UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG
INSTITUTO DE CIÊNCIAS EXATAS - ICEX
DEPARTAMENTO DE MATEMÁTICA

# IDENTIDADES EM VARIÁVEIS SIMÉTRICAS PARA $M_{2^m}(\mathbb{C})$ COM INVOLUÇÃO SIMPLÉTICA

DAFNE CAMPOS LIMA BESSADES
ORIENTADORA: PROF(a). ANA CRISTINA VIEIRA

BELO HORIZONTE - MG
2017

UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG
INSTITUTO DE CIÊNCIAS EXATAS - ICEX
DEPARTAMENTO DE MATEMÁTICA

# IDENTIDADES EM VARIÁVEIS SIMÉTRICAS PARA $M_{2^m}(\mathbb{C})$ COM INVOLUÇÃO SIMPLÉTICA

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Matemática, como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

DAFNE CAMPOS LIMA BESSADES
ORIENTADORA: PROF(a). ANA CRISTINA VIEIRA

BELO HORIZONTE - MG
2017

*"But at night, when all the world's asleep*

*The questions run so deep for such a simple man"*

The Logical Song, Roger Hodgson and Richard Davies.

# Agradecimentos

Gostaria de salientar que o mestrado foi um período muito importante e especial em minha vida. Tenho certeza que tudo de bom que aprendi e vivenciei foi somente possível e concretizado devido a muito esforço e apoio das pessoas que serão citadas a seguir, as quais eu agradeço imensamente.

Aos meus pais Marco Antônio e Rosângela Campos por toda confiança, paciência, amor e carinho em mim depositados ao longo de toda a minha vida.

Aos meus avôs Manuel e Brandão (in memorian) por terem sido tão adoráveis e inspiradores, às minhas avós Rita e Ruth por serem essas mulheres fortes e maravilhosas, e por tudo o que me ensinaram até hoje.

À minha irmã Débora e ao meu cunhado Matheus por toda cumplicidade e alegria que sempre me proporcionam nas horas mais difíceis. Eu os amo muito!

Gostaria de agradecer a toda a minha família: tios, tias e primos, vocês são um sopro de amor e felicidade em minha vida.

Ao meu amado amigo e namorado Edno Alan, pelo incentivo, carinho e amizade durante todos os momentos felizes e difíceis da nossa jornada acadêmica.

Aos meus queridos amigos do departamento de Matemática da UFMG, em especial, à Malu, Weberson, Ayane, Mirla, Helen, Jéssica e Marcos por todos os momentos de descontração que dividimos durante o mestrado.

À minha orientadora Ana Cristina Vieira pela sua paciência, dedicação e atenção durante este período. Obrigada por me inspirar a estudar matemática e ser a minha referência como profissional.

Ao professor Csaba Schneider por todo tempo dedicado a ensinar-me os primeiros passos em programação no GAP, passos esses que foram muito importantes para o desenvolvimento deste trabalho.

Aos professores da banca: Osnel Broche Cristo e Rafael Bezerra dos Santos, pelos importantes comentários e sugestões.

A todos os professores e funcionários do Departamento de Matemática da UFMG que contribuíram de algum modo para a minha formação. Muito Obrigada!

Ao CNPq pelo apoio financeiro.

# Resumo

Nessa dissertação estamos interessados no estudo das cotas para o grau mínimo de uma identidade polinomial em variáveis simétricas para a $\mathbb{F}$-álgebra $M_{2m}(\mathbb{F})$ com a involução simplética $s$ ($\mathbb{F}$ um corpo de característica 0). Apresentaremos a demonstração do resultado dado em [11], que estabelece para $m > 1$ um inteiro positivo e $\mathbb{F}$ um corpo qualquer, que $(M_{2m}(\mathbb{F}), s)^+$ satisfaz uma identidade multilinear de grau $4m - 3$. Apresentaremos também a construção e a implementação em GAP de uma base para a $\mathbb{F}$-álgebra $M_{2^m}(\mathbb{C})$ que é particularmente interessante por ser composta por elementos invertíveis, que são simétricos ou antissimétricos com relação a involução simplética. Acreditamos que, explorando a fundo as propriedades dessa base podemos à ultilizar para encontrar outras $*$-identidades polinomiais para $M_{2^m}(\mathbb{C})$.

**Palavras chaves:** Álgebra de matrizes, Involução, Identidades, Base, $*$-identidades.

# Abstract

In this work we are interested in the studying lower and upper bounds for the degree of the polynomial identity in symmetric variables for the $\mathbb{F}$-algebra $M_{2m}(\mathbb{F})$ endowed with the symplectic involution $s$ ($\mathbb{F}$ a field of characteristic 0). We will exhibit the proof of result given in [11], wich establishes that $(M_{2m}(\mathbb{F}), s)^+$ satisfies a multilinear identity of degree $4m-3$ for $m>1$ a positive integer and $\mathbb{F}$ a field. We will also present the construction and the GAP implementation of a basis for the $\mathbb{F}$-algebra $M_{2^m}(\mathbb{C})$, wich is particularly interesting since their elements are invertible and each one of them is symmetric or skew with respect to the symplectic involution. We believe that exploring deeply the properties, of this basis we can use it to find new identities for $M_{2^m}(\mathbb{C})$ with involution $s$.
**Keywords:** Matrix algebra, Involution, Identity, basis, $*$-identity.

# Lista de Símbolos

- $U(A)$: Grupo das unidades (elementos invertíveis) da $\mathbb{F}$-álgebra A.
- $C_n$: Grupo cíclico de ordem $n$.
- $x^g$: Conjugado de $x$ por $g$, isto é, $g^{-1}xg$.
- $[x, y]$: Comutador de $x$ e $y$, ou seja, $x^{-1}y^{-1}xy$.
- $G'$: Subgrupo derivado de $G$, ou seja, $[G, G] = \langle [x, y] \mid x, y \in G \rangle$.
- $Cl_G(g)$: Classe de conjugação de um elemento $g$ do grupo $G$, ou seja, $\{g^x | \ x \in G\}$.
- $C_G(H)$: Centralizador do subgrupo $H$ em $G$, ou seja, $\{g \in G | \ gh = hg \ \forall \ h \in H\}$.
- $\times$: Produto direto.
- $\rtimes$: Produto semi-direto.
- $\otimes$: Produto tensorial.
- $\oplus$: Soma direta de álgebras.
- $\dot{+}$: Soma direta de módulos.
- $I \triangleleft R$: $I$ é um ideal de $R$.
- $S_n$: Grupo simétrico de grau $n$, ou seja, grupo de permutação do conjunto $\{1, \ldots, n\}$.
- