_B(A)$ e R(A). Veremos que, o bar(A) representa um papel importante neste caso.

Teorema 2.3.18. Seja (A, w) álgebra bárica alternativa. Então

$$R_B(A) = bar(A)^2 \cap R(A)$$

Demonstração: Mostremos primeiro que $R_B(A) \subseteq bar(A)^2 \cap R(A)$. Já sabemos que $R_B(A) \subseteq R(A)$, portanto basta mostrar que $R_B(A) \subseteq bar(A)^2$. Para isto consideremos a decomposição de Peirce de A em relação a um idempotente $e \in A$.

$$A = Fe \oplus bar(A) = Fe \oplus bar(A)_{11} \oplus bar(A)_{10} \oplus bar(A)_{01} \oplus bar(A)_{00}$$

Como $bar(A) \subseteq bar(A)^2$ podemos escrever esta decomposição em termos de subespaços $X_{ij} \subseteq bar(A)_{ij}$, da seguinte forma:

$$A = Fe \oplus bar(A)^2 \oplus X_{11} \oplus X_{10} \oplus X_{01} \oplus X_{00}$$

Sejam Y_{ij} bases dos subespaços X_{ij} e tomemos o seguinte conjunto:

$$J_z = bar(A)^2 + \langle Y_{11} \cup Y_{10} \cup Y_{01} \cup Y_{00} \setminus \{z\} \rangle$$

onde $z \in Y_{11} \cup Y_{10} \cup Y_{01} \cup Y_{00}$.

Vamos mostrar que J_z é um ideal bárico maximal de A. Em primeiro lugar provemos que J_z é um ideal. Daí segue que J_z é bárico, uma vez que $J_z \subseteq bar(A)$. Sejam $a \in A$ e $j \in J_z$. Se $a \in bar(A), aj_z, j_z a \in bar(A)^2$, logo $aj_z, j_a z \in J_z$. Resta mostrar que $ej_z, j_z e \in J_z$.

Um elemento genérico $x \in bar(A)^2$ pode ser escrito como $x = \sum a_i b_i$, com $a_i, b_i \in bar(A)$. Então se $j_z \in J_z$, podemos escrever:

$$j_z = \sum a_i b_i + a_{11} + a_{10} + a_{01} + a_{00}$$
, onde $a_{ij} \in Y_{ij}$

$$ej_z = \sum e(a_ib_i) + ea_{11} + ea_{10} + ea_{01} + ea_{00} = \sum e(a_ib_i) + a_{11} + a_{10}$$

Mas, a parcela $\sum e(a_ib_i)$ está em $bar(A)^2$, como podemos verificar, calculando:

$$e(a_ib_i) = (ea_i)b_i - (e, a_i, b_i) = (ea_i)b_i + (a_i, e, b_i)$$

= $(ea_i)b_i + (a_ie)b_i - a_i(eb_i) \in bar(A)^2$

Como a codimensão de J_z é 1, segue que J_z é maximal. Sendo isto válido para todo $z \in Y_{11} \cup Y_{10} \cup Y_{01} \cup Y_{00}$ temos:

$$R_B(A) \subseteq \bigcap_z J_z = bar(A)^2$$

Então:
$$R_B(A) \subseteq bar(A)^2 \implies R_B(A) \subseteq bar(A)^2 \cap R(A)$$

Devemos mostrar agora que $bar(A)^2 \cap R(A) \subseteq R_B(A)$. Para isto vamos considerar a álgebra quociente $A/R_B(A)$. Já vimos que $R_B(A/R_B(A)) = 0$, isto é $A/R_B(A)$ é semisimples no sentido bárico. Sendo assim, ela pode ser escrita como soma direta de ideais báricos simples. Em particular:

$$bar(A/R_B(A)) = I_1 \oplus \cdots \oplus I_r \oplus J_1 \oplus \cdots \oplus J_s$$

onde
$$I_i^2 = I_i$$
, $(1 \le i \le r)$, e $J_i^2 = 0$, $(1 \le j \le s)$.

Notemos agora que $bar(A/R_B(A))^2 = I_1 \oplus \cdots \oplus I_r$. De fato:

$$bar(A/R_B(A))^2 = bar(A/R_B(A)).bar(A/R_B(A))$$

$$= (I_1 \oplus \cdots \oplus I_r \oplus J_1 \oplus \cdots \oplus J_s).(I_1 \oplus \cdots \oplus I_r \oplus J_1 \oplus \cdots \oplus J_s)$$

$$= I_1^2 \oplus \cdots \oplus I_r^2 \oplus J_1^2 \oplus \cdots \oplus J_s^2$$

$$= I_1^2 \oplus \cdots \oplus I_r^2 \oplus 0 \oplus \cdots \oplus 0$$

$$= I_1 \oplus \cdots \oplus I_r$$

Então, pela Proposição 2.3.17 $bar(A/R_B(A))^2$ é semisimples no sentido usual, isto é, $R(bar(A/R_B(A))^2) = 0$.

Mas $bar(A/R_B(A))^2 \cong bar(A)^2/(bar(A)^2 \cap R_B(A))$. De fato:

$$bar(A/R_B(A))^2 \cong bar(A)^2/R_B(A)^2 = bar(A)^2/R_B(A)$$
$$= bar(A)^2/(R_B(A) \cap bar(A)^2).$$

Esta última igualdade resulta do fato que $R_B(A) \subseteq bar(A)^2$, como vimos há pouco, logo $R_B(A) \cap bar(A)^2 = R_B(A)$. Então:

$$0 = R(bar(A/R_B(A))^2) = R(bar(A)^2)/R(R_B(A) \cap bar(A)^2)$$
$$= R(bar(A)^2)/R(R_B(A)) = R(bar(A)^2)/R_B(A)$$
$$= R(bar(A)^2)/R_B(A) \cap bar(A)^2$$

Logo
$$R(bar(A)^2) \subseteq R_B(A) \cap bar(A)^2 = R_B(A)$$
 ou

$$R(bar(A)^2) \subseteq R_B(A)$$

Lembrando, estamos querendo mostrar que $R(A) \cap bar(A)^2 \subseteq R_B(A)$. Mas, é claro que $R(A) \cap bar(A)^2 \subseteq bar(A)^2$. E também, $R(A) \cap bar(A)^2 \subseteq R(A)$, donde $R(A) \cap bar(A)^2$ é um ideal nil. Estando contido em $bar(A)^2$, deve estar contido no radical de $bar(A)^2$. Assim: $R(A) \cap bar(A)^2 \subseteq R(bar(A)^2)$. E, como acabamos de verificar, $R(bar(A)^2) \subseteq R_B(A)$, segue que $R(A) \cap bar(A)^2 \subseteq R_B(A)$, completando a demonstração do teorema.

Corolário 2.3.19. Seja (A, w) álgebra bárica alternativa. Então bar(A) é nilpotente se e somente se $R_B(A) = R(A)^2$.

Demonstração: (\Rightarrow) Se bar(A) é nilpotente então bar(A) = R(A), pois $R(A) \subseteq bar(A)$ e R(A) é o ideal nilpotente maximal de A. Logo

$$R(A) \cap bar(A)^2 = R(A) \cap R(A)^2 = R(A)^2$$
, pois $R(A)^2 \subseteq R(A)$

Como $R(A) \cap bar(A)^2 = R_B(A)$ segue que $R(A)^2 = R_B(A)$.

$$(\Leftarrow)$$
 Se $R_B(A) = R(A)^2$, temos $R(A) \cap bar(A)^2 = R(A)^2$, isto é,

$$R(A) \cap bar(A)^2 \subseteq R(A)$$
.

Logo bar(A) é nilpotente.

Capítulo 3

Álgebras de Composição

O objetivo deste capítulo é apresentar as principais propriedades das chamadas álgebras de Cayley-Dickson sobre as quais estudaremos algumas identidades no próximo capítulo. A relevância deste estudo reside no fato de que a descoberta destas álgebras, bem como a das álgebras dos quatérnios marcou um passo importante no desenvolvimento da Matemática a partir do século XIX. Foram os quatérnios, álgebras de dimensão 4 descobertos em 1843 por Hamilton, que constituíram o primeiro exemplo de anel com divisão não comutativo. Na mesma época surgiram os octônios (generalizados depois nas álgebras de Cayley-Dickson), de dimensão 8, onde não valia a propriedade associativa.

Intimamente relacionado a estas descobertas está um interessante problema numérico que foi objeto de estudo de matemáticos como Euler e Lagrange. Trata-se do "problema da soma dos quadrados", que pode ser enunciado como:

O produto de somas de n quadrados é ainda uma soma de n quadrados

Para n = 1 temos a identidade trivial

$$x^2y^2 = (xy)^2.$$

Para n=2, temos a expressão:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

Se considerarmos os números complexos $z = x_1 + ix_2$ e $z' = y_1 + iy_2$, a expressão acima corresponde à propriedade dos módulos |zz'| = |z||z'|.

A identidade para n=4 já era do conhecimento de Euler e Lagrange. E em 1818, C. F. Digen encontrou a identidade para n=8. Mas foi somente em 1898 que Hurwitz mostrou que tais identidades existem apenas para n=1,2,4,8.

O "Problema de Hurwitz" (isto \acute{e} , a procura dos valores de n para os quais existem as identidades mencionadas), pode ser expresso matematicamente da seguinte forma:

$$\left(\sum_{i=1}^n x_i^2\right) \left(\sum_{i=1}^n y_i^2\right) = \left(\sum_{i=1}^n z_i^2\right),\,$$

onde z_i tem a forma

$$z_i = \sum_{j,k=1}^n a_{ijk} x_j y_k,$$

com a_{ijk} números complexos.

Veremos também neste capítulo como se dá a relação das álgebras de composição com o problema numérico estudado por Hurwitz, em que, da mesma forma que só existem 4 valores de n para o problema da soma de quadrados, são igualmente 4 o número de álgebras de composição existentes, a menos de isomorfismos.

Para resultados mais gerais, pode-se usar a abordagem com representação de grupos, conforme esboçado no exemplo 4 da página 49. Maiores detalhes podem ser encontrados em [11].

3.1 A descoberta dos quatérnios

Por volta de 1830, William Rowen Hamilton (1805-1865) estabeleceu a fundamentação teórica para os números complexos, representando-os como pares ordenados de números reais. Além da forma usual a+bi, passou-se a utilizar também a forma (a,b). Foram definidas as regras das operações de soma e multiplicação de números complexos, que passaram a ser uma ferramenta algébrica importante para se trabalhar com vetores no plano.

Interessava a Hamilton estender as operações e propriedades dos pares ordenados para as ternas ordenadas, de modo a permitir uma aplicação a vetores no espaço. A multiplicação de números complexos tal como formulada por Hamilton e, até hoje em uso, é dada por:

$$(a,b)(c,d) = (ac - bd, ad + bc),$$

ou, na forma algébrica

$$(a+bi)(c+di) = ac - bd + (ad+bc)i.$$

Estendendo este raciocínio, Hamilton tentou definir a multiplicação de ternas de números (a + bi + cj)(d + ei + fj) de tal forma que o resultado também fosse escrito da mesma forma (na linguagem atual, como uma combinação linear de $1, i \in j$). Mas apareciam os termos ij e ji que não permitiam obter um produto como desejado.

Hamilton também queria preservar para as ternas, a lei dos módulos, válida nos complexos, segundo a qual "o módulo do produto de dois complexos é igual ao produto dos módulos", simbolicamente: $|z_1z_2| = |z_1||z_2|$. Supondo que o produto obtido tivesse a forma dos fatores originais, digamos x + yi + zj, esta igualdade seria escrita:

$$(a^2 + b^2 + c^2)(d^2 + e^2 + f^2) = x^2 + y^2 + z^2,$$

que nada mais é do que o problema da soma de quadrados para n=3, o qual sabemos hoje, não tem solução.

Após cerca de dez anos de pesquisas, Hamilton percebeu a necessidade de introduzir um novo símbolo, a que chamou k, tendo descoberto afinal a relação fundamental entre eles:

$$i^2 = j^2 = k^2 = -1,$$

 $ijk = -1.$

Destas identidades foram deduzidas as diversas multiplicações entre os símbolos: Multiplicando a segunda igualdade por k à direita:

$$ijk^2 = -k \Rightarrow ij = k.$$

Multiplicando por i à esquerda:

$$i^2 jk = -i \Rightarrow jk = i.$$

Procedendo de maneira análoga se chega a:

$$ki = j,$$
 $ji = -k,$ $ik = -j,$ $kj = -i.$

Hamilton também percebeu que este problema se relacionava com o problema de Hurwitz, mostrando que a existência de uma identidade para a soma de n quadrados era equivalente à existência de uma álgebra de divisão de dimensão n sobre os reais. Maiores detalhes podem ser encontrados em [16].

3.2 As Álgebras de Composição

Definição 3.2.1. Seja A um espaço vetorial sobre um corpo arbitrário F, com $carF \neq 2$. Uma **forma bilinear** é uma aplicação $f: A \times A \rightarrow F$ que, para todos $x, x', y, y' \in A$, $\alpha \in F$, satisfaz:

- (1) f(x + x', y) = f(x, y) + f(x', y);
- (2) f(x, y + y') = f(x, y) + f(x, y');
- (3) $f(\alpha x, y) = f(x, \alpha y) = \alpha f(x, y)$.

Uma forma bilinear é dita **simétrica** se f(x,y) = f(y,x), para todos $x,y \in A$, e **anti-simétrica** se f(x,y) = -f(y,x), para todos $x,y \in A$.

Definição 3.2.2. Seja A uma álgebra sobre um corpo arbitrário F. Uma aplicação $q:A\to F$ é chamada uma **forma quadrática** se satisfizer:

- (1) $q(\alpha x) = \alpha^2 q(x)$, para todo $\alpha \in F$ e todo $x \in A$;
- (2) a função f(x,y) = q(x+y) q(x) q(y) é uma forma bilinear em A.

Dizemos que uma forma quadrática **admite composição** se existir uma operação binária bilinear xy em A tal que q(x)q(y) = q(xy).

Uma forma quadrática é dita **não degenerada** se $q(x) = 0 \Leftrightarrow x = 0$.

A álgebra A está munida de uma forma quadrática não degenerada que admite composição. Vamos verificar que é possível definir um produto em A de tal forma que exista uma unidade em A.

Lema 3.2.1. Seja A uma álgebra de dimensão finita munida de uma forma quadrática não degenerada q que admite composição. Então existe um novo produto x * y em A tal que A é uma álgebra com 1.

Demonstração: Como q é não degenerada, existe $v \in A$ tal que $q(v) \neq 0$. Seja $u = v^2/q(v)$. Então q(u) = 1, logo q(xu) = q(ux) = q(x). Consideremos os operadores multiplicativos à direita R_u e à esquerda L_u , dados por

$$x \mapsto R_u(x) = xu \ e \ x \mapsto L_u(x) = ux.$$

Pelo fato de q ser não degenerada e A ter dimensão finita, os operadores R_u e L_u são invertíveis. Assim, definimos o seguinte produto:

$$x * y = (R_u^{-1}(x))(L_u^{-1}(y))$$

Como
$$q$$
 admite composição: $q(x * y) = q((R_u^{-1}(x))(L_u^{-1}(y)))$
= $q(R_u^{-1}(x))q(L_u^{-1}(y))$ (1)

Mas, notando que: $q(R_u^{-1}(x)) = q((R_u^{-1}(x)u)) = q(R_uR_u^{-1}(x)) = q(x)$ E também: $q(L_u^{-1}(y)) = q(uL_u^{-1}(y)) = q(L_uL_u^{-1}(y)) = q(y)$

Teremos, em (1): q(x * y) = q(x)q(y)

Temos também: $L_u^{-1}(u^2) = L_u^{-1}(L_u(u)) = u$ e $R_u^{-1}(u^2) = R_u^{-1}(R_u(u)) = u$ Resulta então: $x * u^2 = (R_u^{-1}(x))(L_u^{-1}(u^2)) = R_u^{-1}(x)u = R_u(R_u^{-1}(x)) = x$ E ainda: $u^2 * x = (R_u^{-1}(u^2))(L_u^{-1}(x)) = uL_u^{-1}(x) = L_u(L_u^{-1}(x)) = x$

Logo u^2 é a unidade de A em relação à multiplicação *.

Definição 3.2.3. Uma álgebra A com unidade, sobre um corpo F e munida de uma forma quadrática não degenerada q que admite composição em relação ao produto da álgebra é chamada **álgebra de composição**.

Lema 3.2.2 (Propriedades). Sejam A uma álgebra de composição sobre um corpo F ($carF \neq 2$), q(x) uma forma quadrática não degenerada sobre A e f(x,y) a forma bilinear simétrica associada a q(x). Valem as sequintes propriedades:

- (i) f(x,z)q(y) = f(xy,zy);
- (ii) q(x)f(y,w) = f(xy,xw);
- (iii) f(x,z)f(y,w) = f(xy,zw) + f(xw,zy).

Demonstração:

(i) Em primeiro lugar note que $q(x) = q(x.1) = q(x)q(1) \Rightarrow q(1) = 1$.

Linearizando a lei de composição q(xy) = q(x)q(y), substituindo x por x + z, temos:

$$q((x+z)y) = q(x+z)q(y) \Rightarrow q(xy+zy) = q(x+z)q(y)$$
 (1)

Lembrando que a forma bilinear simétrica associada à forma quadrática q(x) é dada por:

$$f(x,z) = q(x+z) - q(x) - q(y) \implies q(x+z) = f(x,z) + q(x) + q(z)$$
 (2)

Substituindo em (1): q(xy + zy) = f(x, z)q(y) + q(x)q(y) + q(z)q(y)

$$\Rightarrow q(xy + zy) = f(x, z)q(y) + q(xy) + q(zy)$$
 (3)

Ainda, por (2):
$$q(xy + zy) = f(xy, zy) + q(xy) + q(zy)$$
 (4)

Igualando (3) e (4):

$$f(x,z)q(y) + q(xy) + q(zy) = f(xy,zy) + q(xy) + q(zy)$$

$$\Rightarrow f(x,z)q(y) = f(xy,zy)$$
(I)

(ii) Fazendo a linearização, substituindo y por y+w, temos:

$$q(x(y+w)) = q(x)q(y+w) \Rightarrow q(xy+xw) = q(x)q(y+w)$$
 (5)

$$f(y,w) = q(y+w) - q(y) - q(w) \implies q(y+w) = f(y,w) + q(y) + q(w)$$
 (6)

Substituindo em (5):

$$q(xy + xw) = q(x)f(y, w) + q(xy) + q(xw)$$
 (7)

Por outro lado:

$$q(xy + xw) = f(xy, xw) + q(xy) + q(xw)$$
(8)

Igualando (7) e (8):

$$q(x)f(y,w) + q(xy) + q(xw) = f(xy,xw) + q(xy) + q(xw)$$

$$\Rightarrow q(x)f(y,w) = f(xy,xw)$$
(II)

(iii) Linearizando (I) em relação a y, substituindo y por y + w:

$$f(x,z)q(y+w) = f(x(y+w), z(y+w)) = f(xy+xw, zy+zw)$$

= $f(xy, zy) + f(xy, zw) + f(xw, zy) + f(xw, zw)$ (9)

Por outro lado:

$$f(x,z)q(y+w) = f(x,z)f(y,x) + f(x,z)q(y) + f(x,z)q(w)$$
(10)

Aplicando (I) no segundo membro de (9) e comparando com (10), obtemos:

$$f(x,z)f(y,w) = f(xy,zw) + f(xw,zy)$$
(III)

Definição 3.2.4. Seja A uma álgebra. Uma **involução** em A é um operador linear $\rho: A \to A$, satisfazendo:

- (i) $\rho(\rho(x)) = x$;
- (ii) $\rho(xy) = \rho(y)\rho(x)$, para todos $x, y \in A$.

Observação: A definição acima refere-se a uma involução do 1º tipo. Outros tipos de involução podem ser encontrados em [22].

Lema 3.2.3. Seja A uma álgebra de composição. A função dada por $x \mapsto \overline{x} = f(x,1).1 - x$ é uma involução em A. Tem-se também: $x\overline{x} = q(x).1 = \overline{x}x$

Demonstração: Mostremos primeiro que \overline{x} é uma involução. Para isto precisamos mostrar que: (i) $\overline{\overline{x}} = x$ e (ii) $\overline{xy} = \overline{y}\overline{x}$

(i)
$$\overline{\overline{x}} = f(\overline{x}, 1) - \overline{x} = f(f(x, 1) - x, 1) - f(x, 1) + x$$

$$= f(f(x, 1), 1) - f(x, 1) - f(x, 1) + x = f(x, 1)f(1, 1) - 2(f(x, 1)) + x$$

$$\operatorname{Mas} f(1, 1) = q(1+1) - q(1) - q(1) = q(2) - 2 = q(2.1) - 2 = 4q(1) - 2 = 4 - 2 = 2.$$

$$\operatorname{Logo} \overline{\overline{x}} = 2f(x, 1) - 2f(x, 1) + x \implies \overline{\overline{x}} = x.$$

(ii)
$$f(\overline{xy}, z) = f(f(xy, 1) - xy, z) = f(f(xy, 1), z) - f(xy, z)$$

 $= f(xy, 1)f(1, z) - f(xy, z)$
 $= f(xy, z) + f((xy)z, 1) - f(xy, z) = f(1, (xy)z)$
 $f(\overline{y}\overline{x}, z) = f((f(y, 1) - y)(f(x, 1) - x), z)$
 $= f(f(y, 1)f(x, 1) - f(y, 1)x - f(x, 1)y + yx, z)$
 $= f(f(y, 1)f(x, 1), z) - f(f(y, 1)x, z) - f(f(x, 1)y, z) + f(yx, z)$
 $= f(x, 1)f(y, 1)f(1, z) - f(y, 1)f(x, z) - f(x, 1)f(y, z) + f(yx, z)$

$$= f(xy,1)f(1,z) + f(x,y)f(1,z) - f(yx,z) - f(yz,x) - f(xy,z) - f(xz,y) + f(yx,z)$$

$$= f(xy, z) + f((xy)z, 1) + f(x, yz) + f(xz, y) - f(yz, x) - f(xy, z) - f(xz, y)$$

Logo $f(\bar{y}\bar{x},z) = f(1,(xy)z)$ e assim:

$$f(\overline{xy},z) = f(\overline{y}\overline{x},z) \Rightarrow f(\overline{xy},z) - f(\overline{y}\overline{x},z) = 0 \Rightarrow f(\overline{xy} - \overline{y}\overline{x},z) = 0, \ \forall z \in A$$

Como f é não degenerada, segue que: $\overline{xy} - \overline{y}\overline{x} = 0 \implies \overline{xy} = \overline{y}\overline{x}$

Provemos agora que $x\overline{x} = q(x).1 = \overline{x}x$. Para isto calculamos:

$$f(x, \overline{y}z) = f(x, (f(y, 1)z - yz)) = f(x, f(y, 1)z) - f(x, yz)$$
$$= f(y, 1)f(x, z) - f(x, yz)$$

Pela igualdade (III) do lema anterior, temos:

$$f(x, \bar{y}z) = f(yx, z) + f(yz, x) - f(x, yz) \implies f(x, \bar{y}z) = f(yx, z)$$

Trocando x por z e z por x na igualdade acima, obtemos:

$$f(yz,x) = f(z,\bar{y}x) \tag{IV}$$

Por (II) e (IV):
$$q(x)f(1,y) = f(x,xy) = f(\bar{x}x,y)$$

Assim:
$$f(q(x).1, y) = f(\bar{x}x, y) \implies f(q(x).1, y) - f(\bar{x}x, y) = 0$$
$$\implies f(q(x).1 - \bar{x}x, y) = 0, \ \forall y \in A$$

Logo, como f é não degenerada, temos: $q(x).1 - \bar{x}x = 0 \implies q(x).1 = \bar{x}x$.

Mas $q(\bar{x}) = q(x)$. De fato:

$$q(\bar{x}) = q(f(x,1)-x) = q(f(x,1).1-x) = f(f(x,1).1,-x) + q(f(x,1).1) + q(-x)$$

$$= f(x,1)f(1,-x) + f(x,1)f(x,1)q(1) + q(x)$$

$$= -f(x,1)f(x,1) + f(x,1)f(x,1) + q(x) = q(x)$$

Temos também: $q(\bar{x}) = \bar{x}\bar{x} = x\bar{x} \implies x\bar{x} = \bar{x}x$

Lema 3.2.4. Seja A uma álgebra de composição em que foi definida uma involução $j(x) = \overline{x}$. Então as seguintes propriedades são verificadas, para todos $x, y \in A$:

- (i) $\bar{x}(xy) = (\bar{x}x)y$;
- (ii) $(yx)\bar{x} = y(x\bar{x}).$

Demonstração:

(i) Calculamos
$$f(\bar{x}(xy), z) = f(f(x, 1) - x)(xy), z) = f(f(x, 1)(xy) - x(xy), z)$$

 $= f(f(x, 1)(xy), z) - f(x(xy), z)$
 $= f(x, 1)f(xy, z) - f(x(xy), z)$
 $= f(x(xy), z) + f(xz, xy) - f(x(xy), z)$
 $= q(x)f(z, y) = q(x)f(y, z) = f(q(x)y, z)$

Assim: $f(\bar{x}(xy), z) = f(q(x)y, z) \Rightarrow f(\bar{x}(xy), z) - f(q(x)y, z) = 0$ $\Rightarrow f(\bar{x}(xy) - q(x)y, z) = 0, \ \forall z \in A$

Como f é não degenerada, obtemos: $\bar{x}(xy) - q(x)y = 0 \implies \bar{x}(xy) = q(x)y$, mas $q(x) = \bar{x}x$, logo: $\bar{x}(xy) = (\bar{x}x)y$.

(ii) Calculamos
$$f(z, (yx)\bar{x}) = f(z, (yx)(f(x, 1) - x)) = f(z, f(x, 1)(yx) - (yx)x)$$

 $= f(z, f(x, 1)(yx)) - f(z, (yx)x)$
 $= f(x, 1)f(z, yx) - f(z, (yx)x)$
 $= f(z, yx)f(x, 1) - f(z, (yx)x)$
 $= f(zx, yx) + f(z, (yx)x) - f(z, (yx)x)$
 $= f(z, y)q(x) = f(z, yq(x)) = f(z, y(x\bar{x}))$

Assim: $f(z, (yx)\bar{x}) = f(z, y(x\bar{x})) \Rightarrow f(z, (yx)\bar{x} - y(x\bar{x})) = 0, \ \forall z \in A$

Como f é não degenerada, temos: $(yx)\bar{x} - y(x\bar{x}) = 0 \implies (yx)\bar{x} = y(x\bar{x}).$

Teorema 3.2.5. Toda álgebra de composição é alternativa.

Demonstração: Seja A uma álgebra de composição. Pelo Lema 3.2.4, podemos escrever $(\bar{x}, x, y) = 0 = (y, x, \bar{x})$. Daí:

$$0 = (f(x,1) - x, x, y) = (f(x,1), x, y) - (x, x, y) = f(x,1)(1, x, y) - (x, x, y)$$
$$= 0 - (x, x, y) \implies (x, x, y) = 0$$

Analogamente:
$$0 = (y, x, \bar{x}) = (y, x, f(x, 1) - x) = (y, x, f(x, 1)) - (y, x, x)$$

= $0 - (y, x, x) \Rightarrow (y, x, x) = 0$

Portanto A é alternativa.

Teorema 3.2.6. Seja A uma álgebra alternativa com 1, em que está definida uma involução $j: x \mapsto \bar{x}$ tal que $x\bar{x} = q(x).1$, onde q(x) é uma forma quadrática não degenerada. Então A é uma álgebra de composição.

Demonstração: Basta mostrar que q(x) admite composição, i.e. q(xy) = q(x)q(y). Linearizando $x\bar{x} = q(x)1$, substituindo x por x + y, temos:

$$(x+y)(\overline{x+y}) = q(x+y) \implies (x+y)(\overline{x}+\overline{y}) = f(x,y) + q(x) + q(y)$$

$$\Rightarrow x\overline{x} + x\overline{y} + y\overline{x} + y\overline{y} = f(x,y) + x\overline{x} + y\overline{y} \implies x\overline{y} + y\overline{x} = f(x,y)1$$

Fazendo y = 1 na igualdade obtida, vem: $x + \bar{x} = f(x, 1)1$

Denotando f(x,1) por t(x), temos: $x + \bar{x} = t(x)1$

Como A é alternativa, e lembrando que: $(\alpha, x, y) = 0$, para todo $\alpha \in F$, e todos $x, y \in A$, e ainda, $x + \bar{x} \in F$, calculamos:

$$0 = (x + \bar{x}, x, y) = (x, x, y) + (\bar{x}, x, y) \Rightarrow (\bar{x}, x, y) = 0$$
. Analogamente:

$$0 = (y, x, x + \bar{x}) = (y, x, x) + (y, x, \bar{x}) \implies (y, x, \bar{x}) = 0.$$

Calculemos agora:

$$q(xy) = (\overline{xy})(xy) = (\overline{y}\overline{x})(xy) = ((t(y) - y)\overline{x})(xy) = (t(y)\overline{x} - y\overline{x})(xy)$$
$$= t(y)\overline{x}(xy) - (y\overline{x})(xy)$$

Pelo Lema 3.2.4, $\bar{x}(xy)=(\bar{x}x)y=q(x)y$ e, pela identidade (ii) de Moufang (Teorema 1.2.2), $(y\bar{x})(xy)=y(\bar{x}x)y$. Daí:

$$q(xy) = t(y)q(x)y - y(x\bar{x})y = t(y)q(x)y - q(x)y^{2} = q(x)y(t(y) - y)$$

= $(q(x)y)\bar{y} = q(x)y\bar{y} = q(x)q(y)$

3.3 Processo de Duplicação de Cayley-Dickson

Quais são as álgebras de composição? Como obtê-las? Veremos um processo que permite a construção de tais álgebras a partir de uma álgebra A com 1, onde está definida uma involução $x \mapsto \bar{x}$ tal que $x\bar{x} = q(x)1$, sendo q(x) uma forma quadrática não degenerada. Supomos inicialmente que A é alternativa. Pelo Teorema 3.2.6 temos, em A, $x\bar{y} + y\bar{x} = f(x,y)1$ e também $x + \bar{x} = t(x)1$, onde t(x) = f(x,1).

Seja $\alpha \in F$, $\alpha \neq 0$. Vamos construir com A, j e α uma álgebra A_1 satisfazendo as mesmas condições de A e tal que $\dim_F A_1 = 2\dim_F A$. Seja $A_1 = A \oplus A$ o espaço vetorial formado pelos pares ordenados (x,y), com $x,y \in A$. Evidentemente $\dim_F A_1 = 2\dim_F A$. Para que A_1 se torne uma álgebra devemos definir um produto em A_1 . Fazemos:

$$(x,y)(u,v) = (xu + \alpha v\bar{y}, \bar{x}v + uy)$$

Com este produto verifica-se facilmente que A_1 se torna uma álgebra. Além disso, A_1 tem 1, que é dado por (1,0). De fato:

$$(x,y)(1,0) = (x1 + \alpha \bar{0}y, 0x + y\bar{1}) = (x,y)$$
$$(1,0)(x,y) = (1x + \alpha \bar{y}0, y1 + 0\bar{y}) = (x,y)$$

Podemos identificar A como a subálgebra de A_1 formada pelos elementos da forma $(x,0), x \in A$. De fato:

$$(x,0)(y,0) = (xy + \alpha \bar{0}0, 0x + 0\bar{y}) = (xy,0)$$

Assim, existe um monomorfismo de A em A_1 dado por $x \mapsto (x,0)$.

Seja $e = (0,1) \in A_1$. Então $e^2 = \alpha.1$. De fato:

$$e^2 = (0,1)(0,1) = (0.0 + \alpha.1.\overline{1}, \overline{0}.1 + 0.1) = (\alpha.1,0) = \alpha(1,0) = \alpha.1$$

Então todo elemento de A_1 pode ser escrito como:

$$(x,y) = (x,0) + (0,y) = x(1,0) + (0,1)y = x.1 + ey = x + ey$$

Consequentemente, denotamos: $A_1 = A + eA$. É imediato que esta soma é direta, portanto: $A_1 = A \oplus eA$.

Definimos uma involução em A_1 da seguinte forma: $j:(x,y)\to \overline{(x,y)}=(\overline{x},-y)$. Mostremos que j, assim definida, é uma involução:

(i)
$$\overline{\overline{(x,y)}} = \overline{(\overline{x},-y)} = (\overline{\overline{x}},-(-y)) = (x,y)$$

(ii)
$$\overline{(x,y)(u,v)} = \overline{(xu + \alpha v \bar{y}, \bar{x}v + uy)} = (\overline{xu + \alpha v \bar{y}}, -(\bar{x}v + uy))$$

$$= (\overline{xu} + \alpha \overline{v} \overline{y}, -\bar{x}v - uy) = (\bar{u}\bar{x} + \alpha y \bar{v}, -\bar{x}v - uy)$$

$$\overline{(u,v)} \overline{(x,y)} = (\bar{u}, -v)(\bar{x}, -y) = (\bar{u}\bar{x} + \alpha(-y)(-\bar{v}), \bar{u}(-y) + \bar{x}(-v))$$

$$= (\bar{u}\bar{x} + \alpha y \bar{v}, -\bar{x}v - uy)$$

Portanto $\overline{(x,y)(u,v)} = \overline{(u,v)} \overline{(x,y)}$

Vamos agora definir uma forma quadrática não degenerada em A_1 . Como, em A, temos $q(x) = x\bar{x}$, vamos usar esta mesma expressão para definir q(X), onde $X = (x, y) \in A_1$. Assim, temos:

$$X\overline{X} = (x,y)\overline{(x,y)} = (x,y)(\bar{x},-y) = (x\bar{x} + \alpha(-y)\bar{y}, \bar{x}(-y) + \bar{x}y)$$
$$= (x\bar{x} - \alpha y\bar{y}, -\bar{x}y + \bar{x}y) = (x\bar{x} - \alpha y\bar{y}, 0) = q(x) - \alpha q(y)$$

A forma bilinear associada a q(X) é: $f(X,U)=X\overline{U}+U\overline{X}$, onde X=(x,y) e U=(u,v). Calculamos, então:

$$f(X,U) = (x,y)\overline{(u,v)} + (u,v)\overline{(x,y)} = (x,y)(\bar{u},-v) + (u,v)(\bar{x},-y)$$

$$= (x\bar{u} + \alpha(-v)\bar{y}, \bar{x}(-v) + \bar{u}y) + (u\bar{x} + \alpha(-y)\bar{v}, \bar{u}(-y) + \bar{x}v)$$

$$= (x\bar{u} - \alpha v\bar{y}, -\bar{x}v + \bar{u}y) + (u\bar{x} - \alpha y\bar{v}, \bar{u}(-y) + \bar{x}v)$$

$$= (x\bar{u} + u\bar{x} - \alpha(v\bar{y} + y\bar{v}), \bar{x}v + \bar{x}v + \bar{u}y - \bar{u}y)$$

$$= (x\bar{u} + u\bar{x} - \alpha(v\bar{y} + y\bar{v}), 0) = f(x,u) - \alpha f(v,y)$$

Vamos mostrar que q(X) é não degenerada. Suponhamos f(X, U) = 0, $\forall U \in A_1$. Então, pela expressão obtida acima:

 $f(X,U) = (x\bar{u} + u\bar{x} - \alpha(v\bar{y} + y\bar{v}), 0) = 0 \implies x\bar{u} + u\bar{x} - \alpha(v\bar{y} + y\bar{v}) = 0, \quad \forall \ u,v \in A.$

Em particular, para v = 0, esta relação continua válida. Daí:

$$x\bar{u} + u\bar{x} = 0$$
, $\forall u \in A$ ou $f(x, u) = 0$, $\forall u \in A$.

Como f(x, u) é não degenerada em A, segue que x = 0.

Fazendo u=0, obtemos $-\alpha(v\bar{y}+y\bar{v})=0$, e como $\alpha\neq 0$, resulta $v\bar{y}+y\bar{v}=f(v,y)=0$ ou f(y,v)=0 $\forall\,v\in A$.

Novamente, como f(y, v) é não degenerada em A, devemos ter y = 0.

Então X = (x, y) = 0 e q(X) é não degenerada em A_1 .

Obtivemos então uma álgebra A_1 com as mesmas propriedades da álgebra A e com dimensão duas vezes a de A. Denotaremos a álgebra A_1 por (A, α) , enfatizando o escalar usado na construção de A_1 . Mas estamos interessados em obter álgebras de composição. Em que condições a álgebra (A,α) obtida de A pelo processo de duplicação de Cayley-Dickson é uma álgebra de composição? Pelo exposto até agora podemos concluir que basta que (A,α) seja alternativa. Sob que condições isto acontece? É o que provaremos a seguir. Para isto vamos precisar de dois lemas.

Lema 3.3.1. Em uma álgebra (A, α) obtida de uma álgebra A pelo processo de Cayley-Dickson, tem-se que: (X, X, Z) = 0 equivale a (Z, X, X) = 0, para todos $X, Z \in (A, \alpha)$.

Demonstração: Sejam $X, Z \in (A, \alpha)$ tal que (X, X, Z) = 0. Temos também $(\bar{X}, \bar{X}, \bar{Z}) = 0$. Então, aplicando involução nesta igualdade temos:

$$0 = \overline{(\overline{X}, \overline{X}, \overline{Z})} = \overline{(\overline{X} \ \overline{X})} \overline{Z} - \overline{X}(\overline{X} \ \overline{Z}) = \overline{(\overline{X} \ \overline{X})} \overline{Z} - \overline{X}(\overline{X} \ \overline{Z})$$

$$= \overline{\overline{Z}}(\overline{\overline{X}} \ \overline{\overline{X}}) - (\overline{\overline{X}} \ \overline{\overline{Z}}) \overline{\overline{X}} = Z(\overline{\overline{X}} \ \overline{\overline{X}}) - (\overline{\overline{Z}} \ \overline{\overline{X}})X$$

$$= Z(XX) - (ZX)X = -(Z, X, X)$$

A recíproca se prova de forma inteiramente análoga.

Lema 3.3.2. Seja A uma álgebra alternativa com 1, em que está definida uma involução \overline{x} . Então, para todos $x, y \in A$, (x, x, y) = 0 se e somente se $(x, \overline{x}, y) = 0$.

Demonstração: Lembrando que $\overline{x} = f(x,1) - x$, e que $f(x,1) \in F$, temos:

$$(x, \overline{x}, y) = (x, f(x, 1) - x, y) = (x, f(x, 1), y) - (x, x, y) = -(x, x, y)$$

Então: $(x, x, y) = 0$ se e somente se $(x, \overline{x}, y) = 0$.

Podemos agora mostrar o principal resultado desta seção.

Teorema 3.3.3. A álgebra (A, α) obtida de A pelo processo de duplicação de Cayley-Dickson é alternativa se e somente se A é associativa.

Demonstração: Sejam X=(x,y) e $Z=(z,t)\in (A,\alpha)$. Calculemos:

$$(X, \overline{X}, Z) = (X\overline{X})Z - X(\overline{X}Z) = (x\overline{x} - \alpha(y\overline{y}))(z, t) - (x, y)((\overline{x}, -y)(z, t))$$

$$= (q(x) - \alpha q(y))(z, t) - (x, y)((\overline{x}, -y)(z, t))$$

$$= \underbrace{(q(x)z - \alpha q(y)z, q(x)t - \alpha q(y)t)}_{(1)} - \underbrace{(x, y)(\overline{x}z - \alpha t\overline{y}, xt - zy)}_{(2)}$$

Desenvolvendo a parcela (2), temos:

$$(2) = (x(\overline{x}z - \alpha t\overline{y}) + \alpha(xt - zt)\overline{y}, \overline{x}(xt - zy) + (\overline{x}z - \alpha t\overline{y})y)$$

$$= (x(\overline{x}z) - \alpha x(t\overline{y}) + \alpha(xt)\overline{y} - \alpha(zy)\overline{y}, \overline{x}(xt) - \overline{x}(zy) + (\overline{x}z)y - \alpha(t\overline{y})y)$$

Notando que: $x(\overline{x}z) = q(x)z$; $(zy)\overline{y} = q(y)z$; $\overline{x}(xt) = q(x)t$; $(t\overline{y})y = q(y)t$ a expressão (2) fica:

$$(2) = (q(x)z - \alpha q(y)z - \alpha x(t\overline{y}) + \alpha(xt)\overline{y}, q(x)t - \alpha q(y)t - \overline{x}(zy) + (\overline{x}z)y)$$

Finalmente, fazendo (1) – (2) obtemos:
$$(X, \overline{X}, Z) = (-\alpha(x, t, \overline{y}), -(\overline{x}, z, y)).$$

Chegamos assim a uma expressão que relaciona o associador em (A, α) com o associador em A. Concluímos diretamente da expressão obtida que (A, α) é alternativa se e somente se A é associativa.

Cabem ainda algumas investigações na álgebra (A, α) . Os próximos dois teoremas nos trazem mais esclarecimentos.

Teorema 3.3.4. A álgebra (A, α) é associativa se e somente se A é comutativa.

Demonstração: Sejam X=(x,y), U=(u,v) e $Z=(z,t)\in (A,\alpha)$. Calculemos:

$$(X,U,Z) = (XU)Z - X(UZ) = \underbrace{((x,y)(u,v))(z,t)}_{\text{(1)}} - \underbrace{(x,y)((u,v)(z,t))}_{\text{(2)}}$$

$$(1) = (xy + \alpha v \overline{y}, \overline{x}v + uy)(z, t)$$

$$= (xy + \alpha v \overline{y})z + \alpha t(\overline{(\overline{x}v + uy)}, \overline{(xy + \alpha v \overline{y})}t + z(\overline{x}v + uy))$$

$$= (xy)z + \alpha(v\overline{y})z + \alpha t(\overline{x}v + \overline{u}y), (\overline{x}y + \alpha v \overline{y})t + z(\overline{x}v) + z(uy))$$

$$= (xy)z + \alpha(v\overline{y})z + \alpha t(\overline{v}x + \overline{y}\overline{u}), (\overline{y}x + \alpha y\overline{v})t + z(\overline{x}v) + z(uy))$$

$$= (xy)z + \alpha(v\overline{y})z + \alpha t(\overline{v}x) + \alpha t(\overline{y}\overline{u}), (\overline{y}x)t + \alpha(y\overline{v})t + z(\overline{x}v) + z(uy))$$

$$(2) = (x, y)(uz + \alpha t\overline{v}, \overline{u}t + zv)$$

$$= (x(uz + \alpha t\overline{v}) + \alpha(\overline{u}t + zv)\overline{y}, \overline{x}(\overline{u}t + zv) + (uz + \alpha t\overline{v})y)$$

$$= (x(uz) + \alpha x(t\overline{v}) + \alpha(\overline{u}t)\overline{y} + \alpha(zv)\overline{y}, \overline{x}(\overline{u}t) + \overline{x}(zv) + (uz)y + \alpha(t\overline{v})y)$$

Fazendo x = u = t = 0 e y = 1, obtemos:

$$(X, U, Z) = (1) - (2) = \alpha(vz) - \alpha(zv)$$

Como $\alpha \neq 0$, a expressão acima nos diz que (A, α) é associativa se e somente se A é comutativa.

Teorema 3.3.5. A álgebra (A, α) obtida de A pelo processo de duplicação de Cayley-Dickson é comutativa se e somente se A é comutativa e j = 1 (involução identidade).

Demonstração: Sejam X=(x,y) e $U=(u,v)\in (A,\alpha)$. Calculemos:

$$[X, U] = XU - UX = (x, y)(u, v) - (u, v)(x, y)$$

$$= (xu + \alpha v\overline{y}, \overline{x}v + uy) - (ux + \alpha y\overline{v}, \overline{u}y + xv)$$
$$= (xu - ux + \alpha(v\overline{y} - y\overline{v}), (\overline{x} - x)v + (u - \overline{u})y)$$

Vemos assim que, para que (A, α) seja comutativa, isto é [X, U] = 0, A deve ser comutativa e $x = \overline{x}$, para todos $x \in A$, o que significa que a involução j deve ser a identidade.

3.4 Exemplos de Álgebras de Composição

O exemplo mais trivial de álgebra de composição é o próprio corpo F. De fato, em F definimos $q(x)=x^2$, donde $q(xy)=(xy)^2=x^2y^2=q(x)q(y)$, que é claramente não degenerada. Temos também que $q(x)=x^2=x\overline{x} \Rightarrow \overline{x}=x$, logo j=1. Tomando $\alpha \neq 0$ em F construímos a álgebra (F,α) de dimensão 2 que é, pelo que vimos anteriormente, comutativa e associativa.

Tomando outro elemento não nulo em F, digamos $\beta \in F$, duplicamos (F, α) , obtendo $((F, \alpha), \beta)$, que são álgebras de dimensão 4 chamadas álgebras dos quatérnios generalizados, que se costuma designar por Q. Assim $Q(\alpha, \beta) = ((F, \alpha), \beta)$.

Quanto à involução em (F,α) temos, pela expressão geral $j:(F,\alpha)\to (F,\alpha)$ é dada por $j(x,y)=\overline{(x,y)}=(\overline{x},-y)$. Assim, como a involução j não é o operador identidade, a álgebra $Q(\alpha,\beta)$ dos quatérnios generalizados não é comutativa. Mas, sendo (F,α) comutativa, $Q(\alpha,\beta)$ é associativa.

Continuando o processo, ao duplicarmos Q, obteremos uma álgebra alternativa, mas não associativa. Tomando então $\gamma \in F$, $\gamma \neq 0$, obtemos a álgebra $(Q(\alpha, \beta), \gamma)$ de dimensão 8, que denotamos por $C(\alpha, \beta, \gamma)$ ou, simplesmente C. Como C é alternativa, é também uma álgebra de composição. Tal álgebra é chamada álgebra de Cayley-Dickson ou álgebra dos octônios.

Se continuarmos o processo, duplicando agora a álgebra C obteremos uma álgebra que não é alternativa (pois C não é associativa) e, portanto, não é de composição. Desta forma, partindo do corpo F obtemos apenas 4 álgebras de composição: o próprio corpo F, de dimensão 1, as álgebras quadráticas, de dimensão 2, as álgebras dos quatérnios, de dimensão 4 e as álgebras dos octônios, de dimensão 8.

Mostraremos a seguir que estas são as únicas álgebras de composição, a menos de isomorfismos. Para isto consideraremos uma álgebra de composição A arbitrária e B

85

subálgebra de A satisfazendo certas condições. Então B pode ser duplicada através do processo de Cayley-Dickson, obtendo uma álgebra C, subálgebra de A satisfazendo as mesmas condições de B.

Definição 3.4.1. Sejam A um espaço vetorial em que está definida uma forma bilinear não degenerada f(x,y) e B subespaço próprio de A. Chama-se **complemento ortogonal** de B em relação a f(x,y) ao conjunto

$$B^{\perp} = \{ a \in A \mid f(a, b) = 0, \forall b \in B \}.$$

Lema 3.4.1. A forma bilinear f(x,y) é não degenerada em B^{\perp} .

Demonstração: Seja
$$f \mid_{B^{\perp}} (a, b) = 0$$
, para todo $b \in B^{\perp}$. Então $a \in (B^{\perp})^{\perp} = B \implies a \in B^{\perp} \cap B \implies a = 0$

Lema 3.4.2. Seja A uma álgebra de composição e B subálgebra de A contendo 1, tal que a restrição de f(x,y) a B é não degenerada. Valem os seguintes resultados:

- (i) $\overline{e} = -e$, para todo $e \in B^{\perp}$;
- (ii) $xe = e\overline{x}$, para todo $e \in B^{\perp}$ e todo $x \in B$;
- (iii) $x(ey) = e(\overline{x}y);$
- (iv) (ey)x = e(xy);
- (v) $(ex)(ey) = \alpha y\overline{x}$, onde $\alpha = -q(e)$;
- (vi) Seja $e \in B^{\perp}$ tal que $q(e) \neq 0$; Então $B_1 = B \oplus eB$ é a subálgebra de A obtida de B pelo processo de Cayley-Dickson.

Demonstração:

- (i) Para todo $e \in B^{\perp}$, f(e, y) = 0, $\forall y \in B$. Em particular, $f(e, 1) = 0 \Rightarrow \overline{e} + e = 0 \Rightarrow \overline{e} = -e$
- (ii) $f(x,e) = x\overline{e} + e\overline{x} = 0 \implies x\overline{e} = -e\overline{x} \implies -xe = -e\overline{x} \implies xe = e\overline{x}$

(iii) Pelo Lema 3.2.4: $x(\overline{x}y) = (x\overline{x})y = q(x)y$. Linearizando em relação a x, temos:

$$(x+z)(\overline{(x+z)}y) = q(x+z)y \implies (x+z)(\overline{x}y + \overline{z}y) = q(x+z)y$$

$$\Rightarrow x(\overline{x}y) + x(\overline{z}y) + z(\overline{x}y) + z(\overline{z}y) = (x+z)(\overline{x} + \overline{z})y$$

$$\Rightarrow x(\overline{x}y) + x(\overline{z}y) + z(\overline{x}y) + z(\overline{z}y) = (x\overline{x})y + (x\overline{z})y + (z\overline{x})y + (z\overline{z})y$$

$$\Rightarrow x(\overline{z}y) + z(\overline{x}y) = (x\overline{z} + z\overline{x})y \implies x(\overline{z}y) + z(\overline{x}y) = f(x,z)y$$

Substituindo z por e:

$$x(\overline{e}y) + e(\overline{x}y) = 0 \implies x(\overline{e}y) = -e(\overline{x}y) \stackrel{(i)}{\Rightarrow} -x(ey) = e(\overline{x}y) \implies x(ey) = e(\overline{x}y)$$

(iv) Podemos escrever (iii) como $\overline{x}(ey) = e(xy)$. Aplicando involução e usando (ii): $\overline{\overline{x}(ey)} = \overline{e(xy)} \implies \overline{(ey)}x = \overline{(xy)}\overline{e} \implies (\overline{y}\ \overline{e})x = -\overline{(xy)}e \stackrel{(ii)}{\Rightarrow} -(\overline{y}e)x = -e(xy)$ $\Rightarrow (ey)x = e(xy)$

(v)
$$(ex)(ey) \stackrel{(ii)}{=} (ex)(\overline{y}e) \stackrel{*}{=} e(x\overline{y})e \stackrel{*}{=} ((y\overline{x})e)e = y(\overline{x})e^2 = (y\overline{x})(e(-\overline{e})) = -(y\overline{x})(e\overline{e})$$

= $-(y\overline{x})q(e) = \alpha y\overline{x}$

(*) Moufang
$$(**) e(x\overline{y}) = (\overline{x}\overline{y})e = (y\overline{x})e$$

(vi) Calculemos, para $x, y, z, t \in B$:

$$(x + ey)(z + et) = xz + x(et) + (ey)z + (ey)(et) = xz + e(\overline{x}t) + e(zy) + \alpha t\overline{y}$$
$$= xz + \alpha t\overline{y} + e(\overline{x}t + zy)$$

Portanto $(x + ey)(z + et) \in B_1 = B \oplus eB$. Logo, B_1 é subálgebra de A.

O produto em B_1 é o mesmo dado pela duplicação de B por Cayley-Dickson, conforme verificamos a seguir:

$$(x,y)(z,t) = (xz + \alpha t \overline{y}, \overline{x}t + zy) = xz + \alpha t \overline{y} + e(\overline{x}t + zy)$$

Falta ainda mostrar que:

(a) A involução em $B \oplus eB$ é a mesma em (B, α)

Aplicando (i) e (ii):
$$\overline{x + ey} = \overline{x} + \overline{ey} = \overline{x} + \overline{y} \ \overline{e} = \overline{x} - \overline{y}e = \overline{x} - ey$$

(b) $B \in eB$ têm a mesma dimensão

Pelo Lema 3.2.2 (ii) tem-se: q(x)f(y,w) = f(xy,xw), para todos $x,y,w \in A$. Fazendo x=e,y=a e w=b, obtemos: $f(ea,eb)=q(e)f(a,b)=-\alpha f(a,b)$.

Então, a aplicação $\varphi: B \to eB$ dada por $\varphi(b) = eb$ é injetora. De fato, $x \in ker(\varphi) \Rightarrow \varphi(x) = ex = 0$. Como f é não degenerada, devemos ter: $f(ex, ey) = f(0, ey) = -\alpha f(x, y) = 0 \Rightarrow f(x, y) = 0 \Rightarrow x = 0$. Como φ é claramente sobrejetora, temos uma bijeção de B em eB. Logo B e eB têm a mesma dimensão.

(c) A forma f(x,y) restrita a $B \oplus eB$ é não degenerada

Mostremos inicialmente que $ex \in B^{\perp}$, para todo $x \in B$. Basta mostrar que f(b, ex) = 0, para todo $b \in B$. Pelo Lema 3.2.2 (iii):

$$f(b, ex) = f(b.1, ex) = f(b, e)f(1, x) - f(bx, e) = 0f(1, x) - 0 = 0.$$

Seja $f(x + ey, z + et) = 0, \ \forall z + et \in B \oplus eB$. Então:

$$0 = f(x,z) + \underbrace{f(x,et)}_{=0} + \underbrace{f(ey,z)}_{=0} + \underbrace{f(ey,et)}_{=0} \implies f(x,z) = 0 \implies x = 0.$$

Tem-se ainda: $f(ey, et) = -\alpha f(y, t) = 0 \stackrel{\alpha \neq 0}{\Rightarrow} f(y, t) = 0 \Rightarrow y = 0.$

Portanto x + ey = 0 e f é não degenerada em $B \oplus eB$.

Mostramos assim que $B \oplus eB$ é a subálgebra de A obtida de B pelo processo de Cayley-Dickson. Podemos escrever então: $B_1 = (B, \alpha) = B \oplus eB$.

Pelo que foi mostrado, (B, α) satisfaz as mesmas condições de B e podemos aplicar o processo de Cayley-Dickson em (B, α) . Veremos no próximo teorema que as álgebras de composição se restringem aos quatro exemplos apresentados.

Teorema 3.4.3 (Hurwitz). As únicas álgebras de composição sobre um corpo F de característica $\neq 2$ são:

- (i) F;
- (ii) As álgebras quadráticas (F, α) ;
- (iii) As álgebras de quatérnios;

(iv) As álgebras de Cayley-Dickson.

Demonstração: As álgebras citadas são de composição conforme já sabemos. Para mostrar que estas são as únicas, consideremos uma álgebra de composição A. Se A = F então temos o caso (i). Se $A \neq F$, tomamos B = F, subálgebra de A contendo 1 e, como f é não degenerada em F podemos aplicar Cayley-Dickson em F obtendo $(F,\alpha) \subseteq A$. Se $A = (F,\alpha)$ obtemos (ii). Se $A \neq (F,\alpha)$, fazemos $B = (F,\alpha)$, podemos duplicar B por Cayley-Dickson, pois, pelo Lema 3.4.1, f é não degenerada em B. Obtemos a álgebra Q dos quatérnios, $Q \subseteq A$. Se A = Q o item (iii) está demonstrado. Se $A \neq Q$, duplicamos Q (f é não degenerada em Q), obtendo uma álgebra de Cayley-Dickson C contida em A. Se A = C provamos (iv). Se $A \neq C$, podemos duplicar C por Cayley-Dickson obtendo uma álgebra D que não é de composição, pois C não é associativa. Mas isto é impossível, pois $D \subseteq A$ e A é de composição. Devemos ter então, necessariamente A = C e o teorema está provado.

3.5 Hurwitz e a Soma de Quadrados

Vamos agora fazer uma relação das álgebras de composição com o problema da soma de quadrados. Para isto precisaremos construir a tábua de multiplicação da álgebra de Cayley, C. Definiremos os produtos para esta tábua a partir dos elementos de uma base de C. Como é uma base de C visto como um espaço vetorial de dimensão 8? Vamos fazer esta construção passo a passo, começando com o corpo F, definindo as diversas multiplicações em cada uma das álgebras de composição.

A primeira álgebra de composição é o próprio $corpo\ F$, cuja base é $\{1\}$, a unidade de F. Vamos designar $e_0=1$. Para um dado $\alpha\in F$, $\alpha\neq 0$, obtemos (F,α) na qual um elemento se escreve $x.1+e_1y$ onde $e_1=(0,1)$ e $e_1^2=\alpha$. São as álgebras quadráticas sobre F, que vamos denotar por $F\oplus e_1F$. Uma base de (F,α) é $\{1,e_1\}$. Como F é corpo, podemos fazer a multiplicação por e_1 à esquerda, como usualmente se procede para escrever combinações lineares em um espaço vetorial. Assim, se $X=(x,y)\in (F,\alpha)$, temos: $X=x+ye_1$ e daí $(F,\alpha)=F\oplus Fe_1$. A tábua de multiplicação em (F,α) é dada a seguir:

	1	e_1	
1	1	e_1	
e_1	e_1	α	

Tomamos agora $\beta \in F$, $\beta \neq 0$, e construímos a álgebra dos quatérnios Q designada por $((F,\alpha),\beta)$. Um elemento de Q se escreve $X+e_2Z$, com $X,Z\in (F,\alpha)$, X=(x,y), Z=(z,t) e $e_2^2=\beta$. Desta forma escrevemos $Q=(F,\alpha)\oplus e_2(F,\alpha)$. Assim como fizemos nas álgebras quadráticas gostaríamos de multiplicar por e_2 à esquerda, para podermos formalizar uma base em Q. Notando que $e_2 \in Q^{\perp}$, o Lema 3.4.2 (i),(ii) permite fazer esta alteração. Escrevemos, então: $Q=(F,\alpha)\oplus (F,\alpha)e_2$. Assim, um elemento de Q é dado por:

$$X + Ze_2 = x + ye_1 + (z + te_1)e_2 = x + ye_1 + ze_2 + (te_1)e_2$$

Como Q é associativa, $(te_1)e_2 = t(e_1e_2)$. Logo:

$$X + Ze_2 = x + ye_1 + ze_2 + t(e_1e_2)$$

Temos então que $\{1, e_1, e_2, e_1e_2\}$ é uma base de Q. Ou, simplificando a notação, fazemos $e_1e_2=e_3$ e daí, a base de Q será: $\{1, e_1, e_2, e_3\}$. A tábua de multiplicação em Q é indicada abaixo:

	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	α	e_3	αe_2
$ e_2 $	e_2	$-e_3$	β	$-\beta e_1$
e_3	e_3	$-\alpha e_2$	βe_1	$-\alpha\beta$

Destacamos alguns cálculos realizados para se chegar a estes valores. Lembrando que, pela regra de multiplicação estabelecida por Hamilton, temos:

Calculamos:
$$e_1e_2 = -e_2e_1 \qquad e_1e_3 = -e_3e_1 \qquad e_2e_3 = -e_3e_2$$

$$e_1e_3 = e_1(e_1e_2) = e_1^2e_2 = \alpha e_2$$

$$e_3e_2 = (e_1e_2)e_2 = e_1e_2^2 = \beta e_1$$

$$e_3^2 = (e_1e_2)^2 = (e_1e_2)(e_1e_2) = -(e_2e_1)(e_1e_2) = -((e_2e_1)e_1)e_2$$

$$= -(e_2e_1^2)e_2 = -(\alpha e_2)e_2 = -\alpha e_2^2 = -\alpha \beta$$

Vamos agora à construção da álgebra dos octônios. Tomamos $\gamma \in F$, $\gamma \neq 0$ e obtemos a álgebra $C = (Q(\alpha, \beta), \gamma)$, que é formada por pares de elementos de $Q(\alpha, \beta)$. Escrevemos então $C = (Q(\alpha, \beta), \gamma) = Q(\alpha, \beta) \oplus Q(\alpha, \beta)e_4$, onde $e_4^2 = \gamma$. Assim, um elemento de C se escreve: $u + ve_4$, com $u, v \in Q(\alpha, \beta)$. Sejam $u = a + be_1 + ce_2 + de_3$ e $v = e + fe_1 + ge_2 + he_3$. Daí:

$$u + ve_4 = (a + be_1 + ce_2 + de_3) + (e + fe_1 + ge_2 + he_3)e_4$$
$$= a + be_1 + ce_2 + de_3 + ee_4 + f(e_1e_4) + g(e_2e_4) + h(e_3e_4)$$

Fazemos: $e_1e_4=e_5,\ e_2e_4=e_6,\ e_3e_4=e_7$ e obtemos uma base de C:

$$\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}.$$

A tábua de multiplicação de C é dada abaixo:

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	α	e_3	αe_2	e_5	αe_4	$-e_7$	$-\alpha e_6$
e_2	e_2	$-e_3$	β	$-\beta e_1$	e_6	e_7	βe_4	βe_5
e_3	e_3	$-\alpha e_2$	βe_1	$-\alpha\beta$	e_7	αe_6	$-\beta e_5$	$-\alpha\beta e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	γ	$-\gamma e_1$	$-\gamma e_2$	$-\gamma e_3$
e_5	e_5	$-\alpha e_4$	$-e_7$	$-\alpha e_6$	γe_1	$-\alpha\gamma$	γe_3	$\alpha \gamma e_2$
e_6	e_6	e_7	$-\beta e_4$	βe_5	γe_2	$-\gamma e_3$	$-\beta\gamma$	$-\beta\gamma e_1$
e_7	e_7	αe_6	$-\beta e_5$	$\alpha \beta e_4$	γe_3	$-\alpha\gamma e_2$	$\beta \gamma e_1$	$\alpha \beta \gamma$

Indicamos a seguir o cálculo de alguns dos elementos da tabela:

$$e_{1}e_{6} = e_{1}(e_{2}e_{4}) \stackrel{*}{=} e_{1}(e_{4}\overline{e}_{2}) \stackrel{**}{=} e_{4}(\overline{e}_{1} \ \overline{e}_{2}) \stackrel{***}{=} e_{4}(e_{1}e_{2}) = e_{4}e_{3} = -e_{7}$$

$$(*) \text{ Lema } 3.4.2 \text{ (ii)} \qquad (***) \text{ Lema } 3.4.2 \text{ (iii)} \qquad (****) \text{ Lema } 3.4.2 \text{ (i)}$$

$$e_{5}^{2} = (e_{1}e_{4})(e_{1}e_{4}) = (e_{1}e_{4})(e_{4}\overline{e}_{1}) = e_{4}((\overline{e}_{1}\overline{e}_{4})\overline{e}_{1}) = e_{4}((\overline{e}_{4}\overline{e}_{1})\overline{e}_{1}) = e_{4}(\overline{e}_{4}e_{1}^{2})$$

$$= -\alpha e_{4}^{2} = -\alpha \gamma$$

$$e_{6}e_{7} = (e_{2}e_{4})(e_{3}e_{4}) \stackrel{*}{=} e_{2}((e_{3}e_{4})e_{4}) = e_{2}(e_{3}e_{4}^{2}) = \gamma e_{2}e_{3} = -\beta \gamma e_{1}$$

$$(*) \text{ Fazendo } e = e_{2}, \ y = e_{4} \text{ e } x = (e_{3}e_{4}) \text{ no Lema } 3.4.2 \text{ (iv)}$$

Evidentemente existem outras maneiras de se efetuar estes cálculos.

Vamos agora relacionar o problema de Hurwitz (Teorema 3.4.3) com o correspondente problema numérico, a que nos referimos como a "soma de quadrados" no início deste capítulo. Tal relação é possível devido à propriedade da forma quadrática q de admitir composição, isto é, q(xy) = q(x)q(y). Ilustraremos esta relação com a álgebra dos quatérnios, uma vez que, para as outras álgebras de composição, o procedimento é idêntico, sendo bastante elementar nos casos do corpo F e das quadráticas (F, α) e um tanto trabalhoso para os octônios.

Consideremos então o produto de dois elementos dos quatérnios, a que chamaremos X e Y, por simplicidade de notação. Façamos $X = a + be_1 + ce_2 + de_3$ e $Y = e + fe_1 + ge_2 + he_3$.

Calculemos
$$XY = (a + be_1 + ce_2 + de_3)(e + fe_1 + ge_2 + he_3)$$

= $(ae + \alpha bf + \beta cg - \alpha \beta dh) + (af + be - \beta ch + \beta dg)e_1$
+ $(ag + ce + \alpha bh - \alpha df)e_2 + (ah + de + bg - cf)e_3$

Pelo que já vimos até agora, resulta imediato que a involução em Q é dada por:

$$\overline{X} = a - be_1 - ce_2 - de_3$$

Calculando $q(X) = X\overline{X} = (a + be_1 + ce_2 + de_3)(a - be_1 - ce_2 - de_3)$ encontramos $q(X) = a^2 - \alpha b^2 - \beta c^2 + \alpha \beta d^2$.

De maneira análoga, obtemos para $Y = e + fe_1 + ge_2 + he_3$

$$q(Y) = e^2 - \alpha f^2 - \beta g^2 + \alpha \beta h^2$$

Da expressão de XY deduzida anteriormente, temos:

$$q(XY) = (ae + \alpha bf + \beta cg - \alpha \beta dh)^2 - \alpha (af + be - \beta ch + \beta dg)^2$$
$$-\beta (ag + ce + \alpha bh - \alpha df)^2 + \alpha \beta (ah + de + bg - cf)^2$$

Se $F=\mathbb{R}$ e $\alpha=\beta=-1$ temos a expressão do produto de uma soma de 4 quadrados é também uma soma de 4 quadrados:

$$(a^{2} + b^{2} + c^{2} + d^{2})(e^{2} + f^{2} + g^{2} + h^{2}) = (ae - bf - cg - dh)^{2} + (af + be + ch - dg)^{2} + (ag + ce - bh + df)^{2} + (ah + de + bg - cf)^{2}.$$

Ainda sobre o Teorema de Hurwitz, é importante destacar as álgebras de composição obtidas fazendo $F = \mathbb{R}$, e os escalares $\alpha = \beta = \gamma = -1$. Ao duplicarmos \mathbb{R} pelo processo de Cayley-Dickson obtemos a Álgebra dos Complexos, $\mathbb{C} = (\mathbb{R}, -1)$. Duplicando \mathbb{C} obtemos os Quatérnios de Hamilton, $\mathbb{H} = (\mathbb{C}, -1)$. Finalmente, a partir de \mathbb{H} chegamos aos Octônios, $\mathbb{O} = (\mathbb{H}, -1)$. São estes casos particulares de álgebras de composição, mais especificamente os dois últimos, que serão estudados no próximo capítulo.

Capítulo 4

Identidades em Álgebras de Cayley

Faremos um breve estudo das identidades de graus 4 e 5 nas álgebras de Cayley, de acordo com algumas das mais recentes pesquisas realizadas sobre o assunto. Nossa abordagem se apóia no artigo *Minimal Identities of Octonion Algebras*, de M. L. Racine (ref. [19]), onde é provado que não existem identidades de grau 4 nas álgebras de octônios e, que as identidades de grau 5 resultam de outras duas identidades conhecidas.

Mencionamos também alguns resultados obtidos por outros estudiosos do assunto sobre identidades de grau 6 ou maior, sempre em um corpo de característica 0 ou maior que o grau da identidade em estudo.

4.1 Introdução

Para uma primeira noção do que é uma identidade, consideremos um corpo F, uma F-álgebra A e um polinômio $f(x_1, \ldots, x_n)$ nas indeterminadas não comutativas e não associativas $x_1, \ldots x_n$ e com coeficientes em F. Dizemos que f é uma identidade de A se $f(a_1, \ldots, a_n) = 0$ para todos $a_1, \ldots, a_n \in A$. Dizemos também que A satisfaz f. Assim, uma álgebra comutativa satisfaz a identidade xy - yx e, uma álgebra associativa satisfaz a identidade (xy)z - x(yz). Daremos adiante uma definição mais formal, abrangendo outros conceitos importantes para as considerações aqui apresentadas.

De fundamental importância para o estudo das identidades são as álgebras de matrizes $M_n(F)$, ou mais genericamente, $M_n(R)$, onde R é um anel comutativo. De que forma se relacionam matrizes e identidades? Para as identidades polinomiais pode-se definir o seu grau. Veremos em breve que uma identidade de grau t satis-

fazendo certas condições é múltipla do polinômio standard do grau t, denotado por s_t , que será definido oportunamente. Escrevemos: $f = \alpha s_t$. Por outro lado, o Teorema de Amitsur-Levitzki, que daremos uma demonstração adiante, afirma que s_{2n} é uma identidade do anel das matrizes de ordem n com coeficientes em R, que designamos por $M_n(R)$.

Vamos agora formalizar estes resultados para podermos abordar as identidades de grau 4 e 5 nas álgebras de Cayley.

4.2 Álgebras Livres

Seja X um conjunto arbitrário, podendo ser infinito. Designamos por V[X] o conjunto obtido a partir de X das palavras não associativas e não comutativas, formado pelos elementos de X mais os parêntesis à esquerda e à direita.

Os elementos de V[X] são agrupamentos convenientes dos elementos de X, de tal forma que se $x_1, x_2, x_3 \in X$, o agrupamento $x_1x_2 \in V[X]$, mas $x_1x_2x_3 \notin V[X]$. Para agrupar mais de dois elementos devemos usar os parêntesis. Assim, $(x_1x_2)x_3 \in V[X]$ e $x_2(x_3x_1) \in V[X]$. É claro que $x_1, x_2 \in V[X]$ e mais ainda, $X \subseteq V[X]$.

Sejam $u, v \in V[X] \setminus X$. Se $x_1, x_2 \in X$, temos que $x_1x_2, x_1(u), (v)x_2, (u)(v) \in V[X]$. Podemos definir em V[X] uma multiplicação. Se $x_1, x_2, u, v \in V[X]$, com $x_1, x_2 \in X$, definimos:

$$x_1 \cdot x_2 = x_1 x_2;$$
 $x_1 \cdot u = x_1(u)$
 $v \cdot x_2 = (v)x_2;$ $u \cdot v = (u)(v)$

Então, \cdot é uma operação binária em V[X], isto é, $x \cdot y \in V[X]$, para todos x, y em V[X]. Seja agora um corpo F. O conjunto V[X] pode ser considerado uma base do F-espaço vetorial F[X], cujos elementos são da forma:

$$\sum_{i} \alpha_i u_i, \quad \alpha_i \in F, \ u_i \in V[X],$$

onde $\sum \alpha_i u_i$ indica uma soma finita.

Definimos uma multiplicação em F[X] estendendo a multiplicação definida em V[X], por:

$$\left(\sum_{i} \alpha_{i} u_{i}\right)\left(\sum_{j} \beta_{j} v_{j}\right) = \sum_{i} \sum_{j} \alpha_{i} \beta_{j} (u_{i} \cdot v_{j}), \quad \alpha_{i}, \beta_{j} \in F, \quad u_{i}, v_{j} \in V[X]$$

Obtemos assim, uma F-álgebra F[X], que é chamada álgebra livre não associativa. Os elementos de F[X] são chamados polinômios não associativos. Um elemento da forma αu , com $\alpha \in F$ e $u \in V[X]$ é chamado um monômio não associativo.

O grau de um monômio é igual ao número de variáveis que nele comparecem, notando que, para todo x em F[X], $xx=x^2$, neste caso contam-se duas variáveis. Citamos alguns exemplos:

$$(uv)w$$
 tem grau 3; $(u^2v)(wx)$ tem grau 5

De maneira análoga, o grau de um polinômio é definido como o maior grau dos monômios que o formam. Assim, o polinômio $u^2 + uv + (uv)w^2$ tem grau 4.

Consideremos agora um conjunto enumerável $X = \{x_1, x_2, \ldots\}$. Seja $f \in F[X]$ arbitrário (sem o termo independente, se A não tiver unidade), que é formado por uma quantidade finita de elementos de X. Indicamos por $f = f(x_1, x_2, \ldots, x_n)$. Seja A uma F-álgebra e a_1, a_2, \ldots, a_n em A. Ao substituirmos os x_i de f pelos a_i obtemos o elemento $f(a_1, a_2, \ldots, a_n)$ em A. O polinômio não associativo e não comutativo f é chamado uma identidade da álgebra A se $f(a_1, a_2, \ldots, a_n) = 0$, para todos a_1, a_2, \cdots, a_n em A.

O conjunto de todas as identidades para uma dada álgebra A é um ideal de F[X], chamado *ideal de identidades* de A ou T-ideal de A, denotado por T(A).

Definição 4.2.1. Seja I um subconjunto de F[X]. A classe de todas as F-álgebras satisfazendo cada identidade de I é chamada **variedade de álgebras** definida pelo conjunto de identidades I.

Exemplos:

- 1. A variedade das F-álgebras associativas é definida pela identidade f = (xy)z x(yz);
- 2. A variedade das F-álgebras alternativas é definida pelas identidades $f_1 = x^2y x(xy)$ e $f_2 = xy^2 (xy)y$, com f_1 definindo as álgebras alternativas à esquerda e f_2 definindo as álgebras alternativas à direita;
- 3. A variedade das álgebras de Lie é definida por $f_1 = x^2$ e $f_2 = (xy)z + (yz)x + (zx)y$

4. A variedade das álgebras de Jordan é definida por

$$f_1 = xy - yx$$
 e $f_2 = (x^2y)x - y^2(yx)$

Serão de importância para o nosso estudo, as variedades de álgebras dos exemplos 1 e 2, acima, nas quais estudaremos as álgebras associativas livres, designadas por Ass[X] e as álgebras alternativas livres, designadas por Alt[X], ambas sobre um conjunto de geradores X.

Dado um monômio nas variáveis x_1, x_2, \ldots, x_s , definimos o seu *tipo* como uma lista de números indicando o grau de cada uma das variáveis, designado por $[n_1, n_2, \ldots, n_s]$. Vejamos alguns exemplos:

- 1. $(x_1^2x_2)(x_2x_3^2)$ é do tipo [2,2,2]
- 2. $((x_1x_2)x_3)(x_3x_2^2)$ é do tipo [1,3,2]
- 3. $(x_1x_3)(x_4(x_1x_3^2))$ é do tipo [2,0,3,1]

Naturalmente, um polinômio f pode ser escrito como soma de monômios.

Definição 4.2.2. Seja f um polinômio nas variáveis x_1, \ldots, x_s , indicado por $f(x_1, \ldots, x_s)$. Dizemos que:

- (i) $f \notin \mathbf{homog\hat{e}neo} \ em \ x_i, \ 1 \leq i \leq s, \ se \ o \ grau \ de \ x_i \ for \ o \ mesmo \ em \ cada monômio \ de \ f;$
- (ii) $f \notin \mathbf{homog\hat{e}neo}$, se for homog $\hat{e}neo \ em \ x_i, \ \forall i = 1, \dots, s;$
- (iii) $f \notin \mathbf{linear} \ em \ x_i, \ 1 \leq i \leq s, \ se \ grau \ de \ x_i = 1 \ em \ cada \ monômio \ de \ f;$
- (iv) $f \notin \mathbf{linear}$, se for linear em x_i , $\forall i = 1, \dots, s$;
- (v) $f \notin \mathbf{t\text{-linear}}, 1 \le t \le s, \text{ se for linear em } x_i, i = 1, \dots, t;$
- (vi) $f \notin \mathbf{multilinear}$, se grau de $x_i = 0$ ou grau de $x_i = 1, \forall i = 1, \dots, s$;
- (vii) $f \notin \mathbf{t}$ -alternado, $se\ f(x_1, \dots, x_i, \dots, x_j, \dots) = -f(x_1, \dots, x_j, \dots, x_i, \dots)$ $\forall i, j, 1 \leq i, j \leq t, i \neq j;$
- (viii) f é alternado, se for s-alternado;

- (ix) f é t-normal, se for t-linear e t-alternado;
- (x) f é normal, se for linear e alternado.

Os conceitos de grau, homogeneidade e polinômio multilinear homogêneo, conforme definidos acima, se aplicam à álgebra livre não associativa e não comutativa F[X], sobre um conjunto gerador X. Para podermos aplicar estes conceitos nas álgebras associativas livres Ass[X] e nas álgebras alternativas livres Alt[X], precisamos identificar qual é o conjunto gerador X para tais álgebras. Porém, não se conhece uma base natural em Alt[X].

Passamos então a considerar o ideal I das identidades definidoras da variedade das álgebras associativas, que é o ideal gerado pelo conjunto

$$I_0 = \{(x, y, z) \mid x, y, z \in F[X]\}.$$

Podemos escrever ainda: Ass[X] = F[X]/I. Assim, cada elemento de Ass[X], isto é, cada identidade polinomial associativa, é a imagem do homomorfismo canônico de um polinômio em F[X], retirando-se os parêntesis. Designando este homomorfismo por $\phi: F[X] \to Ass[X]$, se $f \in F[X]$, então ϕf é a imagem de f por ϕ e $\phi f \in Ass[X]$.

De maneira análoga, seja J o ideal das identidades definidoras das álgebras alternativas. Então, J é o ideal gerado pelo conjunto

$$J_0 = \{(x, x, y); (z, t, t) \mid x, y, z, t \in F[X]\}.$$

Assim, Alt[X] = F[X]/J e, designando por $\nu : F[X] \to Alt[X]$ o homomorfismo canônico entre estas duas álgebras, temos que, se $f \in F[X]$, então $\nu f \in Alt[X]$.

4.3 Identidades Polinomiais

Consideremos agora o grupo simétrico de ordem t, que denotaremos por S_t , também chamado de grupo de permutações, que é formado pelas permutações de t elementos. Cada permutação será designada por π , em geral, afetada de um índice, como π_1 ou π_{i_1} . O grupo simétrico S_t está intimamente relacionado com os polinômios multilineares associativos, uma vez que podemos facilmente verificar que se f é um polinômio multilinear de grau t em Ass[X], então:

$$f = \sum_{\pi \in S_t} \alpha_{\pi} x_{\pi_1} \cdots x_{\pi_t}, \quad \text{com } \alpha_{\pi} \in F$$

Temos ainda que os polinômios multilineares associativos de grau t, designados por P_t , são isomorfos à álgebra de grupo FS_t , e que P_t é um S_t -módulo.

Vejamos alguns exemplos:

O grupo simétrico do grau 2 é simplesmente formado pelas permutações (12) e
 (21). Assim, um polinômio multilinear do grau 2 poderá ser escrito:

$$f(x_1, x_2) = \alpha x_1 x_2 + \beta x_2 x_1, \quad \text{com } \alpha, \beta \in F.$$

2. Em grau 3, temos 3! = 6 permutações de 3 elementos: (123), (132), (213), (231), (312), (321). Então um polinômio multilinear do grau 3 terá a forma:

$$f(x_1, x_2, x_3) = \alpha_1 x_1 x_2 x_3 + \alpha_2 x_1 x_3 x_2 + \dots + \alpha_6 x_3 x_2 x_1, \quad \text{com } \alpha_i \in F.$$

3. Um caso particular de polinômio multilinear de grau 3 é:

$$f_1(x_1, x_2, x_3) = \alpha x_1 x_3 x_2 + \beta x_2 x_3 x_1, \quad \alpha, \beta \in F$$

Definição 4.3.1. O polinômio standard do grau t é dado por:

$$s_t(x_1,\ldots,x_t) = \sum_{\pi \in S_t} (\operatorname{sgn}\pi) x_{\pi_1} \cdots x_{\pi_t}$$

onde S_t é o grupo das permutações de t elementos e $\operatorname{sgn}\pi$ indica o sinal da permutação.

Vê-se claramente que s_t é um polinômio normal. Examinaremos a seguir alguns critérios que permitem estabelecer quando um polinômio linear é normal. No que segue, assumiremos que f é um polinômio t-linear.

Definição 4.3.2. Para todas as permutações $\pi \in S_k$, $k \le t$, definimos $f_{(k,\pi)}$ como a soma dos monômios nos quais as variáveis x_1, \ldots, x_k aparecem na ordem $x_{\pi_1} \cdots x_{\pi_k}$ $Se \pi = 1$ (permutação identidade) escrevemos $f_{(k)}$. Em particular, se k = t, obtemos: $f = \sum_{\pi \in S_t} f_{(t,\pi)}$.

Definição 4.3.3. Seja $f(x_1, ..., x_s)$ um polinômio t-linear. Definimos a composta $\pi \circ f, \pi \in S_t$, por:

$$f(x_{\pi_1},\ldots,x_{\pi_t},x_{t+1},\ldots,x_s).$$

Para ilustrar um caso simples de uso da composta, podemos fazer $\pi=(12)$ e $f=x_1x_3x_2+x_3x_2x_1+x_2x_1x_3$. Então $(12)\circ f=x_2x_3x_1+x_3x_1x_2+x_1x_2x_3$.

Lema 4.3.1. Um polinômio t-linear f é t-normal se e somente se $(ij) \circ f = -f$ $\forall i < j \leq t$.

Demonstração: (\Rightarrow) Se f é normal, então:

$$(ij) \circ f + f = f(\dots, x_j, \dots, x_i, \dots) + f(\dots, x_i, \dots, x_j, \dots)$$

= $f(\dots, x_i + x_j, \dots, x_i + x_j, \dots) - f(\dots, x_i, \dots, x_i, \dots)$
 $-f(\dots, x_j, \dots, x_j, \dots) = 0$

(\Leftarrow) Por hipótese, $(ij) \circ f = -f$. Podemos escrever $f = \sum_{\pi \in S_t} f_{(t,\pi)}$. Então $(ij) \circ f_{(t,\pi)} = -f_{(t,(ij)\pi)}, \ \forall \ \pi \in S_t$.

Consideremos o conjunto $G = \{ \pi \in S_t \mid \pi(i) < \pi(j) \}.$

Assim:
$$f = \sum_{\pi \in G} (f_{(t,\pi)} + f_{(t,(ij)\pi)}) = \sum_{\pi \in G} (f_{(t,(ij)\pi)} - (ij) \circ f_{(t,\pi)}).$$

Agora, fazendo i = j, seja $f(\ldots, x_i, \ldots, x_i, \ldots)$. Temos:

$$f(\dots, x_i, \dots, x_i, \dots) = \sum_{\pi \in G} (f_{(t,\pi)}(\dots, x_i, \dots, x_i, \dots) - (ij) \circ f_{(t,\pi)}(\dots, x_i, \dots, x_i, \dots))$$

= $\sum_{\pi \in G} (f_{(t,\pi)}(\dots, x_i, \dots, x_i, \dots) - f_{(t,\pi)}(\dots, x_i, \dots, x_i, \dots)) = 0$

Portanto f é normal.

Lema 4.3.2. $f \notin t$ -normal se e somente se, $\forall \pi \in S_t, f_{(t,\pi)} = (\operatorname{sgn} \pi)\pi \circ f_{(t)}$.

Demonstração: Lembrando que $f_{(t,\pi)}$ é a soma dos monômios de f em que as variáveis x_1, \ldots, x_t aparecem na ordem π_1, \ldots, π_t . Toda permutação é um produto de transposições. Se π for produto de um número par de transposições, π é uma permutação par e, será uma permutação ímpar se for produto de um número ímpar de transposições. Seja $\pi \in S_t$. Temos que: $\pi = \tau_1 \ldots \tau_s$, onde cada τ_i é uma transposição, $1 \le i \le s$.

Pelo lema anterior, $(ij) \circ f = -f$ e, em particular, $(ij) \circ f_{(t)} = -f_{(t)}$, ou especificamente, para a permutação π fixada, $\tau_1 \circ f_{(t)} = -f_{(t)}$. Aplicando sucessivamente τ_2, \ldots, τ_s obtemos: $f_{(t,\pi)} = (\operatorname{sgn} \pi)\pi \circ f_{(t)}$.

Lema 4.3.3. $f \notin t$ -normal se e somente se $f = \sum_{\pi \in S_t} (\operatorname{sgn} \pi) \pi \circ f_{(t)}$

Demonstração: Resulta imediatamente do fato visto no Lema 4.3.1, de que $f = \sum_{\pi \in S_t} f_{(t,\pi)}$ e do lema anterior.

Proposição 4.3.4. Se f é normal de grau t então $f = \alpha s_t$ para algum $\alpha \in F$.

Demonstração: Sabemos, da definição do polinômio $f_{(k,\pi)}$, que se k=t, então $f=\sum_{\pi\in S_t}f_{(t,\pi)}$. Ainda, para cada $\pi\in S_t$:

$$f_{(t,\pi)}(x_1,\ldots,x_t) = \alpha_{\pi}x_{\pi_1}\ldots x_{\pi_t}, \ \alpha_{\pi} \in F, \text{ e se } \pi = 1$$
:

$$f_{(t)}(x_1,\ldots,x_t)=\alpha x_1\ldots x_t, \ \alpha\in F.$$

Pelo Lema 4.3.2, $f_{(t,\pi)} = (\operatorname{sgn} \pi)\pi \circ f_{(t)}$. Então:

$$\alpha_{\pi} x_{\pi_1} \dots x_{\pi_t} = (\operatorname{sgn} \pi) \pi \circ \alpha x_1 \dots x_t = (\operatorname{sgn} \pi) \alpha x_{\pi_1} \dots x_{\pi_t} \Rightarrow \alpha_{\pi} = (\operatorname{sgn} \pi) \alpha.$$

Escrevemos então:

$$f = \sum_{\pi \in S_t} (\operatorname{sgn}\pi) \alpha x_{\pi_1} \dots x_{\pi_t} = \alpha \sum_{\pi \in S_t} (\operatorname{sgn}\pi) x_{\pi_1} \dots x_{\pi_t} \Rightarrow f = \alpha s_t$$

Proposição 4.3.5. Seja
$$f = \sum_{\pi \in S_{2t}} (\operatorname{sgn} \pi) [x_{\pi_1}, x_{\pi_2}] \dots [x_{\pi_{(2t-1)}}, x_{\pi_{(2t)}}]$$
. Então $f = 2^t s_{2t}$.

Demonstração: Cada comutador se desenvolve numa soma de monômios da forma $x_{\pi_{(i)}}x_{\pi_{(i+1)}} - x_{\pi_{(i+1)}}x_{\pi_{(i)}}$. Fixemos $\pi \in S_t$. O produto de todos estes t binômios (pois são t comutadores) é formado por 2^t parcelas onde em cada uma aparecem todas as 2t variáveis x_1, \ldots, x_{2t} sem repetição. Assim, cada parcela é da forma $x_{\pi_1} \ldots x_{\pi_{(2t)}}$. Para a permutação π fixada temos então:

$$[x_{\pi_1}, x_{\pi_2}] \dots [x_{\pi_{(2t-1)}}, x_{\pi_{(2t)}}] = 2^t x_{\pi_1} \dots x_{\pi_{(2t)}}$$

$$\Rightarrow f = \sum_{\pi \in S_{2t}} (\operatorname{sgn}\pi) 2^t [x_{\pi_1}, x_{\pi_2}] \dots [x_{\pi_{(2t-1)}}, x_{\pi_{(2t)}}]$$

$$= 2^t \sum_{\pi \in S_{2t}} (\operatorname{sgn}\pi) [x_{\pi_1}, x_{\pi_2}] \dots [x_{\pi_{(2t-1)}}, x_{\pi_{(2t)}}]$$

$$\Rightarrow f = 2^t s_{2t}$$

Proposição 4.3.6. Para o polinômio standard s_t , valem as seguintes igualdades:

(i)
$$s_t = \sum_{i=1}^t (-1)^{i-1} x_i s_{t-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_t);$$

(ii)
$$s_t = \sum_{i=1}^t (-1)^{t-1} s_{t-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_t) x_i$$
.

Demonstração:

(i) Faremos indução em t. Como, pela própria expressão, é imediato que, sendo ela válida para k é também válida para k+1, basta verificar para um valor inicial de t, digamos, t=3. Teremos:

$$s_3(x_1, x_2, x_3) = x_1 x_2 x_3 - x_1 x_3 x_2 + x_2 x_1 x_3 - x_2 x_3 x_1 + x_3 x_1 x_2 - x_3 x_2 x_1$$

$$= x_1(x_2 x_3) - x_2(x_1 x_3 - x_3 x_1) + x_3(x_1 x_2 - x_2 x_1)$$

$$= x_1 s_2(x_1, x_2) - x_2 s_2(x_1, x_3) + x_3 s_2(x_1 x_2)$$

$$= \sum_{i=1}^{3} (-1)^{i-1} x_i s_2(\dots, x_{i-1}, x_{i+1}, \dots)$$

(ii) É inteiramente análoga.

Neste ponto introduziremos as matrizes em conjunto com o polinômio standard, e mostraremos duas propriedades do *traço* de uma matriz. Uma delas será usada na demonstração do *Teorema de Amitsur-Levitzki*, de vital importância no estudo das identidades.

Lema 4.3.7. Seja $M_n(R)$ o anel das matrizes de ordem n sobre um anel comutativo arbitrário R. Então $tr[M_n(R), M_n(R)] = 0$.

Demonstração: Sejam $A, B \in M_n(R)$. Devemos mostrar que tr[A, B] = 0. Isto equivale a: $tr(AB - BA) = 0 \Rightarrow tr(AB) - tr(BA) = 0$, pois o traço é aditivo. Vamos então mostrar que tr(AB) = tr(BA).

$$AB = (AB)_{ij} = \left(\sum_{k=1}^{n} a_{ik} b_{kj}\right)_{ij}$$

$$tr(AB) = \sum_{k=1}^{n} a_{1k} b_{k1} + \dots + \sum_{k=1}^{n} a_{nk} b_{kn} = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} b_{ki}$$

$$BA = (BA)_{ij} = \left(\sum_{k=1}^{n} b_{ik} a_{kj}\right)_{ij}$$

$$tr(BA) = \sum_{i=1}^{n} \sum_{k=1}^{n} b_{ik} a_{ki} = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ki} b_{ik} = tr(AB)$$

Proposição 4.3.8. Seja R um anel comutativo arbitrário e $A_1, \ldots, A_{2k} \in M_n(R)$. $Então\ trs_{2k}(A_1, \ldots, A_{2k}) = 0$, para k, n arbitrários.

Demonstração: Pelas propriedades do polinômio standard, dadas na Proposição 4.3.6, podemos escrever:

$$2trs_{2k}(A_1, \dots, A_{2k}) = tr\left(\sum_{i=1}^{2k} (-1)^{i-1} A_i s_{2k-1}(A_1, \dots, A_{i-1}, A_i, \dots, A_{2k})\right) + tr\left(\sum_{i=1}^{2k} (-1)^{2k-i} s_{2k-1}(A_1, \dots, A_{i-1}, A_i, \dots, A_{2k})a_i\right)$$

Simplificando um pouco a notação, calculamos:

$$2trs_{2k}(A_1, \dots, A_{2k}) = tr\left(\sum_{i=1}^{2k} (-1)^{i-1} A_i s_{2k-1}\right) + tr\left(\sum_{i=1}^{2k} (-1)^{2k-i} s_{2k-1} A_i\right)$$

$$= tr(A_1 s_{2k-1}) - tr(s_{2k-1} A_1) - tr(A_2 s_{2k-1}) + tr(s_{2k-1} A_2)$$

$$+ \dots - tr(A_{2k} s_{2k-1}) + tr(s_{2k-1} A_{2k})$$

$$= tr(A_1 s_{2k-1} - s_{2k-1} A_1) - tr(A_2 s_{2k-1} - s_{2k-1} A_2)$$

$$+ \dots - tr(A_{2k} s_{2k-1} - s_{2k-1} A_{2k})$$

$$= tr[A_1 s_{2k-1}, s_{2k-1} A_1] - tr[A_2 s_{2k-1} - s_{2k-1} A_2]$$

$$+ \dots - tr[A_{2k} s_{2k-1} - s_{2k-1} A_{2k}]$$

Vemos assim que, quando i é par, $tr[A_i, s_{2k-1}]$ é afetado do sinal -, e quando i é ímpar, esta expressão leva o sinal +. Podemos escrever então, voltando à notação de somatório:

$$2trs_{2k}(A_1,\ldots,A_{2k}) = \sum_{i=1}^{2k} (-1)^{i-1} tr[A_i, s_{2k-1}(A_1,\ldots,A_{i-1},A_i,\ldots,A_{2k})]$$

De acordo com o Lema 4.3.7 o segundo membro se anula, pois é uma soma do traço do comutador de matrizes em $M_n(R)$. Portanto $trs_{2k}(A_1, \ldots, A_{2k}) = 0$.

Os resultados que acabamos de apresentar formam o embasamento teórico para o estudo das identidades nos octônios. Para completar tais fundamentos necessitamos do Teorema de Amitsur-Levitzki, que afirma que o polinômio standard s_{2n} é uma identidade em $M_n(R)$ (ou $M_n(F)$, F corpo). Daremos a demonstração devida a Rosset (ref. [20]), que considera este teorema como uma conseqüência do Teorema de Cayley-Hamilton para matrizes. Esta demonstração faz uso de resultados referentes a álgebra exterior. Para isto dedicaremos a próxima seção a um estudo sucinto desta álgebra. Maiores detalhes podem ser encontrados em [23].

4.4 A Álgebra Exterior - Principais Resultados

Sejam U, V espaços vetoriais sobre um mesmo corpo F, com dim U=m e dim V=n. Queremos definir um "espaço produto" entre U e V. A primeira idéia que poderia nos ocorrer seria o produto cartesiano $U \times V$. Mas, notando que, se $(u_1, v), (u_2, v) \in U \times V$, então $(u_1, v) + (u_2, v) \neq (u_1 + u_2, v)$. Mas se w for uma função bilinear, $w : U \times V \to F$, então, para todos $u, u_1, u_2 \in U$, $v, v_1, v_2 \in V$ e $a \in F$:

(i)
$$w(u_1 + u_2, v) = w(u_1, v) + w(u_2, v);$$

(ii)
$$w(u, v_1 + v_2) = w(u, v_1) + w(u, v_2);$$

(iii)
$$w(au, v) = w(u, av) = aw(u, v)$$
.

Define-se o produto tensorial de U por V como sendo o espaço dual do espaço das funções bilineares de $U \times V$ em F. Denotamos por $U \otimes V$:

$$U \otimes V = L^*(U \times V; F) = L(L(U \times V; F); F)$$

Assim, os elementos de $U \otimes V$ são funcionais lineares em $L(U \otimes V; F)$, e tem-se dim $U \otimes V = \dim L(U \otimes V; F) = mn$. Dos resultados conhecidos sobre funcionais lineares, sabemos que, se $\{u_1, \ldots, u_m\}$ é uma base de U e $\{v_1, \ldots, v_n\}$ é uma base de V, então $\{\alpha_{ij}\}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, é uma base de $L(U \otimes V; F)$, onde α_{ij} é um funcional bilinear definido por:

$$\alpha_{ij}(u_k, v_l) = \begin{cases} 1 & \text{se } i = k \text{ e } j = l \\ 0 & \text{caso contrário} \end{cases}$$

Definimos $(u_i \otimes v_j)(\alpha_{kl}) = \alpha_{kl}(u_i, v_j)$. Assim, $(u_i \otimes v_j)$, $1 \leq i \leq m$, $1 \leq j \leq n$, é uma base de $U \otimes V$. Por exemplo, se m = 2 e n = 3, então $U \otimes V$ tem dimensão 6 e sua base será:

$$\{u_1 \otimes v_1, u_1 \otimes v_2, u_1 \otimes v_3, u_2 \otimes v_1, u_2 \otimes v_2, u_2 \otimes v_3\}$$

Um elemento de $U \otimes V$ é escrito como $\sum_{ij} a_{ij} (u_i \otimes v_j)$.

Estendemos naturalmente a definição de produto tensorial para um número maior de espaços vetoriais. Sejam, então U_1, \ldots, U_r espaços vetoriais de dimensão finita. Uma função multilinear em r variáveis é uma aplicação $\alpha: U_1 \times \ldots \times U_r \to F$, que é linear em cada variável, sendo também chamada de uma r-forma. Assim, podemos considerar que um funcional linear é uma 1-forma, um funcional bilinear é uma 2-forma, e assim por diante. Também chamamos de uma 0-forma, um elemento do corpo F.

O espaço vetorial de todas as r-formas é $L(U_1, \ldots, U_r; F)$ e o seu dual é o espaço tensorial $U_1 \otimes \ldots \otimes U_r$.

Consideremos agora as r-formas do tipo

$$\alpha: V \times \ldots \times V \to F$$

O espaço vetorial de todas as formas deste tipo é $L(V^r; F)$ e o seu dual é chamado espaço tensorial contravariante de ordem r, denotado por $\overset{r}{\otimes} V$. Se dim V=n, então dim $\overset{r}{\otimes} V=n^r$.

Sejam $v_1, \ldots, v_r \in V$. Uma r-forma α pode ser calculada nestes v_i , resultando $\alpha(v_1, \ldots, v_r) = k, \ k \in F$. Poderíamos perguntar o que acontece quando permutamos os v_i , isto é, quando calculamos $\alpha(v_{\pi_1}, \ldots, v_{\pi_r})$, sendo $\pi \in S_r$, o grupo das permutações de r elementos. Interessam-nos somente as r-formas que satisfazem as seguintes condições:

1. Uma r-forma α em V é dita simétrica se

$$\alpha(v_1,\ldots,v_r)=\alpha(v_{\pi_1},\ldots,v_{\pi_r}), \ \forall \ v_i\in V \ \forall \ \pi\in S_r$$

2. Uma r-forma α em V é dita anti-simétrica se

$$\alpha(v_1, \ldots, v_r) = \operatorname{sgn}(\pi)\alpha(v_{\pi_1}, \ldots, v_{\pi_r}), \ \forall \ v_i \in V \ \forall \ \pi \in S_r,$$

onde $\operatorname{sgn}(\pi)$ é o sinal de π .

3. Uma r-forma α em V é dita alternada se for igual a 0 sempre que houver duas variáveis repetidas.

Toda forma alternada é anti-simétrica. Se o corpo F tem característica $\neq 2$, então toda forma anti-simétrica é também alternada. De fato, seja α anti-simétrica. Então $\alpha(v_1, v_1, \ldots, v_r) = -\alpha(v_1, v_1, \ldots, v_r) \Rightarrow 2\alpha(v_1, v_1, \ldots, v_r) = 0$. E como F não é de característica 2, segue que $\alpha(v_1, v_1, \ldots, v_r) = 0$. Portanto α é alternada.

O conjunto das r-formas sim'etricas em V, denotado por $L_S(V^r;F)$ é um subespaço de $L(V^r;F)$, como se verifica facilmente. Da mesma maneira o conjunto das r-formas alternadas em V, denotado por $L_A(V^r;F)$ é um subespaço de $L(V^r;F)$. Seja $\{v_i\}$ uma base de V. É possível provar que a dimensão de $L_A(V^r;F)$ é dada por

$$\dim L_A(V^r; F) = \left\{ \begin{array}{c} \binom{n}{r} & \text{se } r \leq n \\ 0 & \text{se } r > n \end{array} \right.$$

Definição 4.4.1. Seja V um espaço vetorial de dimensão n. O produto exterior de ordem r de V é o dual das r-formas alternadas, $L_A(V^r; F)$, denotado por $\stackrel{r}{\wedge} V$. Em símbolos: $\stackrel{r}{\wedge} V = L_A^*(V^r; F) = L(L_A(V^r; F); F)$.

Observação: A definição acima é restrita para característica zero. Para uma definição mais geral que independe da característica do corpo, veja, por exemplo, Jacobson (ref. [13]).

Tem-se também: dim
$$L_A(V^r; F) = \binom{n}{r} \Rightarrow {}^r V = \binom{n}{r}$$

Sejam x_1, \ldots, x_r elementos fixados de V, e α uma r-forma em $L_A(V^r; F)$. Um elemento de $\stackrel{r}{\wedge} V$ é um funcional linear (1-forma) que associa a cada $\alpha \in L_A(V^r; F)$, um escalar. Assim, se definirmos

$$\beta: L_A(V^r; F) \to F$$

$$\alpha \mapsto \beta(\alpha) = \alpha(x_1, \dots, x_r)$$
(1)

então $\beta \in \stackrel{r}{\wedge} V$. Um elemento β de $\stackrel{r}{\wedge} V$ é uma 1-forma, como definido em (1), e é chamado produto exterior de x_1, \ldots, x_r . Usamos a notação $\beta = x_1 \wedge \ldots \wedge x_r$. Assim, podemos reescrever (1):

$$(x_1 \wedge \ldots \wedge x_r)(\alpha) = \alpha(x_1, \ldots, x_r)$$

É possível provar que se $\{v_1, \ldots, v_r\}$ é uma base de V, então o conjunto de $\binom{n}{r}$ vetores $v_{i_1} \wedge v_{i_2} \wedge \ldots \wedge v_{i_r}$, com $1 \leq i_1 < i_2 < \ldots < i_r \leq n$ é uma base de $\stackrel{r}{\wedge} V$. Vejamos alguns exemplos:

1. Se r=2 e n=3, $\binom{3}{2}=3$; $\{v_1,v_2,v_3\}$ é base de V e $\{v_1 \wedge v_2, v_1 \wedge v_3, v_2 \wedge v_3\}$ é base de $\stackrel{2}{\wedge}V$. Todo elemento de $\stackrel{2}{\wedge}V$ é da forma

$$x = \lambda_{12}v_1 \wedge v_2 + \lambda_{13}v_1 \wedge v_3 + \lambda_{23}v_2 \wedge v_3, \ \lambda_{ij} \in F.$$

2. Se r=2 e n=4, $\left(\begin{array}{c}4\\2\end{array}\right)=6$, daí: $\left\{v_1\wedge v_2,v_1\wedge v_3,v_1\wedge v_4,v_2\wedge v_3,v_2\wedge v_4,v_3\wedge v_4\right\}$ é base de $\stackrel{2}{\wedge}V$. Um elemento $x\in V\times V$ tem a forma

$$\sum_{i,j} \lambda_{ij}(v_i \wedge v_j), \quad 1 \leq i < j \leq 4, \ \lambda_{ij} \in F$$

3. Se
$$r = 3$$
 e $n = 4$, $\binom{4}{3} = 4$, e uma base de $\stackrel{3}{\wedge} V$ é $\{v_1 \wedge v_2 \wedge v_3, v_1 \wedge v_2 \wedge v_4, v_1 \wedge v_3 \wedge v_4, v_2 \wedge v_3 \wedge v_4\}$

Um elemento de $\stackrel{r}{\wedge} V$ é chamado um r-vetor. Se um elemento de $\stackrel{r}{\wedge} V$ puder ser escrito como produto exterior de r elementos de V, então tal elemento é chamado um $r\text{-}vetor\ simples$. Usa-se a notação $v^{(r)}$ para indicar um $r\text{-}vetor\ simples$.

Consideremos agora dois produtos exteriores, $\overset{r}{\wedge} V$ e $\overset{s}{\wedge} V$, com $r \neq s$. Sejam $v^{(r)} \in \overset{r}{\wedge} V$ um r-vetor simples e $v^{(s)} \in \overset{s}{\wedge} V$ um s-vetor simples. Podemos escrever:

$$v^{(r)} = x_1 \wedge ... \wedge x_r$$
 e $v^{(s)} = x_{r+1} \wedge ... \wedge x_{r+s}$

com $x_i \in V, i = 1, ..., r + s$. Vamos definir o produto exterior de $v^{(r)}$ por $v^{(s)}$ como

$$v^{(r)} \wedge v^{(s)} = x_1 \wedge \ldots \wedge x_r \wedge x_{r+1} \wedge \ldots \wedge x_{r+s}$$
.

Claro que esta definição só tem sentido se $r+s \leq n$, onde $n=\dim V$. Mas podemos ter elementos em $\stackrel{r}{\wedge} V$ (e em $\stackrel{s}{\wedge} V$) que não são simples. Porém são combinações lineares de elementos da base de $\stackrel{r}{\wedge} V$, isto é, de r-vetores simples. Assim, qualquer vetor $v^{(r)} \in \stackrel{r}{\wedge} V$ pode ser escrito:

$$v^{(r)} = \sum_{i=1}^{\binom{n}{r}} \lambda_i v_i^{(r)}, \quad \lambda_i \in F.$$

onde cada elemento da base de $\stackrel{r}{\wedge} V$ foi designado por $v_i^{(r)}$. Como um exemplo, se r=3 e n=4, a base de $\stackrel{3}{\wedge} V$ é

$$\{v_1^{(3)} = v_1 \wedge v_2 \wedge v_3, \ v_2^{(3)} = v_1 \wedge v_2 \wedge v_4, \ v_3^{(3)} = v_1 \wedge v_3 \wedge v_4, \ v_4^{(3)} = v_2 \wedge v_3 \wedge v_4\}$$

Um elemento qualquer de $\stackrel{3}{\wedge}V$ é um 3-vetor, que pode ser escrito como:

$$v^{(3)} = \sum_{i=1}^{4} \lambda_i v_i^{(3)}, \ \lambda_i \in F.$$

Vamos definir o produto exterior de um r-vetor por um s-vetor, estendendo a definição dada para vetores simples. Sejam $v^{(r)} = \sum_i \lambda_i v_i^{(r)}$ e $v^{(s)} = \sum_j \mu_j v_j^{(s)}$, $\lambda_i, \mu_j \in F$. Definimos:

$$v^{(r)} \wedge v^{(s)} = \left(\sum_{i} \lambda_i v_i^{(r)}\right) \wedge \left(\sum_{j} \mu_j v_j^{(s)}\right) = \sum_{i,j} \lambda_i \mu_j (v_i^{(r)} \wedge v_j^{(s)})$$

É possível provar que:

- 1. Esta definição é válida, isto é, independe de como $v^{(r)}$ e $v^{(s)}$ são escritos em termos de vetores simples;
- 2. $v^{(r)} \wedge v^{(s)} = (-1)^{rs} v^{(s)} \wedge v^{(r)}$.

Seja V um F-espaço vetorial de dimensão n. Definimos:

$$\wedge V = \stackrel{0}{\wedge} V \oplus \stackrel{1}{\wedge} V \oplus \cdots \oplus \stackrel{n}{\wedge} V = \bigoplus_{r=0}^{n} \stackrel{r}{\wedge} V$$

onde $\overset{0}{\wedge}V=F$ e $\overset{1}{\wedge}V=V.$ Tem-se ainda:

$$\dim \wedge V = \begin{pmatrix} n \\ 0 \end{pmatrix} + \begin{pmatrix} n \\ 1 \end{pmatrix} + \dots + \begin{pmatrix} n \\ n \end{pmatrix} = 2^n$$

Vamos definir um produto em $\wedge V$. Sejam $v_1 = \bigoplus_{r=0}^n v_1^{(r)}$ e $v_2 = \bigoplus_{s=0}^n v_2^{(r)}$. Definimos: $v_1 \wedge v_2 = \bigoplus_{r=1}^n \sum_{r} v_1^{(r)} \wedge v_2^{(s)}.$

É fácil verificar que $\wedge V$ com o produto assim definido é uma álgebra. A álgebra $\wedge V$ assim constituída é chamada álgebra exterior ou álgebra de Grassmann. Vejamos alguns exemplos:

- 1. n=3: $\{e_1,e_2,e_3\}$ base de V, $\wedge V=F\oplus V\oplus \overset{2}{\wedge}V\oplus \overset{3}{\wedge}V$, $\dim \wedge V=2^3=8$. Sejam $v_1, v_2 \in \wedge V$. Vamos explicitar cada um deles como soma direta de elementos de cada $\stackrel{\imath}{\wedge} V,\ i=1,2,3,4.$ Assim, na notação indicada anteriormente, $v_1 = v_1^{(0)} \oplus v_1^{(1)} \oplus v_1^{(2)} \oplus v_1^{(3)}$ e $v_2 = v_2^{(0)} \oplus v_2^{(1)} \oplus v_2^{(2)} \oplus v_2^{(3)}$, onde

 - (i) $v_1^{(0)} \in F$ $\Rightarrow v_1^{(0)} = \lambda$ (ii) $v_1^{(1)} \in V$ $\Rightarrow v_1^{(1)} = \lambda_{11}e_1 + \lambda_{12}e_2 + \lambda_{13}e_3$
 - (iii) $v_1^{(2)} \in {}^2V \implies v_1^{(2)} = \lambda_{21}e_1 \wedge e_2 + \lambda_{22}e_1 \wedge e_3 + \lambda_{23}e_2 \wedge e_3$
 - (iv) $v_1^{(3)} \in {}^{3}V \implies v_1^{(3)} = \lambda_{31}e_1 \wedge e_2 \wedge e_3$

onde $\lambda, \lambda_{ij} \in F$, i, j = 1, 2, 3.

Naturalmente temos expressões análogas para v_2 . Assim, uma base de $\wedge V$, para dim V = 3 é:

$$\{1, e_1, e_2, e_3, e_1 \land e_2, e_1 \land e_3, e_2 \land e_3, e_1 \land e_2 \land e_3\}$$

Vamos calcular o produto $v_1 \wedge v_2$ de acordo com a definição dada:

$$v_{1} \wedge v_{2} = \bigoplus_{t=0}^{3} \sum_{r+s=t} v_{1}^{(r)} \wedge v_{2}^{(s)}$$

$$= v_{1}^{(0)} \wedge v_{2}^{(0)} \oplus v_{1}^{(0)} \wedge v_{2}^{(1)} \oplus v_{1}^{(1)} \wedge v_{2}^{(0)} \oplus v_{1}^{(0)} \wedge v_{2}^{(2)} \oplus v_{1}^{(2)} \wedge v_{2}^{(0)} \oplus v_{1}^{(1)} \wedge v_{2}^{(1)}$$

$$\oplus v_{1}^{(0)} \wedge v_{2}^{(3)} \oplus v_{1}^{(1)} \wedge v_{2}^{(2)} \oplus v_{1}^{(2)} \wedge v_{2}^{(1)} \oplus v_{1}^{(3)} \wedge v_{2}^{(0)}$$

2. Se n=4, o produto $v_1 \wedge v_2$ apresenta os mesmos termos acima mais os termos correspondentes a t=4. Indicamos sinteticamente:

$$v_{1} \wedge v_{2} = \overset{(t=0)}{\cdots} \oplus \overset{(t=1)}{\cdots} \oplus \overset{(t=2)}{\cdots} \oplus \overset{(t=3)}{\cdots}$$

$$\oplus v_{1}^{(0)} \wedge v_{2}^{(4)} \oplus v_{1}^{(1)} \wedge v_{2}^{(3)} \oplus v_{1}^{(2)} \wedge v_{2}^{(2)} \oplus v_{1}^{(3)} \wedge v_{2}^{(1)} \oplus v_{1}^{(4)} \wedge v_{2}^{(0)}$$

Encerramos esta seção com a demonstração do Teorema de Amitsur-Levitzki. Precisaremos ainda de um lema que trata das *fórmulas de Newton* para matrizes genéricas. Daremos apenas uma idéia da sua demonstração, cujos detalhes podem ser vistos em [21].

Lema 4.4.1 (Fórmulas de Newton). Seja $A \in M_n(F)$ e $(-1)^k \alpha_k$ o coeficiente de λ^{n-k} no polinômio característico da matriz A, então:

$$k\alpha_k = \sum_{i=1}^k (-1)^{i-1} \alpha_{k-i} tr(A^i), \ \forall k, \ 1 \le k \le n.$$

Demonstração: $(id\acute{e}ia)$ Considera o polinômio característico q da matriz A na variável λ . Calcula a derivada formal q' em relação a λ e a desenvolve em série de potências. Deste desenvolvimento obtém-se as fórmulas de Newton.

Teorema 4.4.2 (Amitsur-Levitzki). O polinômio standard s_{2n} é uma identidade na álgebra $M_n(F)$ das matrizes de ordem n sobre um corpo F.

Demonstração: Seja V espaço vetorial de dimensão 2n sobre um corpo F com car F = 0. Para facilitar a notação vamos indicar por E a álgebra exterior de V, ao invés de $\wedge V$. Seja $\{e_1, \ldots, e_{2n}\}$ uma base de V e consideremos 2n matrizes A_1, \ldots, A_{2n} em $M_n(F)$. É possível associar o produto tensorial $M_n(F) \otimes E$ com $M_n(E)$, obtendo matrizes de ordem n cujas entradas são indeterminadas, mais especificamente, elementos da forma λe_i , com $\lambda \in F$, $e_i \in E$. Esta associação é feita calculando: $A = A_1e_1 + \cdots + A_{2n}e_{2n} \in M_n(E)$. Calculemos as potências da matriz genérica A, para o caso particular n = 2. Temos:

$$A^{2} = (A_{1}A_{2} - A_{2}A_{1})e_{1} \wedge e_{2} + (A_{1}A_{3} - A_{3}A_{1})e_{1} \wedge e_{3} + (A_{1}A_{4} - A_{4}A_{1})e_{1} \wedge e_{4}$$

$$+ (A_{2}A_{3} - A_{3}A_{2})e_{2} \wedge e_{3} + (A_{2}A_{4} - A_{4}A_{1})e_{2} \wedge e_{4} + (A_{3}A_{4} - A_{4}A_{3})e_{3} \wedge e_{4}$$

$$A^{3} = (A_{1}A_{2}A_{3} - A_{2}A_{1}A_{3})e_{1} \wedge e_{2} \wedge e_{3} + (A_{1}A_{2}A_{4} - A_{2}A_{1}A_{4})e_{1} \wedge e_{2} \wedge e_{4} + \cdots$$

$$A^{4} = (A_{1}A_{2}A_{3}A_{4} - A_{2}A_{1}A_{3}A_{4} + A_{1}A_{3}A_{4}A_{2} - A_{2}A_{4}A_{3}A_{1} + \cdots)e_{1} \wedge e_{2} \wedge e_{3} \wedge e_{4}$$

É possível concluir então que, para um n qualquer, teremos:

$$A^{2n} = s_{2n}(A_1, \dots, A_{2n})e_1 \wedge e_2 \wedge \dots e_{2n}$$

Para mostrar que s_{2n} é uma identidade em $M_n(F)$, basta mostrar que $A^{2n} = 0$. Consideremos então as *fórmulas de Newton* para matrizes genéricas, que dão os coeficientes do polinômio característico de uma matriz A em função do traço das potências de A. Como vimos no lema anterior, tais fórmulas podem ser escritas:

$$k\alpha_k = \sum_{i=1}^k (-1)^{i-1} \alpha_{k-i} tr(A^i), \ \forall \ k, \ 1 \le k \le n$$

Com isto, se mostrarmos que $tr(A^i) = 0$ para todo i, teremos, pelo Teorema de Cayley-Hamilton, que $A^{2n} = 0$. No caso em estudo as potências da matriz A têm a forma

$$A^{k} = \sum_{i_{1} < \dots < i_{k}} s_{k}(A_{i_{1}}, \dots, A_{i_{k}}) e_{i_{1}} \wedge \dots \wedge e_{i_{k}}$$

como podemos facilmente comprovar das expressões indicadas acima. Mas queremos $A^{2n}=0$. Sabemos pela Proposição 4.3.8 que o traço da matriz $s_{2n}(A_1,\ldots,A_{2n})$ é igual a zero, para todo n. Daí segue o resultado.

Corolário 4.4.3. Todo polinômio f normal de grau 4 é uma identidade em $M_2(F)$.

Demonstração: Pela Proposição 4.3.4, $f = \alpha s_4$. Mas, pelo Teorema, s_4 é uma identidade em $M_2(F)$, logo f é uma identidade em $M_2(F)$.

O próximo resultado estabelece uma espécie de recíproca do Teorema de Amitsur-Levitzki. Sua demonstração pode ser encontrada em [21].

Teorema 4.4.4. (i) A álgebra das matrizes $M_n(F)$ não satisfaz qualquer identidade polinomial de grau menor que 2n.

(ii) Se f é uma identidade multilinear de $M_n(F)$ de grau 2n então, para algum $\alpha \in F$, $f = \alpha S_{2n}$.

4.5 Identidades nos Octônios - Grau 4

Mostraremos nesta seção que não existem identidades de grau 4 ou menor na álgebra dos octônios, que não sejam conseqüências das leis alternativas à direita e à esquerda. Identidades que são conseqüências das duas leis alternativas são chamadas *identidades* triviais (ou óbvias).

Conforme notação introduzida no final do capítulo anterior, designaremos por \mathbb{O} a álgebra dos octônios. Dada uma identidade f em \mathbb{O} , podemos agrupar os monômios do mesmo tipo. Cada grupo destes, ou seja, cada soma de monômios de um certo tipo produz um polinômio homogêneo deste tipo. A identidade f será então, uma soma de polinômios homogêneos, digamos $f = f_1 + f_2 + \cdots + f_t$. Os polinômios f_i são chamados componentes homogêneos de f. Com isto, algumas importantes simplificações podem ser feitas, conforme indicamos a seguir.

Teorema 4.5.1. Seja A uma F-álgebra. Se o corpo F tem mais elementos que o grau máximo de qualquer variável de uma identidade f em A, então todo componente homogêneo de f é uma identidade.

Demonstração: $(id\acute{e}ia)$ Seja t o grau de f. A essência do teorema está em provar que: Se existirem escalares α_1,\ldots,α_t tais que, para o determinante de Vandermonde d formado pelas potências de α_i , a equação da=0 implica a=0, para todo $a\in A$, então todo componente homogêneo da identidade f é também uma identidade em A. Escreve f como uma soma de polinômios $f=f_0+f_1+\cdots+f_j$, onde em cada f_i , a variável x_1 tem grau i. Supondo f um polinômio em n variáveis, tomamse $a_1,\ldots,a_n\in A$, elementos arbitrários. Para cada $i=1,\ldots,j+1$, a expressão $f(\alpha_ia_1,a_2,\ldots,a_n)=0$, implica que $d_1f_k(a)=0$, onde $a=(a_1,\ldots,a_n), k=0,1,\ldots,j$ e d_1 é o determinante de Vandermonde formado por $\alpha_1,\ldots,\alpha_{j+1}$. Finalmente, sendo d_1 divisor de d, a equação $d_1f_k(a)=0$ implica que $f_k(a)=0$ e, portanto, que f_0,f_1,\ldots,f_j são identidades em A.

Note que, como estamos num corpo F cuja característica é maior que o grau da identidade, as condições do teorema são verificadas. Para maiores detalhes, veja a referência [25].

Vamos verificar que podemos assumir que uma identidade homogênea é também alternada nas variáveis lineares. Ordene os componentes homogêneos de uma iden-

tidade f, primeiro pelo grau e depois pelo número de variáveis. Então, se y e z são variáveis lineares e se $f_k(\ldots,y,z,\ldots)+f_k(\ldots,z,y,\ldots)$ não é o polinômio nulo, então, fazendo z=y, obtemos $f_k(\ldots,y,y,\ldots)$ também não nulo e com menor número de variáveis. Supondo que conhecemos os resultados sobre identidades alternadas mais baixas na nossa classificação (isto é, com menor número de variáveis), vamos linearizar $f_k(\ldots,y,y,\ldots)$, obtendo

$$f_k(\ldots, y, z, \ldots) + f_k(\ldots, z, y, \ldots) \tag{1}$$

Mas
$$f_k(\ldots, y, z, \ldots) - f_k(\ldots, z, y, \ldots)$$
 (2)

é uma identidade alternada em y e z. Somando as identidades (1) e (2) obtemos:

$$2f_k(\ldots,y,z,\ldots)$$

Portanto, podemos assumir que f é alternada em y e z.

Uma outra simplificação que podemos obter se refere ao isomorfismo entre os quatérnios e as matrizes 2×2 , conforme mostramos no próximo lema.

Lema 4.5.2. Os quatérnios Q(0,1) e as matrizes $M_2[F]$ são isomorfos.

Demonstração: Seja $a \in Q$. Então $a = a_0.1 + a_1e_1 + a_2e_2 + a_3e_3$, onde $a_i \in F$, $i = 0, \ldots, 3$. Podemos escrever também, $a = (a_0, a_1, a_2, a_3)$. Considere a aplicação

$$\varphi: Q \to M_2(F)$$

$$\varphi(a_0, a_1, a_2, a_3) \mapsto \begin{pmatrix} a_0 + a_1 & a_2 + a_3 \\ a_2 & a_0 \end{pmatrix}$$

 φ é claramente um isomorfismo.

Precisaremos ainda de algumas importantes propriedades do associador em uma álgebra alternativa, que são dadas no seguinte lema operacional.

Lema 4.5.3. Em uma álgebra alternativa A valem as seguintes igualdades, para todos $x, y, z \in A$:

- (i) (x, xy, z) = (x, y, z)x;
- (ii) (x, yx, z) = x(x, y, z);

(iii)
$$(x, y, z^2) = z \circ (x, y, z)$$
.

Demonstração:

(i) Note que: (x, xy, z) = -(z, xy, x) e que (x, y, z) = (z, x, y). Então: $(z, xy, x) = (z(xy))x - z(xyx) \stackrel{*}{=} (z(xy))x - ((zx)y)x$ $= (z(xy) - (zx)y)x = -(z, x, y)x \implies (x, xy, z) = (x, y, z)x$ (*) Moufang (iii) (Teorema 1.2.2)

(ii)
$$(x, yx, z) = (xyx)z - x((yx)z) \stackrel{**}{=} x(y(xz)) - x((yx)z) = x(-(y, x, z))$$

= $x(x, y, z)$
(**) Moufang (i)

(iii) Em uma álgebra alternativa, temos a seguinte identidade: $(x^2, y, x) = 0$, que resulta da *lei flexível*, como mostramos a seguir:

$$(x^2, y, x) = (x^2y)x - x^2(yx) = (x(xy))x - x(x(yx)) = x((xy)x) - x((xy)x) = 0.$$

Linearizando esta expressão com $x \to x + \lambda z$:

$$\begin{split} ((x+\lambda z)^2,y,x+\lambda z) &= (x^2+\lambda xz+\lambda zx+\lambda^2 z^2,y,x+\lambda z) \\ &= \underbrace{(x^2,y,x)}_{=0} + \lambda(x^2,y,z) + \lambda(xz,y,x) + \lambda^2(xz,y,z) \\ &+ \lambda(zx,y,x) + \lambda^2(zx,y,z) + \lambda^2(z^2,y,x) + \underbrace{\lambda^3(z^2,y,z)}_{=0} \end{split}$$

$$=\lambda[(x^2,y,z)+(xz,y,x)+(zx,y,x)]+\ \lambda^2[(z^2,y,x)+(zx,y,z)+(xz,y,z)]=0$$

Note que os coeficientes de λ e de λ^2 são equivalentes, bastando trocar x por z e z por x. Portanto, tomando a expressão para λ^2 :

$$(z^2, y, x) + (zx, y, z) + (xz, y, z) = 0 \implies (x, y, z^2) = (x \circ z, y, z)$$
 (I)

Fazendo y=z e z=y em (i) e (ii) e somando:

 $(x,xz,y)+(x,zx,y)=(x,y,z)\circ x,$ que também pode ser escrito:

 $(x,x\circ z,y)=x\circ (x,z,y).$ Agora, trocando x por z e z por x, obtemos:

 $(z, x \circ z, y) = z \circ (z, x, y)$, o que equivale a:

$$(x \circ z, y, z) = z \circ (x, y, z) \tag{II}$$

Comparando (I) e (II) obtemos:
$$(x, y, z^2) = z \circ (x, y, z)$$

Um polinômio homogêneo do grau 4 pode ser de um dos seguintes tipos: [4], [3,1], [2,2], [2,1,1] e [1,1,1,1]. Por exemplo, x^4 é um polinômio do tipo [4]. Do tipo [3,1], temos x^3y e $x^2(yx)$. Já x^2y^2 e $(xy^2)x$ são do tipo [2,2]. Do tipo [2,1,1], são identidades em 3 variáveis x,y e z, sendo do grau 2 em x e do grau 1 em y e z. Como exemplo citamos: x(xyz) e (xy)(zx). Finalmente o tipo [1,1,1,1] se refere às identidades multilineares em 4 variáveis, como x((yz)w) ou (xy)(zw).

Os três primeiros tipos são associativos, pois têm apenas 1 ou 2 variáveis, logo pelo Teorema de Artin, geram uma subálgebra associativa. Uma identidade deste tipo é portanto, gerada pelo ideal das identidades dos quatérnios, que é o mesmo das matrizes 2×2 , conforme Lema 4.5.2. Mas em $M_2(F)$ só existem identidades multilineares de grau 4. Assim, podemos nos restringir ao estudo das identidades dos dois últimos tipos, [2, 1, 1] e a multilinear [1, 1, 1, 1].

Seja f(x, y, z) uma identidade dos octônios, de grau 2 em x e de grau 1 em y e z. Pelas considerações acima, podemos assumir f alternado em y e z. Vamos mostrar que: (i) A imagem de f em Ass[X] é zero; (ii) νf está no ideal associador de Alt[X].

(i) $\phi f \in Ass[X] \Rightarrow \phi f = \alpha s_4, \ \alpha \in F$. E como s_4 é multilinear, segue que $\alpha = 0$ e $\phi f = 0$.

(ii)
$$\nu f = f + J \implies \phi(\nu f) = \phi(f + J) = \phi f = 0.$$

Assim, como $\phi(\nu f) = 0$, devemos considerar o homomorfismo canônico de Alt[X] para Ass[X]. A rigor, não é o mesmo $\phi: F[X] \to Ass[X]$, mas lembrando que a finalidade da ϕ é retirar os parêntesis, fica justificado o uso do mesmo símbolo.

Como νf está no ideal associador de Alt[X] deverá ser combinação linear de $(x^2, y, z), (x, xy, z)$ e (x, yx, z). Mas, pelo Lema 4.5.3, podemos escrever:

$$(x^2, y, z) = x \circ (x, y, z) = x(x, y, z) + (x, y, z)x = (x, yx, z) + (x, xy, z).$$

Portanto νf é combinação linear de x(x,y,z) e (x,y,z)x. Sendo f uma identidade, f(a,b,c)=0, para todos $a,b,c\in\mathbb{O}$. Em particular, para elementos da base de \mathbb{O} . Lembramos que a base de \mathbb{O} , conforme estabelecemos no capítulo anterior, é dada por:

$$\{1, e_1, e_2, \ldots, e_7\}.$$

Façamos as seguintes substituições: $x=e_1,\ y=e_2,\ z=e_3.$ Calculando, obtemos:

$$\nu f = \alpha e_1(e_1, e_2, e_3) + \beta(e_1, e_2, e_3)e_1
= \alpha e_1((e_1e_2)e_3 - e_1(e_2e_3)) + \beta((e_1e_2)e_3 - e_1(e_2e_3))e_1
= \alpha e_1(e_3e_3 - e_1e_1) + \beta(e_3e_3 - e_1e_1) = 0$$

Assim, νf é o polinômio nulo. Provamos então que não existem identidades do tipo [2,1,1] em Alt[X], além das triviais.

Para tratarmos deste tipo de polinômio precisamos determinar as possíveis formas de se arranjar parêntesis em 4 variáveis. Não é difícil perceber que tais arranjos se resumem nos seguintes, indicados esquematicamente:

$$s_4^1 = _(_(__))$$
 $s_4^2 = _((__)_)$ $s_4^3 = ((__)_)_$ $s_4^4 = (_(__))_$ $s_4^5 = (__)(__)$

É importante notar que, ao fazermos substituições por elementos da base dos octônios, não precisamos levar em conta todas as possibilidades de distribuição das variáveis em cada s_4^i , uma vez que os polinômios são alternados. Assim, uma troca de posição de duas variáveis afetará o monômio com o sinal da permutação. Por exemplo, no caso de s_4^1 , teremos:

$$e_1(e_2(e_3e_4)) = -e_2(e_1(e_3e_4)) = e_2(e_1(e_4e_3))$$

Basta portanto fazer uma única substituição por elementos da base. Então, notando que f é combinação linear dos monômios s_4^i indicados acima, temos:

$$f = as_4^1 + bs_4^2 + cs_4^3 + ds_4^4 + es_4^5$$

Fazendo as seguintes substituições:

(1)
$$e_1, e_2, e_3, e_4$$
; (2) e_1, e_2, e_3, e_5 ;
(3) e_1, e_2, e_3, e_6 ; (4) e_2, e_3, e_4, e_6
(5) e_2, e_3, e_4, e_7

obtemos um sistema homogêneo com 5 equações nas incógnitas a,b,c,d,e. Desenvolvendo:

(1)
$$ak_1 + bk_2 + ck_3 + dk_4 + ek_5 = 0$$
, onde
 $k_1 = e_1(e_2(e_3e_4)) = e_1(e_2e_7) = -e_1e_5 = e_4$
 $k_2 = e_1((e_2e_3)e_4) = e_1(e_1e_4) = e_1e_5 = -e_4$
 $k_3 = ((e_1e_2)e_3)e_4 = (e_3e_3)e_4 = -e_4$
 $k_4 = (e_1(e_2e_3))e_4 = (e_1e_1)e_4 = -e_4$
 $k_5 = (e_1e_2)(e_3e_4) = e_3e_7 = -e_4$
A equação (1) fica: $(a - b - c - d - e)e_4 = 0$ ou $a - b - c - d - e = 0$

(2) A equação (2) tem a mesma expressão acima, com as substituições agora por outros elementos, dando os seguintes resultados:

$$k_1 = e_1(e_2(e_3e_5)) = e_1(e_2e_6) = -e_1e_4 = -e_5$$

 $k_2 = e_1((e_2e_3)e_5) = e_1(e_1e_5) = -e_1e_4 = -e_5$
 $k_3 = ((e_1e_2)e_3)e_5 = (e_3e_3)e_5 = -e_5$
 $k_4 = (e_1(e_2e_3))e_5 = (e_1e_1)e_5 = -e_5$
 $k_5 = (e_1e_2)(e_3e_5) = e_3e_6 = e_5$
A equação (2) fica: $(-a - b - c - d + e)e_5 = 0$ ou $-a - b - c - d + e = 0$

(3) De maneira análoga para a equação (3) obtemos:

$$k_1 = e_1(e_2(e_3e_6)) = e_1(e_2e_5) = e_1e_7 = e_6$$

 $k_2 = e_1((e_2e_3)e_6) = e_1(e_1e_6) = -e_1e_7 = -e_6$
 $k_3 = ((e_1e_2)e_3)e_6 = (e_3e_3)e_6 = -e_6$
 $k_4 = (e_1(e_2e_3))e_6 = (e_1e_1)e_6 = -e_6$
 $k_5 = (e_1e_2)(e_3e_6) = e_3e_5 = e_6$
A equação (3) fica: $(a - b - c - d + e)e_6 = 0$ ou $a - b - c - d + e = 0$

(4) Agora, para a equação (4):

$$k_1 = e_2(e_3(e_4e_6)) = e_2(e_3e_2) = -e_2e_1 = e_3$$

$$k_2 = e_2((e_3e_4)e_6) = e_2(e_7e_6) = -e_2e_1 = e_3$$

$$k_3 = ((e_2e_3)e_4)e_6 = (e_1e_4)e_6 = e_5e_6 = -e_3$$

$$k_4 = (e_2(e_3e_4))e_6 = (e_2e_7)e_6 = -e_5e_6 = e_3$$

$$k_5 = (e_2e_3)(e_4e_6) = e_1e_2 = e_3$$

A equação (4) fica:
$$(a + b - c + d + e)e_3 = 0$$
 ou $a + b - c + d + e = 0$

(5) Finalmente para a equação (5):

$$k_1 = e_2(e_3(e_4e_7)) = e_2(e_3e_3) = -e_2$$

$$k_2 = e_2((e_3e_4)e_7) = e_2(e_7e_7) = -e_2$$

$$k_3 = ((e_2e_3)e_4)e_7 = (e_1e_4)e_7 = e_5e_7 = -e_2$$

$$k_4 = (e_2(e_3e_4))e_7 = (e_2e_7)e_7 = -e_5e_7 = e_2$$

$$k_5 = (e_2e_3)(e_4e_7) = e_1e_3 = -e_2$$
A equação (5) fica: $(-a - b - c + d - e)e_3 = 0$ ou $-a - b - c + d - e = 0$

Temos então o seguinte sistema:

$$a - b - c - d - e = 0$$

$$-a - b - c - d + e = 0$$

$$a - b - c - d + e = 0$$

$$a + b - c + d + e = 0$$

$$-a - b - c + d - e = 0$$

que facilmente verificamos, só apresenta a solução trivial: a=b=c=d=e=0.

Portanto f é o polinômio nulo. Concluímos assim que não existem identidades de grau 4 em uma álgebra de octônios, além das triviais.

4.6 Identidades nos Octônios - Grau 5

Mostraremos nesta seção que as identidades de grau 5 nos octônios são conseqüências de apenas duas identidades conhecidas, designadas por χ e κ , definidas da seguinte maneira:

$$\chi = [[x_1, x_2] \circ [x_3, x_4], x_5]$$

$$\kappa(x; x_1, x_2, x_3) = s_3^+(x_1, x_2, x_3)(x^2) - (s_3^+(x_1, x_2, x_3)(x)) \circ x$$

$$\kappa(x; y; x_1, x_2, x_3) = s_3^+(x \circ y) - (s_3^+(x)) \circ y - (s_3^+(y)) \circ x$$

onde s_3^+ é o operador definido por

$$s_3^+(x_1, x_2, x_3)(y) = s_3(V_{x_1}, V_{x_2}, V_{x_3})(y) = \sum_{\pi \in S_3} (\operatorname{sgn}\pi) V_{x_{\pi_1}} V_{x_{\pi_2}} V_{x_{\pi_3}}(y)$$

e V_x é o produto de Jordan, dado por $V_x(y) = x \circ y = xy + yx$.

No que segue, adotaremos a seguinte simplificação na notação: Indicaremos $x_{\pi i}$ ao invés de $x_{\pi i}$ para a permutação πi do elemento x.

Lema 4.6.1. Os polinômios χ e κ definidos acima são identidades nas álgebras de Cayley.

Demonstração:

(1) Provemos que χ é uma identidade em C.

Seja C uma álgebra de Cayley. Então todo elemento $a \in C$ satisfaz uma equação quadrática do tipo $x^2 - t(x)x + n(x).1 = 0$, onde t(x) é o traço de x e n(x) é a norma de x. Linearizando esta equação obtemos:

$$x \circ y - t(x)y - t(y)x + n(x, y).1 = 0$$

Fazendo x = [a, b] e y = [c, d], nos dá:

$$[a,b] \circ [c,d] - t([a,b])[c,d] - t([c,d])[a,b] + n([a,b],[c,d]).1 = 0$$

Mas
$$t([a,b]) = t([c,d]) = 0$$
, logo: $\chi(a,b,c,d,e) = [n([a,b],[c,d]).1,e] = 0$

(2) Provemos que κ é uma identidade em C^+ .

Obtemos a partir da álgebra C dos octônios, uma álgebra de Jordan C^+ , definindo o produto por $x \circ y$, conforme já indicado. Para maiores detalhes sobre a relação entre as álgebras alternativas e as álgebras de Jordan, ver referência [22].

Em C^+ podemos considerar o traço T(x) e a norma Q(x) de um elemento e, de acordo com o que já estudamos no capítulo anterior, temos as seguintes igualdades:

$$x^{2} = T(x) - Q(x)1; (1)$$

$$Q(x,y) = q(x+y) - q(x) - q(y); (2)$$

$$T(x) = Q(x,1); (3)$$

$$x \circ y = T(x)y + T(y)x - Q(x,y)1 \tag{4}$$

Para mostrar (4) fazemos:

$$T(x)y + T(y)x - Q(x,y)1 = (x + \overline{x})y + (y + \overline{y})x - \overline{x}y - \overline{y}y = xy + yx$$

Usando estas igualdades, reescrevemos κ da seguinte maneira:

$$\kappa(x; x_1, x_2, x_3) = s_3^+(T(x)x - Q(x)1) - (T(s_3^+(x))x + T(x)s_3^+(x) - Q(s_3^+(x), x)1)$$

Vamos começar calculando a expressão $s_3^+(x)$, aplicando sua definição:

$$s_{3}^{+}(x) = s_{3}(V_{x_{1}}, V_{x_{2}}, V_{x_{3}})(x) = \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_{x_{\pi 2}} V_{x_{\pi 3}}(x)$$

$$= \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_{x_{\pi 2}}(x_{\pi 1} \circ x)$$

$$= \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_{x_{\pi 2}}(T(x_{\pi 1})x + T(x)x_{\pi 1} - Q(x_{\pi 1}, x)1)$$

$$= \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}}(x_{\pi 2} \circ (T(x_{\pi 1})x + T(x)x_{\pi 1} - Q(x_{\pi 1}, x)1))$$

$$= \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}}(x_{\pi 2} \circ T(x_{\pi 1})x + x_{\pi 2} \circ T(x)x_{\pi 1} - x_{\pi 2} \circ Q(x_{\pi 1}, x)1)$$

$$= \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_{1} + \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_{2} - \sum_{\pi \in S_{3}} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_{3}$$

onde $V_1 = x_{\pi 2} \circ T(x_{\pi 1})x$, $V_2 = x_{\pi 2} \circ T(x)x_{\pi 1}$ e $V_3 = x_{\pi 2} \circ Q(x_{\pi 1}, x)1$.

Analisemos cada uma destas parcelas separadamente. Comecemos pela segunda:

$$\sum_{\pi \in S_3} (\operatorname{sgn} \pi) V_{x_{\pi 3}} V_2 = \sum_{\pi \in S_3} (\operatorname{sgn} \pi) x_{\pi 3} \circ (x_{\pi 2} \circ T(x) x_{\pi 1}) = T(x) \sum_{\pi \in S_3} (\operatorname{sgn} \pi) x_{\pi 3} \circ (x_{\pi 2} \circ x_{\pi 1})$$

Temos uma soma de elementos simétricos em s_3 , uma vez que $x_{\pi 2} \circ x_{\pi 3} = x_{\pi 3} \circ x_{\pi 2}$. Mas, como s_3 é alternado estes dois termos têm sinais contrários, logo se anulam. Portanto:

$$\sum_{\pi \in S_3} (\operatorname{sgn} \pi) V_{x_{\pi 3}} V_2 = 0.$$

Vejamos agora a terceira parcela.

$$\sum_{\pi \in S_3} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_3 = \sum_{\pi \in S_3} (\operatorname{sgn}\pi) x_{\pi 3} \circ (x_{\pi 2} \circ Q(x_{\pi 1}, x)1)$$

$$= 2(Q(x_1, x)x_3 \circ x_2 - Q(x_2, x)x_3 \circ x_1 - Q(x_1, x)x_2 \circ x_3$$

$$+ Q(x_3, x)x_2 \circ x_1 + Q(x_2, x)x_1 \circ x_3 - Q(x_3, x)x_1 \circ x_3)$$

Novamente temos uma soma de elementos simétricos que, pela alternatividade de s_3 (que agora explicitamos), resulta na nulidade da expressão. Assim:

$$\sum_{\pi \in S_3} (\operatorname{sgn}\pi) V_{x_{\pi 3}} V_3 = 0$$

Para a primeira parcela temos:

$$\sum_{\pi \in S_3} (\operatorname{sgn} \pi) V_{x_{\pi 3}} V_1 = \sum_{\pi \in S_3} (\operatorname{sgn} \pi) V_{x_{\pi 3}} (x_{\pi 2} \circ T(x_{\pi 1}) x)$$

$$\stackrel{(4)}{=} \sum_{\pi \in S_3} (\operatorname{sgn}\pi) V_{x_{\pi 3}} (T(x_{\pi 2}) T(x_{\pi 1}) x + T(T(x_{\pi 1}) x) x_{\pi 2} - Q(x_{\pi 2}, T(x_{\pi 1}) x) 1)$$

$$= \sum_{\pi \in S_3} (\operatorname{sgn}\pi) V_{x_{\pi 3}} (T(x_{\pi 2}) T(x_{\pi 1}) x + T(x) T(x_{\pi 1}) x_{\pi 2} - T(x_{\pi 1}) Q(x_{\pi 2}, x) 1)$$

$$= \sum_{\pi \in S_3} (\operatorname{sgn}\pi) \underbrace{(T(x_{\pi 1}) T(x_{\pi 2}) (x_{\pi 3} \circ x)}_{(i)} + \underbrace{T(x) T(x_{\pi 1}) x_{\pi 3} \circ x_{\pi 2}}_{(ii)} - 2T(x_{\pi 1}) Q(x_{\pi 2}, x) x_{\pi 3})$$

Verifiquemos que as parcelas (i) e (ii) se anulam. De fato:

(i) =
$$T(x_1)T(x_2)(x_3 \circ x) - T(x_1)T(x_3)(x_2 \circ x) - T(x_2)T(x_1)(x_3 \circ x)$$

+ $T(x_2)T(x_3)(x_1 \circ x) + T(x_3)T(x_1)(x_2 \circ x) - T(x_3)T(x_2)(x_1 \circ x) = 0$

De maneira análoga se mostra que a parcela (ii) também se anula.

Ficamos então com a seguinte expressão de s_3^+ :

$$s_3^+(x) = s_3(V_{x_1}, V_{x_2}, V_{x_3})(x) = -2\sum_{\pi \in S_3} (\operatorname{sgn}\pi) T(x_{\pi 1}) Q(x_{\pi 2}, x) x_{\pi 3}$$

Vamos desenvolver a expressão de κ obtida há pouco, usando a linearidade de s_3^+ :

$$\kappa(x; x_1, x_2, x_3) = s_3^+(T(x)x - Q(x)1) - (T(s_3^+(x))x + T(x)s_3^+(x) - Q(s_3^+(x), x)1)$$

$$= T(x)s_3^+(x) - Q(x)s_3^+(1) - T(s_3^+(x))x - T(x)s_3^+(x) + Q(s_3^+(x), x)1$$

$$\kappa(x; x_1, x_2, x_3) = -Q(x)s_3^+(1) - T(s_3^+(x))x + Q(s_3^+(x), x)1$$

Afirmamos que: $s_3^+(1) = 0$. De fato,

$$s_3^+(1) = -2 \sum_{\pi \in S_3} (\operatorname{sgn}\pi) T(x_{\pi 1}) Q(x_{\pi 2}, 1) x_{\pi 3} = -2 \sum_{\pi \in S_3} (\operatorname{sgn}\pi) T(x_{\pi 1}) T(x_{\pi 2}) x_{\pi 3} = 0$$
 pois temos uma soma alternada de elementos simétricos.

Verifiquemos que $Q(s_3^+(x), x) = 0$.

$$Q(s_3^+(x), x) = Q(-2 \sum_{\pi \in S_3} (\operatorname{sgn}\pi) T(x_{\pi 1}) Q(x_{\pi 2}, x) x_{\pi 3}, x)$$

= $-2 \sum_{\pi \in S_3} (\operatorname{sgn}\pi) T(x_{\pi 1}) Q(x_{\pi 2}, x) Q(x_{\pi 3}, x) = 0$

pois temos também uma soma alternada de elementos simétricos.

Mostraremos agora que $T(s_3^+(x)) = 0$. Para isto linearizamos $Q(s_3^+(x), x) = 0$, substituindo x por x + 1:

$$0 = Q(s_3^+(x+1), x+1) = Q(s_3^+(x), x) + Q(s_3^+(x), 1) + Q(s_3^+(1), x) + Q(s_3^+(1), 1)$$

$$= 0 + T(s_3^+(x)) + 0 + 0$$

$$\Rightarrow T(s_3^+(x)) = 0.$$

Portanto
$$\kappa(x; x_1, x_2, x_3) = 0.$$

Teorema 4.6.2. O T-ideal das identidades em $M_2(F)$, sendo car F = 0, é gerado por $s_4(x, y, z, w)$ e por $[[x, y]^2, x]$.

Demonstração: $(id\acute{e}ia)$ Consiste em verificar a chamada $conjectura\ de\ Razmyslov$ para n=2, segundo a qual, em uma álgebra associativa de matrizes de ordem n sobre um corpo de característica zero, a base das identidades consiste das seguintes identidades:

$$s_{2n}(x_1,\ldots,x_{2n})=0$$
 e $s_n([x_1^n,x_2],[x_1^{n-1},x_2],\ldots,[x_1,x_2])=0.$

Esta conjectura é provada para n=2. Utiliza a teoria das representações do grupo simétrico. Ressalta o fato de que as identidades nas bases consideradas são de graus 4, 5 e 6. Os detalhes podem ser encontrados em [4].

Se $car F \neq 2$, as identidades de grau 5 em $M_2(F)$ podem ser de um dos seguintes tipos:

$$_s_4(_,_,_,_)$$
 $s_4(_,_,_,_)$ $s_4(_,_,_,_)$ $[[_,_] \circ [_,_],_]$

Para tratarmos o caso das identidades de grau 5, são válidas as mesmas simplificações assumidas no grau 4, isto é, que basta considerar polinômios homogêneos e alternados.

Um polinômio homogêneo do grau 5 pode ser obtido a partir das partições de 5, que são: [5], [4,1], [3,2], [3,1,1], [2,2,1], [2,1,1,1] e [1,1,1,1,1]. Daqui para frente, ao invés de nos referirmos a um polinômio (ou identidade) de grau 5, vamos falar de polinômio de grau [5] ou de grau [4,1], etc, enfatizando a partição em estudo.

As três primeiras partições resultam em polinômios associativos, pois têm apenas 1 ou 2 variáveis, logo pelo Teorema de Artin, geram uma subálgebra associativa, isto é, pertencem a $M_2(F)$. É fácil ver que não existem identidades dos dois primeiros tipos em $M_2(F)$. Se houver uma identidade de grau [3,2] em $M_2(F)$, ela é múltipla de $[[x,y]^2,x]$. Nosso estudo das identidades de grau 5 se resumirá, portanto, às identidades de grau [3,1,1], [2,2,1], [2,1,1,1] e [1,1,1,1,1].

Interessa agora explicitar os geradores de cada um desses graus, com base no Teorema 4.6.2. Mostraremos a seguir que as identidades de grau [3, 1, 1] são consequência apenas de s_4 , e que as identidades de grau [2, 2, 1] são consequência de s_4 e de χ .

Lema 4.6.3. Sejam f uma identidade de grau [3,1,1] e g uma identidade de grau [2,2,1]. A imagem de f em Ass[X], ϕf , é conseqüência de s_4 e a imagem de g em Ass[X], ϕg , é conseqüência de χ .

Demonstração: Linearizando $[[x, y]^2, x]$ para 3 variáveis, temos:

$$\begin{aligned} [[x+z,y]^2,x+z] &= [([x,y]+[z,y])^2,x+z] \\ &= [[x,y]^2,x] + [[z,y]^2,x] + [[x,y]^2,z] + [[z,y]^2,z] \\ &+ [[x,y]\circ[z,y],x] + [[x,y]\circ[z,y],z] \end{aligned}$$

Os elementos acima obtidos são de graus: [3,2,0],[1,2,2],[2,2,1],[0,2,3],[2,2,1] e [1,2,2], respectivamente. Portanto, dentre os dois casos em estudo, vemos que somente o de grau [2,2,1] é conseqüência de χ . Mais especificamente, temos que uma identidade de grau [2,2,1] é conseqüência de $[[x,y]^2,z]$ e de $[[x,y]\circ[z,y],x]$.

Por outro lado, uma identidade de grau [3,1,1] pode ser obtida a partir de $s_4(x,y,z,x^2)$, que é um dos cinco tipos possíveis para uma identidade associativa de grau 5, a saber, $s_4(\underline{\ \ \ },\underline{\ \ \ \ },\underline{\ \ \ \ \ })$. Podemos ter um polinômio de grau [3,1,1] do tipo $[[x,y]\circ[x,z],x]$, mas este é um polinômio simétrico em y e z. Como estamos supondo identidades alternadas nas variáveis lineares, um polinômio deste tipo só pode ser o polinômio nulo.

Pelo mesmo argumento, temos que uma identidade de grau [2, 2, 1] é gerada somente por $s_4(x, y, z, xy)$ e $s_4(x, y, z, yx)$, pois não há outra distribuição das variáveis em s_4 que resulte no grau em questão.

Veremos adiante que também as identidades de grau [2, 1, 1, 1] são conseqüência de χ e de s_4 . Mas queremos mostrar que qualquer identidade de grau 5 é conseqüência de χ e de κ . Precisamos, então, relacionar s_4 com κ . Para isto, o conceito de derivação tem importância.

Definição 4.6.1. Seja A uma álgebra sobre um corpo K. Chama-se **derivação** de A a um operador linear D que satisfaz:

$$D(xy) = (D(x))y + x(D(y))$$

Como exemplo, citamos: Em uma álgebra alternativa, $D=(x,y,\underline{\ })$ é uma derivação. De fato, se $D(z^2)=D(zz)=zD(z)+(D(z))z$, então, de acordo com o Lema 4.5.3 (iii), $(x,y,z^2)=z(x,y,z)+(x,y,z)z$.

A proposição a seguir relaciona s_4 com κ .

Proposição 4.6.4. Em uma álgebra associativa vale a seguinte igualdade:

$$\kappa(x; y, z, w) = s_4(y, z, w, x^2) - s_4(y, z, w, x) \circ x$$

Demonstração: Substituindo a expressão de κ pela sua definição, trocando x_1 por y, x_2 por z e x_3 por w, temos:

$$\kappa(x;y,z,w) = s_3^+(y,z,w)(x^2) - (s_3^+(y,z,w)(x)) \circ x$$

Provar a tese equivale a mostrar que:

$$s_3^+(y,z,w)(x^2) - (s_3^+(y,z,w)(x)) \circ x = s_4(y,z,w,x^2) - s_4(y,z,w,x) \circ x$$

$$\Rightarrow s_3^+(y,z,w)(x^2) - s_4(y,z,w,x^2) = (s_3^+(y,z,w)(x) - s_4(y,z,w,x)) \circ x$$

Por sua vez, a validade desta última expressão equivale a mostrar que:

 $s_3^+(y,z,w)(x) - s_4(y,z,w,x)$ é uma derivação em qualquer álgebra associativa.

Façamos $D_{y,z,w}(x) = s_3^+(y,z,w)(x) - s_4(y,z,w,x)$. Desenvolvendo cada parcela:

$$s_{3}^{+}(y, z, w)(x) = s_{3}(V_{y}, V_{z}, V_{w})(x)$$

$$= V_{y}V_{z}V_{w}(x) - V_{y}V_{w}V_{z}(x) - V_{z}V_{y}V_{w}(x)$$

$$= V_{z}V_{w}V_{y}(x) + V_{w}V_{y}V_{z}(x) - V_{w}V_{z}V_{y}(x)$$

$$= V_{z}V_{w}(y \circ x) - V_{w}V_{z}(y \circ x) + V_{w}V_{y}(z \circ x) - V_{y}V_{w}(z \circ x)$$

$$+ V_{y}V_{z}(w \circ x) - V_{z}V_{y}(w \circ x)$$

$$= [V_{z}, V_{w}](y \circ x) + [V_{w}, V_{y}](z \circ x) + [V_{y}, V_{z}](w \circ x)$$

$$= \sum_{(y, z, w)} [V_{y}, V_{z}](x \circ y)$$

onde a notação $\sum\limits_{(y,z,w)}$ indica a soma cíclica em y,z,w.

No desenvolvimento de $s_4(y, z, w, x)$ existirão parcelas em que o x será o último elemento, as quais poderão ser escritas como $s_3(y, z, w)x$. Teremos também termos em que o x será o primeiro elemento, que escreveremos $xs_3(y, z, w)$.

Teremos ainda parcelas com o x aparecendo em segundo lugar, como yxzw, as quais serão indicadas por $\sum_{(y,z,w)} wx[y,z]$.

Finalmente, quando o x ocupar o terceiro lugar, como em yzxw, estes termos se escreverão: $-\sum_{(y,z,w)}[y,z]xw$. Temos então:

$$D_{y,z,w}(x) = \sum_{(y,z,w)} [V_y, V_z](x \circ y) - s_3(y, z, w)x + xs_3(y, z, w) + \sum_{(y,z,w)} [y, z]xw - \sum_{(y,z,w)} wx[y, z]$$

Mas

$$\sum_{(y,z,w)} [V_y, V_z](x \circ y) = \sum_{(y,z,w)} (V_z V_w (x \circ y) - V_w V_z (x \circ y))
= \sum_{(y,z,w)} (V_w (z \circ (x \circ y)) - V_z (w \circ (x \circ y)))
= \sum_{(y,z,w)} (wzxy + wzyx + wxyz + wyxz + zxyw + zyxw
+ xyzw + yxzw - zwxy - zwyx - zxyw - zyxw
- wxyz - wyxz - xywz - yxwz)
= \sum_{(y,z,w)} [xy + yx, [z,w]]$$

Resulta então:

$$\begin{split} D_{y,z,w}(x) &= \sum_{(y,z,w)} [xy + yx, [z,w]] + [x,s_3(y,z,w)] + \sum_{(y,z,w)} [z,w] xy - \sum_{(y,z,w)} yx[z,w] \\ &= [x,s_3(y,z,w)] + \sum_{(y,z,w)} ([xy,[z,w]] + [yx,[z,w]] + [z,w]xy - yx[z,w]) \\ &= [x,s_3(y,z,w)] \\ &+ \sum_{(y,z,w)} (xy[z,w] - [z,w]xy + yx[z,w] - [z,w]yx + [z,w]xy - yx[z,w]) \\ &= [x,s_3(y,z,w)] + \sum_{(y,z,w)} (xy[z,w] - [z,w]yx) \\ &= [x,s_3(y,z,w)] + x(\sum_{(y,z,w)} y[z,w]) - (\sum_{(y,z,w)} [z,w]y)x \end{split}$$

Mas

$$\begin{split} x(\sum_{(y,z,w)}y[z,w]) - (\sum_{(y,z,w)}[z,w]y)x &= x(y[z,w] + w[y,z] + z[w,y]) \\ &= x(yzw - ywz + wyz - wzy + zwy - zyw) \\ &- (zwy - wzy + yzw - zyw + wyz - ywz)x \\ &= xs_3(y,z,w) - s_3(y,z,w)x = [x,s_3(y,z,w)] \\ \Rightarrow D_{y,z,w}(x) &= 2[x,s_3(y,z,w)] = [x,2s_3(y,z,w)]. \end{split}$$

Isto mostra que $D_{y,z,w}(x)$ é uma derivação, pois em uma álgebra associativa, $D_z(x) = [x, z]$ é uma derivação. De fato:

$$D_{z}(xy) = [xy, z] = (xy)z - z(xy) = xyz - zxy.$$

$$D_{z}(x)y + xD_{z}(y) = [x, z]y + x[y, z] = (xz - zx)y + x(yz - zy)$$

$$= xzy - zxy + xyz - xzy = xyz - zxy$$

Identidades de grau [3, 1, 1]

Seja f(x, y, z) uma identidade dos octônios, de grau [3, 1, 1] alternada em y e z. Considerando o homomorfismo canônico ϕ já definido, que leva uma identidade f de Alt[X] em Ass[X], temos que $\phi f \in Ass[X]$, logo ϕf é uma identidade em $M_2(F)$. Uma identidade de grau [3, 1, 1] deve ter sua imagem em Ass[X] múltipla de $s_4(x, y, z, x^2)$, de acordo com o Lema 4.6.3. Escrevemos então, para $\lambda \in F$:

$$\phi f = \lambda s_4(x, y, z, x^2) \tag{4.1}$$

Fazendo $y=x,\ z=y,\ w=z$ na Proposição 4.6.4, teremos: $\kappa(x;x,y,z)=s_4(x,y,z,x^2)$, uma vez que s_4 é alternado. Substituindo este dado em 4.1, temos: $\phi f=\lambda \kappa$.

Se f e $\lambda \kappa$ são identidades, então $f' = f - \lambda \kappa$ também é. Daí:

 $\phi f' = \phi(f - \lambda \kappa) = \phi f - \phi(\lambda \kappa) = \phi f - \phi f = 0$ e f' está no ideal associador. Então f' é combinação linear de $x^2(x, y, z), x(x, y, z)x$ e $(x, y, z)x^2$. Assim:

$$f' = ax^2(x, y, z) + bx(x, y, z)x + c(x, y, z)x^2$$

Vamos fazer as seguintes substituições por elementos da base de C:

(1)
$$x = e_1$$
, $y = e_2$, $z = e_4$
 $(e_1, e_2, e_4) = (e_1e_2)e_4 - e_1(e_2e_4) = e_3e_4 - e_1e_6 = e_7 - (-e_7) = 2e_7$
 $f' = -2ae_7 + be_1(2e_7)e_1 - 2ce_7 = (-2a + 2b - 2c)e_7$

(2)
$$x = 1 + e_1$$
, $y = e_2$, $z = e_4$
 $(1 + e_1, e_2, e_4) = (1, e_2, e_4) + (e_1, e_2, e_4) = 0 + 2e_7 = 2e_7$
 $(1 + e_1)^2 = 1 + 2e_1 + e_1^2 = 1 + 2e_1 - 1 = 2e_1$
 $f' = -2ae_1(2e_7) + 2be_1(2e_7) + 2ce_1(2e_7) = (4a + 4b + 4c)e_6$

(3)
$$x = e_1$$
, $y = e_2$, $z = e_6$
 $(e_1, e_2, e_6) = (e_1 e_2)e_6 - e_1(e_2 e_6) = e_3 e_6 - e_1(-e_4) = e_5 + e_5 = 2e_5$
 $f' = -2a(2e_5) - 2be_5 - 2ce_5 = (-4a - 2b - 2c)e_5$

Obtemos o sistema:

$$-a+b-c = 0$$

$$a+b+c = 0$$

$$2a+b+c = 0$$

que facilmente verificamos, só apresenta a solução trivial: a=b=c=0. Portanto f' é o polinômio nulo.

Neste caso formaremos, a partir de uma identidade do tipo [2, 2, 1], duas outras identidades, sendo uma simétrica e a outra alternada. Seja f(x, y, z) uma identidade do tipo [2, 2, 1]. Então

- 1. g(x,y,z) = f(x,y,z) + f(y,x,z) é simétrico em x e y. De fato, g(y,x,z) = f(y,x,z) + f(x,y,z) = g(x,y,z)
- 2. h(x,y,z)=f(x,y,z)-f(y,x,z) é alternado em x e y. De fato, h(y,x,z)=f(y,x,z)-f(x,y,z)=-h(x,y,z)

Basta provar que g e h são conseqüências de χ e κ , uma vez que $f = \frac{g+h}{2}$. Sabemos, pelo Lema 4.6.3, que uma identidade de grau [2,2,1] é conseqüência de $s_4(x,y,z,xy)$, de $s_4(x,y,z,yx)$ e de χ . Mas não temos uma relação entre s_4 com estas distribuições de variáveis e κ . Vamos mostrar que, na verdade, estes s_4 estão relacionados com χ no caso simétrico e com κ no caso alternado. Para isto precisaremos de um lema operacional.

Lema 4.6.5. Em Ass[X] são válidas as sequintes iqualdades:

(i)
$$s_4(x, y, z, w) = [x, y] \circ [z, w] + [x, z] \circ [w, y] + [x, w] \circ [y, z];$$

(ii)
$$[x, y] \circ z = [x, y \circ z] - y \circ [x, z]$$

(iii)
$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$$
 (identidade de Jacobi)

Demonstração: As três igualdades são de verificação imediata, bastando apenas desenvolver os comutadores.

Teorema 4.6.6. O subespaço dos elementos simétricos de grau [2, 2, 1] no ideal das identidades de grau 5 é gerado por $[z, [x, y]^2]$, $[x, [x, y] \circ [y, z]]$ e $[y, [x, y] \circ [x, z]]$.

Demonstração: Pelo Lema 4.6.3, sabemos que uma identidade de grau [2, 2, 1] é conseqüência de $[[x, y]^2, z]$, de $[[x, y] \circ [z, y], x]$, de $s_4(x, y, z, xy)$ e de $s_4(x, y, z, yx)$. O primeiro elemento é simétrico em x e y, pois:

$$[[x, y]^2, z] = [(xy - yx)^2, z] = [(yx - xy)^2, z] = [[y, x]^2, z]$$

O elemento $[[x, y] \circ [z, y], x]$ não é simétrico, mas notando que:

$$[[x,y] \circ [z,y], x] = [x, [x,y] \circ [y,z]]$$

podemos fazer:

$$p(x, y, z) = [x, [x, y] \circ [y, z]] - [y, [x, y] \circ [x, z]]$$

$$= -[x, [y, x] \circ [y, z]] + [y, [y, x] \circ [x, z]]$$

$$= p(y, x, z)$$

obtendo o elemento simétrico $p(x, y, z) = [x, [x, y] \circ [y, z]] - [y, [x, y] \circ [x, z]].$

Os outros elementos de grau [2, 2, 1], provenientes de $s_4(x, y, z, xy)$ e $s_4(x, y, z, yx)$, podem ser escritos na forma $s_4(x, y, z, [x, y])$, para os elementos simétricos. Vamos mostrar agora que este elemento é consequência de $[z, [x, y]^2]$ e p(x, y, z). Pelo Lema 4.6.5 (i):

$$s_4(x, y, z, [x, y]) = \underbrace{[x, y] \circ [z, [x, y]]}_{(1)} + \underbrace{[x, z] \circ [[x, y], y]}_{(2)} + \underbrace{[x, [x, y]] \circ [y, z]}_{(3)}$$

Aplicando a cada uma das 3 parcelas à direita o Lema 4.6.5 (ii), temos:

$$\begin{aligned} (1) \colon & \quad [x,y] \circ [z,[x,y]] = [z,[x,y]] \circ [x,y] = [z,2[x,y]^2] - [x,y] \circ [z,[x,y]] \\ & \quad = 2[z,[x,y]^2] - [z,[x,y]] \circ [x,y] \\ & \quad \Rightarrow 2[z,[x,y]] \circ [x,y] = 2[z,[x,y]^2] \\ & \quad \Rightarrow [z,[x,y]] \circ [x,y] = [z,[x,y]^2] \end{aligned}$$

(2):
$$[x, z] \circ [[x, y], y] = [x, z] \circ [y, [y, x]] = [y, [y, x] \circ [x, z]] - [y, x] \circ [y, [x, z]]$$

= $-[y, [x, y] \circ [x, z]] + [x, y] \circ [y, [x, z]]$

(3):
$$[x, [x, y]] \circ [y, z] = [x, [x, y] \circ [y, z]] - [x, y] \circ [x, [y, z]]$$

Reescrevendo a expressão de s_4 :

$$s_4(x, y, z, [x, y]) = [x, y] \circ [z, [x, y]] + [x, y] \circ [y, [x, z]] - [x, y] \circ [x, [y, z]] + [x, [x, y] \circ [y, z]] - [y, [x, y] \circ [x, z]]$$

A parcela (1) pode ser escrita:

$$[x,y] \circ [z,[x,y]] = 2([x,y] \circ [z,[x,y]]) - [x,y] \circ [z,[x,y]]$$

$$= 2[z,[x,y]^2] + [x,y] \circ [z,[y,x]]$$

Logo:

$$s_{4}(x, y, z, [x, y]) = 2[z, [x, y]^{2}] + [x, y] \circ ([z, [y, x]] + [y, [x, z]] + [x, [z, y]])$$

$$+ [x, [x, y] \circ [y, z]] - [y, [x, y] \circ [x, z]]$$

$$\Rightarrow s_{4}(x, y, z, [x, y]) = 2[z, [x, y]^{2}] + [x, [x, y] \circ [y, z]] - [y, [x, y] \circ [x, z]]$$

como queríamos.

Proposição 4.6.7. Em uma álgebra de Cayley tem-se:

$$\kappa(x; y; z, v, w) = s_4(z, v, w, x \circ y) - x \circ s_4(z, v, w, y) - y \circ s_4(z, v, w, x)$$

Demonstração: Lembrando a conclusão da Proposição 4.6.4, tivemos:

$$s_3^+(y,z,w)(x) - s_4(y,z,w,x) = [x, 2s_3(y,z,w)]$$

Fazendo y=z, z=v, e pondo $x\circ y$ no lugar do argumento x, teremos:

$$s_3^+(z, v, w)(x \circ y) - s_4(z, v, w, x \circ y) = 2(x \circ y)s_3 - 2s_3(x \circ y)$$

$$\Rightarrow s_3^+(x \circ y) = s_4(z, v, w, x \circ y) + 2(x \circ y)s_3 - 2s_3(x \circ y)$$
(1)

Voltando à forma original da expressão obtida na mesma proposição, calculemos:

$$(s_3^+(x)) \circ y = s_4(z, v, w, x) \circ y + 2(xs_3) \circ y - 2(s_3x) \circ y \tag{2}$$

$$(s_3^+(y)) \circ x = s_4(z, v, w, y) \circ x + 2(ys_3) \circ x - 2(s_3y) \circ x$$
 (3)

Fazendo (1)-(2)-(3) teremos no primeiro membro a expressão de definição de κ . No segundo membro temos os termos desejados mais as seguintes parcelas, que mostraremos que se anulam:

$$2(x \circ y)s_3 - 2s_3(x \circ y) - 2(xs_3) \circ y + 2(s_3x) \circ y - 2(ys_3) \circ x + 2(s_3y) \circ x$$

$$= 2(xys_3 + yxs_3 - s_3xy - s_3yx - xs_3y - yxs_3 + s_3xy + ys_3x - ys_3x - xys_3 + s_3yx + xs_3y) = 0$$

Corolário 4.6.8. Em uma álgebra de Cayley tem-se:

$$\kappa(x, y; x, y, z) = s_4(x, y, z, x \circ y).$$

Demonstração: É imediato, bastando fazer z = x, v = y e w = z. Teremos:

$$\kappa(x, y; x, y, z) = s_4(x, y, z, x \circ y) - x \circ s_4(x, y, z, y) - y \circ s_4(x, y, z, x)$$

$$\Rightarrow \kappa(x, y; x, y, z) = s_4(x, y, z, x \circ y).$$

Teorema 4.6.9. O subespaço dos elementos alternados em x e y de grau [2,2,1] no ideal I das identidades de grau 5 é gerado por $s_4(x,y,z,x\circ y)$ e $q(x,y,z)=[x,[x,y]\circ[y,z]]+[y,[x,y]\circ[x,z]].$

Demonstração: A argumentação é inteiramente análoga a do caso simétrico.

Mostramos assim que g e h são conseqüências de χ e κ , logo, f também é. Qualquer outra identidade obtida de f deve pertencer ao ideal associador dos elementos de grau [2,2,1]. Um elemento qualquer deste ideal associador é uma combinação linear de (xy)a, (yx)a, (xa)y, (ax)y, (ya)x e (ay)x, onde a=(x,y,z). Vamos mostrar que, neste caso, f=0. Mas antes, cabe esclarecer porque não precisamos dos termos com parêntesis à direita no ideal associador, como x(ya), x(ay), etc. Para isto iremos demonstrar um lema que estabelece importantes relações entre o associador e o comutador em uma álgebra alternativa.

Lema 4.6.10. Em uma álgebra alternativa A, são válidas as seguintes igualdades, para todos $x, y, z \in A$:

- (i) (x, y, (x, y, z)) = [x, y](x, y, z);
- (ii) ((x, y, z), x, y) = -(x, y, z)[x, y];
- (iii) $[x, y] \circ (x, y, z) = 0;$
- (iv) [x, (y, z, w)] = (x, y, zw) + (x, z, wy) + (x, w, yz).

Demonstração:

(i) Vamos provar antes a seguinte identidade, válida para álgebras alternativas: (xy)(x,y,z) = y(x(x,y,z)). Devemos linearizar a identidade (i) de Moufang, (xyx)z = x(y(xz)), com $x \to x + w$:

$$((x+w)y(x+w))z = (x+w)(y((x+w)z))$$

$$\Rightarrow ((xy+wy)(x+w))z = (x+w)(y(xz+wz))$$

$$\Rightarrow (xyx + (xy)w + (wy)x + wyw)z = (x + w)(y(xz) + y(wz))$$

$$\Rightarrow (xyx)z + ((xy)w)z + ((wy)x)z + (wyw)z$$

$$= x(y(xz)) + x(y(wz)) + w(y(xz)) + w(y(wz))$$

$$\Rightarrow ((xy)w)z + ((wy)x)z = x(y(wz)) + w(y(xz))$$

Fazendo w = xy, x = y e y = x, obtemos:

$$((yx)(xy))z + ((xyx)y)z = y(x((xy)z)) + (xy)(x(yz))$$

Note que: $(xyx)y = (xy)^2$. De fato:

$$(xyx)y - (xy)^2 = ((xy)x)y - (xy)(xy) = (xy, x, y) = 0$$
, por 4.5.3 (i).

Ficamos então com:
$$((yx)(xy))z + (xy)^2z = y(x((xy)z)) + (xy)(x(yz))$$
 (I)

Calculamos agora: (xy)(x, y, z) - y(x(x, y, z))

$$= (xy)((xy)z - x(yz)) - y(x((xy)z - x(yz)))$$

$$= (xy)(xy)z - (xy)(x(yz)) - y(x((xy)z) - x(x(yz)))$$

$$= (xy)^2z - (xy)(x(yz)) - y(x((xy)z)) + y(x^2(yz))$$

$$\stackrel{(I)}{=} (xy)^2z - ((yx)(xy))z - (xy)^2z + y(x^2(yz)) \stackrel{*}{=} -(yx^2y)z + (yx^2y)z = 0$$
(*) Moufang (i) e (ii)

Calculamos, finalmente:

$$(x, y, (x, y, z)) = -(y, x, (x, y, z)) = y(x(x, y, z)) - (yx)(x, y, z)$$
$$= (xy)(x, y, z) - (yx)(x, y, z) = [x, y](x, y, z)$$

(ii) De maneira análoga ao caso anterior, provemos primeiro que, em uma álgebra alternativa vale: (x, y, z)(xy) = ((x, y, z)y)x. Vamos agora linearizar Moufang (ii), (xy)(zx) = x(yz)x, com $x \to x + w$:

$$((x+w)y)(z(x+w)) = (x+w)(yz)(x+w)$$

$$\Rightarrow (xy+wy)(zx+zw) = (x(yz)+w(yz))(x+w)$$

$$\Rightarrow (xy)(zx) + (xy)(zw) + (wy)(zx) + (wy)(zw)$$

$$= x(yz)x + (x(yz))w + (w(yz))x + (w(yz))w$$

$$\Rightarrow (xy)(zw) + (wy)(zx) = (x(yz))w + (w(yz))x$$

$$\Rightarrow (xy)(zw) - (x(yz))w = (w(yz))x - (wy)(zx)$$

Fazendo w = xy, obtemos:

$$(xy)(z(xy)) - (x(yz))(xy) = ((xy)(yz))x - ((xy)y)(zx)$$
$$= ((xy)(yz))x - x(y^2z)x$$
(II)

Calculamos agora: (x, y, z)(xy) - ((x, y, z)y)x

$$= ((xy)z - x(yz))(xy) - (((xy)z - x(yz))y)x$$

$$= (xy)z(xy) - (x(yz))(xy) - (((xy)z)y)x + ((x(yz))y)x$$

$$\stackrel{(II)}{=} ((xy)(yz))x - x(y^2z)x - x(yzy)x + ((x(yz))y)x$$

$$= [(xy)(yz) - x(y^2z) - x(yzy) + (x(yz))y]x$$

$$= [(xy)(yz) - x(y(yz)) + (x(yz))y - x((yz)y)]x$$

$$= [(xy, yz) + (x, yz, y)]x = 0$$

Calculamos finalmente:

$$((x, y, z), x, y) = -((x, y, z), y, x) = (x, y, z)(yx) - ((x, y, z)y)x$$
$$= (x, y, z)(yx) - (x, y, z)(xy) = -(x, y, z)[x, y]$$

(iii) Usando as igualdades que acabamos de provar, calculamos:

$$[x,y] \circ (x,y,z) = [x,y](x,y,z) + (x,y,z)[x,y]$$
$$= (x,y,(x,y,z)) - ((x,y,z),x,y) = 0$$

(iv) Como em (ii), vamos usar a linearização da identidade (ii) de Moufang,

(xy)(zx) = x(yz)x, onde obtivemos:

$$(xy)(zw) - (x(yz))w = (w(yz))x - (wy)(zx)$$
 (III)

Calculamos agora:

$$x(y, z, w) = x((yz)w) - x(y(zw))$$

$$= -(x, yz, w) + (x(yz))w + (x, y, zw) - (xy)(zw)$$

$$\stackrel{(III)}{=} -(x, yz, w) + (x, y, zw) + (wy)(zx) - (w(yz))x$$

$$= -(x, yz, w) + (x, y, zw) + (w, y, z)x - ((wy)z)x + (wy)(zx)$$

$$= (x, w, yz) + (x, y, zw) + (w, y, z)x - (wy, z, x)$$

$$\Rightarrow x(y,z,w) - (y,z,w)x = (x,y,zw) + (x,z,wy) + (x,w,yz)$$

O lema anterior nos mostra que não são necessários os termos com parêntesis à direita. De fato, fazendo (x, y, z) = a temos:

$$(xy)a - x(ya) = (x, y, a) \stackrel{(i)}{=} [x, y]a = (xy)a - (yx)a \implies x(ya) = (yx)a$$

Analogamente obtemos:

$$x(ay) = (ax)y, y(xa) = (xy)a, a(xy) = (xa)y,$$

 $y(ax) = (ay)x, a(yx) = (ya)x.$

Teorema 4.6.11. Se f é uma identidade de grau [2,2,1] pertencente ao ideal associador, então f=0.

Demonstração: Podemos escrever:

$$f = \alpha_1(xy)a + \alpha_2(yx)a + \alpha_3(xa)y + \alpha_4(ax)y + \alpha_5(ya)x + \alpha_6(ay)x$$

Vamos fazer substituições em x, y, z por elementos da base dos octônios.

Substituição (1): $x = 1 + e_1, y = 1 + e_2, z = e_4$

$$(xy)a = ((1+e_1)(1+e_2))(1+e_1, 1+e_2, e_4)$$

$$= (1+e_1+e_2+e_3)(e_1, e_2, e_4) = (1+e_1+e_2+e_3)(2e_7)$$

$$= 2(e_7+e_6-e_5-e_4)$$

$$(yx)a = ((1+e_2)(1+e_1))(1+e_1, 1+e_2, e_4)$$

$$= (1+e_1+e_2-e_3)(e_1, e_2, e_4) = (1+e_1+e_2-e_3)(2e_7)$$

$$= 2(e_7+e_6-e_5+e_4)$$

Omitimos os detalhes dos próximos cálculos, indicando apenas os resultados obtidos, que são:

$$(xa)y = 2(e_7 + e_6 + e_5 + e_4), (ax)y = 2(e_7 - e_6 + e_5 - e_4),$$

 $(ya)x = 2(e_7 - e_6 - e_5 - e_4), (ay)x = 2(e_7 - e_6 + e_5 + e_4)$

A expressão de f fica então, após cancelarmos o 2:

$$f = \alpha_1(e_7 + e_6 - e_5 - e_4) + \alpha_2(e_7 + e_6 - e_5 + e_4) + \alpha_3(e_7 + e_6 + e_5 + e_4)$$

+ $\alpha_4(e_7 - e_6 + e_5 - e_4) + \alpha_5(e_7 - e_6 - e_5 - e_4) + \alpha_6(e_7 - e_6 + e_5 + e_4)$ (1)

Substituição (2): $e_1, e_1 + e_2, e_4$

$$(xy)a = (e_1(e_1 + e_2))(e_1, e_1 + e_2, e_4)$$

$$= (-1 + e_3)(e_1, e_2, e_4) = (-1 + e_3)(2e_7) = 2(-e_7 - e_4)$$

$$(yx)a = ((e_1 + e_2)e_1)(e_1, e_1 + e_2, e_4)$$

$$= (-1 - e_3)(e_1, e_2, e_4) = (-1 - e_3)(2e_7) = 2(-e_7 + e_4)$$

Após os devidos cálculos obtemos os demais elementos:

$$(xa)y = 2(e_7 + e_4), (ax)y = 2(-e_7 - e_4), (ya)x = 2(e_7 - e_4),$$

 $(ay)x = 2(-e_7 + e_4)$

Resulta, para f:

$$f = \alpha_1(-e_7 - e_4) + \alpha_2(-e_7 + e_4) + \alpha_3(e_7 + e_4) + \alpha_4(-e_7 - e_4) + \alpha_5(e_7 - e_4) + \alpha_6(-e_7 + e_4)$$
(2)

Igualando a 0 as expressões (1) e (2), pois f é uma identidade, obtemos, após colocar em evidência os e_i :

$$(\alpha_{1} + \alpha_{2} + \alpha_{3} + \alpha_{4} + \alpha_{5} + \alpha_{6})e_{7} = 0$$

$$(\alpha_{1} + \alpha_{2} + \alpha_{3} - \alpha_{4} - \alpha_{5} - \alpha_{6})e_{6} = 0$$

$$(-\alpha_{1} - \alpha_{2} + \alpha_{3} + \alpha_{4} - \alpha_{5} + \alpha_{6})e_{5} = 0$$

$$(-\alpha_{1} + \alpha_{2} + \alpha_{3} - \alpha_{4} - \alpha_{5} + \alpha_{6})e_{4} = 0$$

$$(-\alpha_{1} - \alpha_{2} + \alpha_{3} - \alpha_{4} + \alpha_{5} - \alpha_{6})e_{7} = 0$$

$$(-\alpha_{1} + \alpha_{2} + \alpha_{3} - \alpha_{4} - \alpha_{5} + \alpha_{6})e_{4} = 0$$

Os coeficientes dos e_i devem se anular, o que resulta em um sistema homogêneo nas incógnitas $\alpha_1, \ldots, \alpha_6$. Após escalonamento chegamos a:

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 = 0$$

$$\alpha_2 + \alpha_3 + \alpha_6 = 0$$

$$\alpha_3 + \alpha_4 + \alpha_6 = 0$$

$$\alpha_4 - \alpha_5 + \alpha_6 = 0$$

$$-\alpha_5 = 0$$

Trata-se de um sistema indeterminado com variável livre α_6 . Sua solução é:

$$\alpha_3 = \alpha_5 = 0, \quad \alpha_4 = \alpha_2 = -\alpha_6, \quad \alpha_1 = \alpha_6.$$
Assim, $f = \alpha_6((xy)a - (yx)a - (ax)y + (ay)x) = \alpha_6 g.$

$$g = (xy)a - (yx)a - (ax)y + (ay)x$$

$$= [x, y]a - (a, x, y) - a(xy) + (a, y, x) + a(yx)$$

$$= [x, y]a - 2(a, x, y) - a[x, y]$$

Pelo Lema 4.6.10 (iii): $[x,y] \circ a = 0 \implies [x,y]a = -a[x,y]$

e por 4.6.10 (i):
$$(x, y, a) = [x, y]a$$

o que nos leva a:
$$g = 2(x, y, a) - 2(x, y, a) = 0.$$

E portanto:
$$f = 0$$
.

Identidades de grau [2, 1, 1, 1]

Seja f(x, y, z, w) uma identidade de grau [2, 1, 1, 1]. Então ϕf está no ideal das identidades associativas. Vamos explicitar os elementos geradores deste ideal. Veremos que todos são conseqüência de χ e de κ . Por fim, se uma identidade f pertence ao ideal associador de grau [2, 1, 1, 1], provaremos que f = 0.

Proposição 4.6.12. No ideal das identidades associativas, o subespaço das identidades de grau [2,1,1,1] é gerado pelos seguintes elementos:

$$x \circ s_4(x, y, z, w), \quad [x, s_4(x, y, z, w)], \quad s_4(x^2, y, z, w), \quad s_4(x, x \circ y, z, w)$$

 $s_4(x, [x, y], z, w), \quad [x, [x, y] \circ [z, w]], \quad [y, [x, z] \circ [x, w]]$

mais as permutações cíclicas de y, z, w nos 4 últimos polinômios, a saber:

$$s_4(x, x \circ z, w, y), \quad s_4(x, x \circ w, y, z), \quad s_4(x, [x, z], w, y), \quad s_4(x, [x, w], y, z)$$

 $[x, [x, z] \circ [w, y]], \quad [x, [x, w] \circ [y, z]], \quad [z, [x, w] \circ [x, y]], \quad [w, [x, y] \circ [x, z]].$

Demonstração: Uma identidade de grau [2, 1, 1, 1] é formada por monômios de grau 2 em x e grau 1 em y, z, w. Já vimos que as identidades de grau 5 em Ass[X] (ou em $M_2(F)$) são de um dos seguintes tipos:

$$_s_4(_,_,_,_)$$
 $s_4(_,_,_,_)$ $s_4(_,_,_,_)$ $[[_,_] \circ [_,_],_].$

Obtemos os geradores do subespaço das identidades de grau [2,1,1,1], preenchendo os argumentos acima pelas variáveis x,y,z,w com grau [2,1,1,1], de modo a termos todas as possibilidades de distribuições dessas variáveis. Um simples raciocínio combinatório permite concluir que este preenchimento produz os mesmos elementos indicados pela proposição.

Proposição 4.6.13. No conjunto de geradores do subespaço das identidades de grau [2, 1, 1, 1], tem-se:

- (i) $x \circ s_4(x, y, z, w)$ é conseqüência de κ e de $s_4(x^2, y, z, w)$;
- (ii) $[x, s_4(x, y, z, w)]$ é conseqüência de χ ;
- (iii) $s_4(x, [x, y], z, w)$ é conseqüência de χ ;
- (iv) $s_4(x, x \circ y, z, w)$ é conseqüência de κ e de $s_4(x^2, y, z, w)$;
- (v) $[x, [x, y] \circ [z, w]]$ e $[y, [x, z] \circ [x, w]]$ são conseqüências de χ .

Demonstração:

- (i) Pela Proposição 4.6.4: $\kappa(x; y, z, w) = s_4(y, z, w, x^2) s_4(y, z, w, x) \circ x$ Mas, notando que: $s_4(y, z, w, x^2) = s_4(x^2, y, z, w)$, $s_4(y, z, w, x) \circ x = x \circ s_4(y, z, w, x) = s_4(y, z, w, x) = s_4(x, y, z, w)$, podemos escrever: $x \circ s_4(x, y, z, w) = s_4(x^2, y, z, w) - \kappa(x; y, z, w)$
- (ii) $[x, s_4(x, y, z, w)] = x([x, y] \circ [z, w] + [x, z] \circ [w, y] + [x, w] \circ [y, z])$ $-([x, y] \circ [z, w] + [x, z] \circ [w, y] + [x, w] \circ [y, z])x$ $=\underbrace{[x, [x, y] \circ [z, w]]}_{(1)} + \underbrace{[x, [x, z] \circ [w, y]]}_{(2)} + \underbrace{[x, [x, w] \circ [y, z]]}_{(3)}$

Vamos linearizar $\chi = [[x, y]^2, x]$ para obter as parcelas (1), (2) e (3).

$$\begin{split} & [[x+z+w,y+x+z]^2,x+z+w] \\ & = [([x,y]+[x,z]+[z,y]+[w,y]+[w,x]+[w,z])^2 \\ & + [x,y]\circ[x,z]+[x,y]\circ[z,y]+[x,y]\circ[w,y]+[x,y]\circ[w,x] + \underbrace{[x,y]\circ[w,z]}_{(1)} \end{split}$$

$$\begin{split} &+ [x,z] \circ [z,y] + \underbrace{[x,z] \circ [w,y]}_{(2)} + [x,z] \circ [w,x] + [x,z] \circ [w,z] \\ &+ [z,y] \circ [w,y] + \underbrace{[z,y] \circ [w,x]}_{(3)} + [z,y] \circ [w,z] \\ &+ [w,y] \circ [w,x] + [w,y] \circ [w,z] \\ &+ [w,x] \circ [w,z], x + z + w] \end{split}$$

Estão assinalados os termos termos (1), (2) e (3), que formarão com x os comutadores procurados:

$$\begin{split} &[[x,y]\circ[w,z],x] = [x,[x,y]\circ[z,w]] \\ &[[x,z]\circ[w,y],x] = -[x,[x,z]\circ[w,y]] \\ &[[z,y]\circ[w,x],x] = -[x,[x,w]\circ[y,z]] \end{split}$$

(iii) Pelo Lema 4.6.5 (i), temos:

$$s_4(x, [x, y], z, w) = [x, [x, y]] \circ [z, w] + [x, z] \circ [w, [x, y]] + [x, w] \circ [[x, y], z]$$
 (1)

Fazendo em 4.6.5 (ii), y = [x, y] e z = [z, w] e aplicando na primeira parcela de (1):

$$[x, [x, y]] \circ [z, w] = \underbrace{[x, [x, y] \circ [z, w]]}_{(a)} - [x, y] \circ [x, [z, w]]$$
 (2)

Fazendo em 4.6.5 (ii), x=w, y=[x,y] e z=[x,z] e aplicando na segunda parcela de (1):

$$[x,z] \circ [w,[x,y]] = [w,[x,y]] \circ [x,z] = \underbrace{[w,[x,y] \circ [x,z]]}_{(b)} - [x,y] \circ [w,[x,z]] \tag{3}$$

Fazendo em 4.6.5 (ii), x=z, y=[x,y] e z=[x,w] e aplicando na terceira parcela de (1):

$$[x, w] \circ [[x, y], z] = -[z, [x, y]] \circ [x, w] = \underbrace{-[z, [x, y] \circ [x, w]]}_{(c)} + [x, y] \circ [z, [x, w]]$$
(4)

Levando (2), (3) e (4) em (1) e agrupando as expressões (a), (b) e (c), nos dá:

$$s_4(x, [x, y], z, w) = [x, [x, y] \circ [z, w]] + [w, [x, y] \circ [x, z]] - [z, [x, y] \circ [x, w]] + [x, y] \circ ([x, [w, z]] + [w, [z, x]] + [z, [x, w]])$$

Notando que, por 4.6.5 (iii) (identidade de Jacobi),

$$[x,[w,z]]+[w,[z,x]]+[z,[x,w]]=0$$
, podemos escrever:
$$s_4(x,[x,y],z,w)=[x,[x,y]\circ[z,w]]+[w,[x,y]\circ[x,z]]-[z,[x,y]\circ[x,w]]$$
 Portanto, s_4 é conseqüência de χ .

(iv) Fazendo y=x na Proposição 4.6.4, temos: $\kappa(x;x,z,w)=s_4(x,z,w,x^2)$. Linearizando com $x+\lambda y$:

$$\kappa(x + \lambda y; x + \lambda y, z, w) = s_4(x + \lambda y, (x + \lambda y)^2, z, w)$$

$$= s_4(x, x^2, z, w) + \lambda s_4(x, x \circ y, z, w) + \lambda^2 s_4(x, y^2, z, w)$$

$$+ \lambda s_4(y, x^2, z, w) + \lambda^2(y, x \circ y, z, w) + \lambda^3 s_4(y, y^2, z, w)$$

$$= \kappa(x; x, z, w) + \lambda(s_4(x, x \circ y, z, w) - s_4(x^2, y, z, w))$$

$$+ \lambda^2(s_4(y, x \circ y, z, w) - s_4(y^2, x, z, w)) + \lambda^3 \kappa(y; y, z, w)$$

Fazendo:
$$K = \kappa(x + \lambda y; x + \lambda y, z, w), \quad K_1 = \kappa(x; x, z, w),$$

$$K_2 = \kappa(y; y, z, w), \quad L = s_4(x, x \circ y, z, w) - s_4(x^2, y, z, w)$$

$$T = s_4(y, x \circ y, z, w) - s_4(y^2, x, z, w),$$

escrevemos:
$$K = K_1 + \lambda L + \lambda^2 T + \lambda^3 K_2$$

Substituindo alguns valores para λ :

$$\lambda = 1: \quad K = K_1 + L + T + K_2; \qquad \lambda = 2: \quad K' = K_1 + 2L + 4T + 8K_2$$

 $\Rightarrow \quad L = \frac{1}{2} \left(4(K_2 + K) - K' - 3K_1 \right)$

Ou, mais explicitamente:

$$\lambda = 1: \quad \kappa(x+y; x+y, z, w) = \kappa(x; x, z, w)$$

$$+ [s_4(x, x \circ y, z, w) - s_4(x^2, y, z, w)]$$

$$+ [s_4(y, x \circ y, z, w) - s_4(y^2, x, z, w)]$$

$$+ \kappa(y; y, z, w)$$

$$\lambda = 2: \quad \kappa(x+2y; x+2y, z, w) = \kappa(x; x, z, w)$$

$$+ 2[s_4(x, x \circ y, z, w) - s_4(x^2, y, z, w)]$$

$$+ 4[s_4(y, x \circ y, z, w) - s_4(y^2, x, z, w)]$$

$$+ 8\kappa(y; y, z, w)$$

$$\kappa(x + 2y; x + 2y, z, w) - 4\kappa(x + y; x + y, z, w)$$

$$= -3\kappa(x; x, z, w) - 2(s_4(x, x \circ y, z, w) - s_4(x^2, y, z, w))$$

$$+ 4\kappa(y; y, z, w)$$

$$\Rightarrow s_4(x; x \circ y, z, w) - s_4(x^2, y, z, w)$$

$$= -\frac{1}{2} \left[\kappa(x + 2y; x + 2y, z, w) - 4(\kappa(x + y; x + y, z, w) + \kappa(y; y, z, w)) + 3\kappa(y; y; z; w) \right]$$

(v)
$$\acute{\rm E}$$
 imediato.

Lembrando que estamos considerando uma identidade $f \in Alt[X]$ de grau [2,1,1,1], com as três últimas variáveis alternadas. Conforme a proposição anterior sua imagem ϕf em Ass[X] é conseqüência de χ , de κ e de $s_4(x^2,y,z,w)$. Podemos escrever então:

$$\phi f = \lambda \kappa + \mu \chi + \gamma s_4$$

onde $\lambda, \mu, \gamma \in F$.

Notando que $\phi \kappa = \kappa$, $\phi \chi = \chi$ e $\phi s_4^i = s_4$, $\forall i = 1, ..., 5$, podemos fazer:

$$f' = f - \lambda \kappa - \mu \chi - \sum_{i} \gamma_{i} s_{4}^{i} \implies \phi f' = \phi f - \lambda \kappa - \mu \chi - \gamma s_{4} = \phi f - \phi f = 0.$$

Obtivemos assim, uma identidade f' no ideal associador. Mostraremos que f' = 0, mas antes iremos explicitar os elementos do ideal associador das identidades de grau [2,1,1,1]. Os elementos geradores deste ideal são: (xa)y, (ax)y, (xy)a, (yx)a, (ay)x e (ya)x, onde a = (x, z, w), mais as permutações cíclicas de y, z, w e x^2b, xbx, bx^2 , onde b = (y, z, w). Deveríamos ter também os termos com parêntesis à direita, x(ay), x(ya), y(xa), y(xa), y(xa), y(xa). O lema a seguir mostra que bastam os nove primeiros termos e mais apenas um com parêntesis à direita.

Lema 4.6.14. O ideal associador das identidades de grau [2,1,1,1] alternadas nas variáveis lineares, é gerado pelos seguintes elementos:

$$(xy)(x,z,w) + (xz)(x,w,y) + (xw)(x,y,z),$$

$$(yx)(x,z,w) + (zx)(x,w,y) + (wx)(x,y,z),$$

$$(x(x,z,w))y + (x(x,w,y))z + (x(x,y,z))w,$$

$$(y(x,z,w))x + (z(x,w,y))x + (w(x,y,z))x,$$

$$((x,z,w)x)y + ((x,w,y)x)z + ((x,y,z)x)w,$$

$$((x,z,w)y)x + ((x,w,y)z)x + ((x,y,z)w)x,$$

$$x(y(x,z,w)) + x(z(x,w,y)) + x(w(x,y,z)),$$

$$x^2(y,z,w), \quad x(y,z,w)x, \quad (y,z,w)x^2.$$

Demonstração: Basta mostrar que apenas um termo com parêntesis à direita é necessário. Consideremos os produtos à direita: a(bc), b(ac), a(cb), c(ab), b(ca), c(ba).

Fixando um desses produtos, digamos a(bc), vamos tentar obter os outros. Usaremos a alternatividade do associador.

$$(b, a, c) = (ba)c - b(ac) = -(a, b, c) = a(bc) - (ab)c$$

$$\Rightarrow b(ac) = (ba)c + (ab)c - a(bc)$$

$$(c, a, b) = (ca)b - c(ab) = (a, b, c) = (ab)c - a(bc)$$

$$\Rightarrow c(ab) = (ca)b - (ab)c + a(bc)$$

Para os demais produtos os cálculos são inteiramente análogos.

Definição 4.6.2. Chama-se triplo produto de Jordan à expressão:

$$\{xyz\} = (xy)z + z(yx)$$

Teorema 4.6.15. Se f é uma identidade no ideal associador de grau [2, 1, 1, 1], então f = 0.

Demonstração: Vamos fazer substituições nos elementos geradores, por elementos da base dos octônios.

(1)
$$x = 1 + e_1$$
, $y = 1 + e_2$, $z = e_4$, $w = e_3$
 $(x, z, w) = (1 + e_1, e_4, e_3) = (e_1, e_4, e_3) = (e_1e_4)e_3 - e_1(e_4e_3) = 2e_6$
 $(x, w, y) = (e_1, e_3, e_2) = (e_1e_3)e_2 - e_1(e_3e_2) = 0$
 $(x, y, z) = (e_1, e_2, e_4) = 2e_7$

$$(y, z, w) = (e_2, e_4, e_3) = -2e_5$$

Agora calculamos cada um dos dez termos correspondentes aos elementos do conjunto gerador de I. Chamaremos estes termos de u_1, \ldots, u_{10} .

$$(xy)(x, z, w) = ((1 + e_1)(1 + e_2))(2e_6) = 2(e_6 - e_7 - e_4 + e_5)$$

$$(xw)(x, y, z) = ((1 + e_1)e_3)2e_7 = -2(e_4 - e_5)$$

$$\Rightarrow u_1 = -4e_4 + 4e_5 + 2e_6 - 2e_7$$

$$(yx)(x, z, w) = ((1 + e_2)(1 + e_1))(2e_6) = 2(e_6 - e_7 - e_4 - e_5)$$

$$(wx)(x, y, z) = (e_3(1 + e_1))(2e_7) = -2(e_4 + e_5)$$

$$\Rightarrow u_2 = 4e_4 - 4e_5 + 2e_6 - 2e_7$$

Prosseguindo com esses cálculos, que indicaremos de forma sucinta, obtemos os demais valores:

$$(x(x,z,w))y = 2(e_4 - e_5 + e_6 - e_7), \quad (x(x,z,y))w = -2(-e_4 + e_5)$$

$$\Rightarrow u_3 = 4e_4 - 4e_5 + 2e_6 - 2e_7$$

$$(y(x,z,w))x = 2(-e_4 + e_5 + e_6 + e_7), \quad (w(x,y,z))x = -2(e_4 - e_5)$$

$$\Rightarrow u_4 = -4e_4 + 2e_6 + 2e_7 + 4e_5$$

$$((x,z,w)x)y = 2(e_4 + e_5 + e_6 + e_7), \quad ((x,y,z)x)w = -2(-e_4 - e_5)$$

$$\Rightarrow u_5 = 4e_4 - 4e_5 + 2e_6 + 2e_7$$

$$((x,z,w)y)x = 2(e_6 + e_4 + e_7 - e_5), \quad ((x,y,z)w)x = 2(e_4 - e_5)$$

$$\Rightarrow u_6 = -4e_4 - 4e_5 + 2e_6 + 2e_7$$

$$x(y(x,z,w)) = 2(-e_4 - e_5 + e_6 - e_7), \quad x(w(x,y,z)) = -2(e_4 + e_5)$$

$$\Rightarrow u_7 = -4e_4 - 4e_5 + 2e_6 - 2e_7$$

$$x^2(y,z,w) = 4e_4 \quad \Rightarrow u_8 = 4e_4; \quad x(y,z,w)x = -4e_5 \quad \Rightarrow u_9 = -4e_5$$

$$(y,z,w)x^2 = -4e_4 \quad \Rightarrow u_{10} = -4e_4$$

A identidade f pode ser escrita: $f = \alpha_1 u_1 + \cdots + \alpha_{10} u_{10}$

$$\Rightarrow f = (-4e_4 + 4e_5 + 2e_6 - 2e_7)\alpha_1 + \dots + (-4e_4)\alpha_{10}$$

Colocando em evidência os e_i obtemos um conjunto de 4 equações nas variáveis α_i :

$$-\alpha_{1} - \alpha_{2} + \alpha_{3} - \alpha_{4} + \alpha_{5} + \alpha_{6} - \alpha_{7} + \alpha_{8} - \alpha_{10} = 0$$

$$\alpha_{1} + \alpha_{2} + \alpha_{3} + \alpha_{4} + \alpha_{5} + \alpha_{6} + \alpha_{7} = 0$$

$$\alpha_{1} + \alpha_{2} + \alpha_{3} - \alpha_{4} - \alpha_{5} - \alpha_{6} + \alpha_{7} = 0$$

$$\alpha_{1} - \alpha_{2} - \alpha_{3} + \alpha_{4} + \alpha_{5} - \alpha_{6} - \alpha_{7} - \alpha_{9} = 0$$

Com estas equações podemos formar as 4 primeiras linhas de uma matriz:

(2)
$$x = 1 + e_1, y = e_2, z = e_4, w = e_6$$

 $(x, z, w) = (e_1, e_4, e_6) = -2e_3; (x, w, y) = (e_1, e_6, e_2) = -2e_5$
 $(x, y, z) = (e_1, e_2, e_4) = 2e_7; (y, z, w) = (e_2, e_4, e_6) = 0$
 $(xy)(x, z, w) = -2e_1 + 2, (xz)(x, w, y) = -2e_1 + 2, (xw)(x, y, z) = -2e_1 + 2$
 $\Rightarrow u_1 = -6e_1 + 6$

Efetuando os cálculos correspondentes obtemos para os outros u_i :

$$u_2 = -6e_1 - 6$$
, $u_3 = 6e_1 - 6$, $u_4 = -6e_1 + 6$, $u_5 = 6e_1 + 6$, $u_6 = 6e_1 - 6$, $u_7 = -6e_1 + 6$, $u_8 = u_9 = u_{10} = 0$

Mais duas equações são obtidas, que resultarão nas linhas 5 e 6 da matriz $10\times 10\colon$

(3)
$$x = 1 + e_1$$
, $y = e_2$, $z = e_4$, $w = -e_7$
 $(x, z, w) = (e_1, e_4, -e_7) = -2e_2$; $(x, w, y) = (e_1, -e_7, e_2) = -2e_4$
 $(x, y, z) = (e_1, e_2, e_4) = 2e_7$; $(y, z, w) = (e_2, e_4, e_6) = 2e_1$

Indicamos a seguir os valores dos u_i resultantes desta substituição:

$$u_1 = 6e_1 + 6$$
, $u_2 = -6e_1 + 6$, $u_3 = 6e_1 + 6$, $u_4 = 6e_1 + 6$,

$$u_5 = -6e_1 + 6$$
, $u_6 = 6e_1 + 6$, $u_7 = 6e_1 + 6$, $u_8 = u_9 = u_{10} = -4$

Obtemos mais duas equações que nos fornecem as linhas 7 e 8 da matriz:

(4)
$$x = e_1$$
, $y = e_2$, $z = e_4$, $w = e_3$
 $(x, z, w) = (e_1, e_4, e_3) = 2e_6$; $(x, w, y) = (e_1, e_3, e_2) = 0$
 $(x, y, z) = (e_1, e_2, e_4) = 2e_7$; $(y, z, w) = (e_2, e_4, e_3) = -2e_5$

Valores dos u_i resultantes desta substituição:

$$u_1 = 4e_7$$
, $u_2 = -4e_7$, $u_3 = -4e_7$, $u_4 = 4e_7$, $u_5 = 4e_7$, $u_6 = -4e_7$, $u_7 = -4e_7$, $u_8 = 2e_7$, $u_9 = -2e_7$, $u_{10} = 2e_7$

A equação obtida nos dará a linha 9 da matriz:

(5)
$$x = e_1, y = e_1, z = e_2, w = e_4$$

 $(x, z, w) = (e_1, e_2, e_4) = 2e_7; (x, w, y) = (e_1, e_4, e_1) = 0$
 $(x, y, z) = (e_1, e_1, e_2) = 0; (y, z, w) = (e_1, e_2, e_4) = 2e_7$

Valores dos u_i resultantes desta substituição:

$$u_1 = 2e_6$$
, $u_2 = 2e_6$, $u_3 = -2e_6$, $u_4 = -2e_6$, $u_5 = 2e_6$, $u_6 = 2e_6$, $u_7 = 2e_6$, $u_8 = 2e_6$, $u_9 = -2e_6$, $u_{10} = 2e_6$

A equação obtida nos dará a linha 10 da matriz:

A matriz dos coeficientes do sistema homogêneo nas incógnitas $\alpha_1, \ldots, \alpha_{10}$ obtida por meio das substituições indicadas acima, é a seguinte:

Sua forma escalonada é dada a seguir:

Resultam as seguintes relações entre as variáveis, onde fizemos a variável livre $\alpha_{10}=\alpha$:

$$\alpha_1 = \alpha_9 = -2\alpha$$
; $\alpha_2 = \alpha_5 = 0$; $\alpha_3 = \alpha_4 = \alpha_7 = \alpha_8 = \alpha$; $\alpha_6 = -\alpha$.

Substituindo estes valores na expressão de f, teremos:

$$f(x,y,z,w) = \alpha(-2((xy)(x,z,w) + (xz)(x,w,y) + (xw)(x,y,z))$$

$$+ ((x(x,z,w))y + (x(x,w,y))z + (x(x,y,z))w)$$

$$+ ((y(x,z,w))x + (z(x,w,y))x + (w(x,y,z))x)$$

$$- (((x,z,w)y)x + ((x,w,y)z)x + ((x,y,z)w)x)$$

$$+ (x(y(x,z,w)) + x(z(x,w,y)) + x(w(x,y,z)))$$

$$+ x^{2}(y,z,w) - 2x(y,z,w)x + (y,z,w)x^{2})$$

Provaremos que este polinômio é igual a zero em Alt[X].

Afirmação:

$$f = [x, [x, (y, z, w)]] + \sum_{(y, z, w)} (\{x(x, z, w)y\} - \{xy(x, z, w)\} - (x, y, (x, z, w)))$$

onde $\sum_{(y,z,w)}$ indica a soma sobre todas as permutações cíclicas de y,z,w. Analisemos cada parcela.

$$\begin{split} [x,[x,(y,z,w)]] &= [x,x(y,z,w)-(y,z,w)x] = [x,x(y,z,w)]-[x,(y,z,w)x] \\ &= x(x(y,z,w))-x(y,z,w)x-x((y,z,w)x)+((y,z,w)x)x \\ &= x^2(y,z,w)-2x(y,z,w)+(y,z,w)x^2 \end{split}$$

Reconhecemos aí os 3 últimos termos da expressão de f.

 $\{x(x,z,w)y\}=(x(x,z,w))y+(y(x,z,w))x.$ Fazendo as permutações cíclicas em y,z,w, temos:

$$\sum_{(y,z,w)} \{x(x,z,w)y\} = (x(x,z,w))y + (y(x,z,w))x + (x(x,y,z))w + (w(x,y,z))x + (x(x,w,y))z + (z(x,w,y))x$$

Aí estão a segunda e a terceira parcelas de f.

 $\{xy(x,z,w)\}=(xy)(x,z,w)+((x,z,w)y)x$. É fácil ver que as permutações cíclicas em y,z,w do termo acima resultarão na soma da primeira e da quarta parcelas de f.

(x, y, (x, z, w)) = (xy)(x, z, w) - x(y(x, z, w)). Aplicando as permutações cíclicas obtemos a soma da primeira com a quinta parcela de f. Verificamos assim que a nova expressão de f corresponde à anterior, o que comprova a afirmação feita.

Vamos agora desenvolver explicitamente a soma cíclica, designando-a por $\sum\limits_{(y,z,w)}.$ Teremos então:

$$\begin{split} \sum_{(y,z,w)} &= \{x(x,z,w)y\} - \{xy(x,z,w)\} - (x,y,(x,z,w)) \\ &+ \{x(x,w,y)z\} - \{xz(x,w,y)\} - (x,z,(x,w,y)) \\ &+ \{x(x,y,z)w\} - \{zw(x,y,z)\} - (x,w,(x,y,z)) \\ &= \{x(x,z,w)y\} + \{xw(x,z,y)\} \\ &+ \{x(x,w,y)z\} + \{xy(x,w,z)\} \\ &+ \{x(x,y,z)w\} + \{xz(x,y,w)\} \\ &- (x,y,(x,z,w)) - (x,z,(x,w,y)) - (x,w,(x,y,z)) \end{split}$$

As parcelas agrupadas duas a duas têm associadores na forma $(x, z, _), (x, w, _)$ e $(x, y, _)$ respectivamente, o que sugere uma derivação.

Notando que:
$$(x, z, \{xwy\}) = \{(x, z, x)wy\} + \{x(x, z, w)y\} + \{xw(x, z, y)\},\$$

 $(x, w, \{xyz\}) = \{(x, w, x)yz\} + \{x(x, w, y)z\} + \{xy(x, w, z)\}$ e $(x, y, \{xzw\}) = \{(x, y, x)zw\} + \{x(x, y, z)w\} + \{xz(x, y, w)\}$

e ainda que (x, w, x) = (x, y, x) = (x, z, x) = 0, teremos:

$$\sum_{(y,z,w)} = ((x, z, \{xwy\}) + (x, w, \{xyz\}) + (x, y, \{xzw\}) - (x, z, (x, w, y)) - (x, w, (x, y, z)) - (x, y, (x, z, w))$$

Temos ainda: $\{xwy\}-(x,w,y)=(xw)y+(yw)x-(xw)y+x(wy)=(yw)x+x(wy)$. Daí:

$$\sum_{(y,z,w)} = ((x, z, x(wy) + (yw)x) + (x, w, x(yz) + (zy)x) + (x, y, x(zw) + (wz)x))$$

$$= ((x, z, x(wy)) + (x, z, (yw)x) + (x, w, x(yz)) + (x, w, (zy)x)$$

$$+ (x, y, x(zw)) + (x, y, (wz)x))$$

Pelo Lema 4.5.3 (i), (ii):

$$\begin{split} (x,z,x(wy)) + (x,z,(yw)x) &= -(x,x(wy),z) - (x,(yw)x,z) \\ &= -(x,wy,z)x - x(x,yw,z) \\ (x,w,x(yz)) + (x,w,(zy)x) &= -(x,yz,w)x - x(x,zy,w) \\ (x,y,x(zw)) + (x,y,(wz)x) &= -(x,zw,y)x - x(x,wz,y) \end{split}$$

Então:

$$\sum_{(y,z,w)} = x((x,z,yw) + (x,w,zy) + (x,y,wz)) + ((x,z,wy) + (x,w,yz) + (x,y,zw))x$$

Agora o Lema 4.6.10 (iv) nos dá:

$$\sum_{(y,z,w)} = x[x,(z,y,w)] + [x,(y,z,w)]x = x[x,(z,y,w)] - [x,(z,y,w)]x$$
$$= [x,[x,(z,y,w)]] = -[x,[x,(y,z,w)]]$$

Portanto
$$f = [x, [x, (y, z, w)]] - [x, [x, (y, z, w)]] = 0$$

Seja f uma identidade de grau [1,1,1,1,1], ou multilinear. Temos que f é uma combinação linear de produtos de 5 elementos x,y,z,v,w nas possíveis distribuições

de parêntesis entre eles. São ao todo 14 distribuições, que constituirão nos 14 elementos geradores do ideal das identidades multilineares de grau [1, 1, 1, 1, 1]. Designaremos estes geradores por d_1, \ldots, d_{14} , explicitados a seguir:

$$d_{1} = _(_(_(_(__))); d_{2} = _(_((__)_)); d_{3} = _((_(__))_); d_{4} = _(((__))_); d_{5} = _((__)(__)); d_{6} = (_((__)))_; d_{7} = (_((__))_); d_{8} = ((_(__))_)_; d_{9} = (((__))_)_; d_{10} = ((__)(__))_; d_{11} = ((__))(__); d_{12} = (__)(_(__)); d_{13} = (__)((__)); d_{14} = (_(__))(__)$$

Faremos as seguintes substituições:

1.
$$e_1, e_2, e_4, e_3, e_6$$
 2. $e_1, e_2, e_4, e_4, -e_7$ 3. e_1, e_2, e_4, e_3, e_5

4.
$$e_1, e_2, e_4, e_6, -e_7$$
 5. e_1, e_2, e_4, e_6, e_5 6. $e_1, e_2, e_4, -e_7, e_5$

7.
$$e_1, e_2, e_3, e_6, -e_7$$
 8. e_1, e_2, e_3, e_6, e_5 9. $e_1, e_2, e_3, -e_7, e_5$

10.
$$e_1, e_2, e_6, -e_7, e_5$$
 11. $1, e_2, e_4, e_3, e_6$ 12. $1, e_1, e_4, e_3, e_6$

13.
$$1, e_1, e_2, e_3, e_6$$
 14. $1, e_1, e_2, e_4, e_6$ 15. $1, e_1, e_2, e_4, e_3$

Após os cálculos obtemos a matriz dos coeficientes do sistema homogêneo nas incógnitas $\alpha_1, \ldots, \alpha_{14}$ indicada a seguir:

Após escalonamento obtemos a matriz:

Resultam as seguintes relações entre as variáveis, onde fizemos a variável livre $\alpha_{13}=\alpha$:

$$\alpha_1 = \alpha_2 = -\alpha; \quad \alpha_{12} = \alpha; \quad \alpha_3 = \alpha_4 = \dots = \alpha_{11} = \alpha_{14} = 0$$

A identidade f poderá ser escrita como um múltiplo linear dos produtos designados por d_1, d_2, d_{12} e d_{13} , uma vez que os coeficientes dos outros produtos se anulam nas substituições feitas. Temos portanto:

$$f = \alpha \sum_{\substack{(x,y,z,v,w) \\ (x,y,z,v,w)}} (-x(y(z,(vw))) - x(y((zv)w)) + (xy)(z(vw)) + (xy)((zv)w)),$$
 onde
$$\sum_{\substack{(x,y,z,v,w) \\ (x,y,z,v,w)}} \text{indica a soma sobre todas as permutações de } x,y,z,v,w.$$

Podemos escrever esta soma como:

$$(d_{13} - d_1) + (d_{12} - d_2) = (xy)((zv)w) - x(y(z, (vw))) + (xy)(z(vw)) - x(y((zv)w))$$

Note que:

$$(x, y, (z, v, w)) = (x, y, (zv)w) - (x, y, z(vw))$$

$$= \underbrace{(xy)((zv)w)}_{d_{13}} - \underbrace{x(y((zv)w))}_{d_{2}} - \underbrace{x(y(z(vw)))}_{d_{1}} + \underbrace{(xy)(z(vw))}_{d_{12}}$$

Portanto:
$$f = \alpha \sum_{(x,y,z,v,w)} (x,y,(z,v,w))$$

Afirmação:
$$\sum_{(x,y,z,v,w)} (x,y,(z,v,w)) = 0.$$

Vamos desenvolver esta soma sem precisar explicitar todos os 5! = 120 termos resultantes da permutação de 5 elementos. Fixando duas variáveis, permutamos as outras três dentro do associador interno. Obtemos assim uma soma de 6 associadores para cada duas variáveis fixadas. Como temos $A_{5,2} = 20$ maneiras de fixar duas dentre as cinco variáveis, teremos ao todo $6 \times 20 = 120$ termos, como deve ser.

As 20 somas podem ser representadas sinteticamente por:

$$\sum_{i=1}^{20} S_i = [(x, y, (z, v, w)) + \dots + (x, y, (w, v, z))]$$

$$+ [(y, x, (z, v, w)) + \dots + (y, x, (w, v, z))]$$

$$+ [(x, z, (y, v, w)) + \dots + (x, z, (v, w, y))]$$

$$+ [(z, x, (y, v, w)) + \dots + (z, x, (w, v, y))]$$

$$+ \dots + [(w, v, (x, y, z)) + \dots + (w, v, (z, y, x))]$$

Basta provar que uma dessas somas é zero. Por simetria todas serão. Assim, explicitemos a primeira delas:

$$S_{1} = [(x, y, (z, v, w)) + \dots + (x, y, (w, v, z))]$$

$$= (x, y, (z, v, w)) + (x, y, (z, w, v)) + (x, y, (v, z, w)) + (x, y, (v, w, z))$$

$$+ (x, y, (w, q, v)) + (x, y, (w, v, z))$$

$$= (x, y, (z, v, w)) + (x, y, -(z, v, w)) + (x, y, -(z, v, w)) + (x, y, (z, v, w))$$

$$+ (x, y, (z, v, w)) + (x, y, -(z, v, w)) = 0$$

Como todas as somas se anulam, a afirmação está provada. Portanto f = 0.

Provamos assim que uma identidade de grau [1,1,1,1,1] multilinear é nula. Portanto toda identidade de grau 5 não nula é consequência das identidades χ e κ , conforme afirmamos no início desta seção.

4.7 Resultados Recentes

Além das identidades de grau 5 que aqui apresentamos, existem também nas álgebras alternativas, identidades de grau 6 ou maior. Pesquisas recentes já explicitaram tais identidades ou, pelo menos, estabeleceram métodos mais gerais para sua deter-

minação. Em particular, Hentzel e Peresi, em seu trabalho "Identities for Cayley-Dickson Algebras" (ref. [10]) utilizaram métodos computacionais. Destacamos também o artigo "Identities for the Associator in Alternative Algebras", de Bremner-Hentzel (ref. [2]) envolvendo álgebras ternárias alternativas, em que foram encontradas identidades de grau 7, também com o uso de computadores.

Daremos aqui uma breve noção destas pesquisas, procurando apresentar alguns exemplos das identidades estudadas, e dos métodos utilizados pelos autores.

Em [10] é utilizado um algoritmo computacional que permite gerar todos os polinômios multilineares homogêneos candidatos a identidades. Expressando tais polinômios em bases convenientes de matrizes, e como combinações lineares de elementos do anel de grupo FS_n , impõe condições para que sejam identidades. Deduzem assim, as expressões das identidades de grau ≤ 6 .

Trata-se de um processo indutivo de geração de identidades. Embora os autores tenham se limitado a apresentar indentidades de grau ≤ 6 , o processo permite, em teoria, encontrar identidades de qualquer grau. Porém, existem limitações de ordem prática. Por ser geral, produz também identidades que são conseqüências das leis alternativas, devendo ser, então, descartadas. Para identificar quais identidades são efetivamente novas, utiliza as formas canônicas de matrizes que podem ser associadas às identidades. Antes de fazer esta associação é preciso encontrar uma base para expressar um polinômio multilinear homogêneo (candidato a identidade). Mas a álgebra alternativa livre não tem uma base natural. Assim é utilizado um isomorfismo para o anel de grupo das matrizes completas sobre F. Utilizando alguns resultados destas matrizes, mostra que um polinômio pode ser associado a uma soma direta das mesmas, para a qual existe uma base conveniente (em termos computacionais), com elementos não nulos somente na primeira coluna.

Obtém assim candidatos a identidades, substituindo os elementos da base de C(-1,-1,-1) e impondo uma lista de restrições sobre os coeficientes desses candidatos para que o polinômio seja uma identidade. Indicamos a seguir a identidade de grau 6 encontrada por este processo, onde a,b,c,d,e,f representam elementos arbitrários em C:

$$\left[\sum \{24a(b(c(de))) + 8a((b,c,d)e) - 11(a,b,(c,d,e))\}, f\right] = 0$$

Em [2], são pesquisadas identidades nas chamadas álgebras ternárias alternativas. Podemos definir, de maneira bem simples, uma álgebra ternária como sendo um par (A,t), onde A é um espaço vetorial sobre um corpo F e $T: A \times A \times A \rightarrow A$ é uma função trilinear. Esta função serve para definir um produto em (A,t), como t(a,b,c)=(ab)c-a(bc), que nada mais é que o nosso conhecido associador. Com isto, (A,t) se torna uma álgebra ternária.

Os autores apresentam identidades de grau 7 em três tipos de álgebras ternárias:

- 1. Álgebras Alternativas Livres;
- 2. Álgebras de Cayley;
- 3. Produto Cruzado.

Indicaremos aqui somente as identidades referentes ás álgebras ternárias de Cayley. Ressaltam os autores que os cálculos foram feitos em computador com um corpo de 103 elementos (característica 103), mas como o grau das identidades é ≤ 7 , que é muito menor que 103, é provável que esta restrição seja desnecessária. Assim, eles acreditam que os resultados valem em característica zero, o que foi verificado em alguns casos particulares. Mas a questão permanece em aberto.

Da mesma forma que no artigo anterior, aqui é usada a representação de identidades polinomiais por elementos do anel de grupo FS_n , que se apóia na teoria de representações. Conseguem assim uma forma conveniente de representação computacional para um polinômio, em termos de soma direta de matrizes. São apresentadas cinco identidades de grau 7, que são chamadas de não-óbvias. Mais especificamente, eles assinalam tratar-se de identidades satisfeitas pela associador, uma vez que o produto nestas álgebras é dado pelo associador. Antes de apresentar estas cinco identidades, vamos esclarecer alguns pontos quanto à notação utilizada pelos autores.

Para o associador, utilizam a notação (abc) ao invés de (a,b,c), destacando o seu papel de produto nesta álgebra. Em um polinômio multilinear homogêneo I em que uma letra, digamos x, ocorre pelo menos duas vezes, é definida a soma alternada sobre as posições de x, denotada por $\sum_{alt(x)} I$. De forma sucinta, este operador toma a soma alternada sobre k! permutações sobre uma lista de k letras (que não ocorrem em I), onde k indica o número de ocorrências da letra x em cada termo de I. Tal processo é chamado de linearização parcial alternada. Na verdade, x faz o papel de

indeterminada, e os autores alertam para não se confundir entre (axx), que é zero em uma álgebra alternativa, e $\sum_{alt(x)} (axx)$, onde o x deve ser substituído por outras letras, digamos b e c, para se fazer a expansão em somas alternadas antes de se calcular o produto ternário. As cinco identidades de grau 7 satisfeitas pelo associador em uma álgebra de Cayley são as seguintes:

$$C_{1} = \sum_{alt(x)} \{ (((abx)(axx)b) - ((abx)(bxx)z) + 2((abx)(abx)x) + 2(((abx)ax)bx) - 2(((abx)bx)ax) - (((axx)bx)ab) + (((bxx)ax)ab) - 2(((abx)xx)ab) + 3(((abx)ab)xx) + (((xxx)ab)ab) + 4(((axx)ab)bx) - 4(((bxx)ab)ax)\};$$

$$C_{2} = \sum_{alt(x)} \{ 6((axx)(xxx)a) - 2(((axx)ax)xx) + 2(((xxx)ax)ax) - 5(((axx)xx(ax));$$

$$C_{3} = \sum_{alt(x)} \{ (((axx)xx)ax) + 2(((xxx)ax)ax) + 4(((axx)ax)xx));$$

$$C_{4} = \sum_{alt(x)} ((xxx)(xxx)x);$$

$$C_{5} = \sum_{alt(x)} (((xxx)xx)xx).$$

Ao encerrarmos este trabalho, chamamos a atenção para alguns aspectos da pesquisa de identidades em álgebras alternativas que nos pareceram relevantes. Em primeiro lugar, o caráter nada elementar das expressões obtidas, que apresentam uma complexidade crescente a cada aumento de grau. Daí o seu tratamento exigir a utilização de diversos recursos como, triplo produto de Jordan, derivação, linearização, bases do ideal associador, grupos de permutação, etc. Vemos então que a abrangência do tema, por si só, já representa uma motivação para o seu estudo.

Salientamos também a utilização de técnicas computacionais na avaliação das identidades, o que se faz necessário devido ao grande número de operações envolvido. Este fato ressalta a importância do computador como ferramenta auxiliar neste tipo de pesquisa matemática.

Por fim, deixamos como sugestão para futuras pesquisas, a investigação de novas identidades, uma vez que algumas questões permanecem em aberto, e ainda, os novos resultados poderão trazer significativas contribuições para a Matemática.

Bibliografia

- [1] Albert, A.A. Structures of Algebras. American Math Soc., New York, 1939.
- [2] Bremner, M. and Hentzel, I.R. Identities for the associator in alternative algebras. J. Symbolic Computation, 33:255–273, 2002.
- [3] Bruck, R.H. and Kleinfeld, E. The structure of alternative division rings. *Proc. American Math.*, (2):878–890, 1951.
- [4] Drenski, V.S. A minimal basis of identities for a second-order matrix algebra over a field of characteristic 0. *Algebra i Logika*, 20:188–194, 1982.
- [5] FARENICK, D.R. Algebras of Linear Transformation. Springer-Verlag, New York, 2001.
- [6] Guzzo, Jr. H. O Teorema de Frobenius para álgebras não associativas. IME-USP, 1985. Dissertação de mestrado.
- [7] Guzzo, Jr. H. The bar-radical of baric algebras. *Arch. Math.*, 67(2):106–118, 1996.
- [8] Guzzo, Jr. H. and Couto, M.A. The radical in alternative baric algebras. *Arch. Math. (Basel)*, 75(3):178–187, 2000.
- [9] HENTZEL, I.R. Processing identities by group representation. In *Computers in Non-associative Rings and Algebras*, pages 13–40. R.E. Beck and B. Kolmann, eds., Academic Press, New York, 1977.
- [10] Hentzel, I.R and Peresi, L.A. Identities of Cayley-Dickson algebras. J. Algebra, 188:292–309, 1997.

BIBLIOGRAFIA 151

[11] Herstein, I.N. *Noncommutative Rings*. The Mathematical Association of America, USA, 1973.

- [12] HERSTEIN, I.N. Rings with Involution. University of Chicago Press, Chicago, 1976.
- [13] JACOBSON, N. Basic Algebra I. Van Nostrand, New York, 1974.
- [14] KURAMOCHI, C. C. Identidades Polinomiais para as Álgebras de Matrizes, Álgebras de Jordan de grau 2 e Álgebras de Cayley-Dickson. IME-USP, 1994. Dissertação de mestrado.
- [15] KUZMIN, E.N. and SHESTAKOV, I.P. Non-associative structure. In Algebra VI. Encyclopedia of Mathematical Sciences, volume 57. Kostrikin, A.I. Shafarevich, I.R. eds., Springer-Verlag, New York, 1995.
- [16] MILIES, C.P. Breve história da Álgebra abstrata. II Bienal da SBM, UFBA, 2004.
- [17] PROCESI, C. Polynomial Identities in Algebras. Marcel Dekker, New York, 1973.
- [18] RACINE, M.L. Minimal identities of Jordan algebras of degree 2. Communications in Algebra, 13:2493–2506, 1985.
- [19] RACINE, M.L. Minimal identities of octonion algebras. *Journal of Algebra*, 115:251–260, 1988.
- [20] ROSSET, S. A new proof of the Amitsur-Levitzki identity. *Israel Journal of Mathematics*, 23(2):187–188, 1976.
- [21] ROWEN, L.H. *Polynomial Identities in Ring Theory*. Academic Press, New York, 1980.
- [22] Schafer, R.D. An Introduction to Nonassociative Algebras. Dover Publications, New York, 1995.
- [23] Shephard, G.C. Vector Spaces of Finite Dimension. John Wiley & Sons, New York, 1966.

BIBLIOGRAFIA 152

[24] WÖRZ-BUSEKROS, A. Algebras in Genetics, volume 36 of Lecture Notes in Biomathematics. Springer-Verlag, Berlin/New York, 1980.

[25] Zhevlakov, K.A., Slin'ko, A.M., Shestakov, I.P., and Shirshov, A.I. Rings that are nearly associative. Academic Press, New York, 1982.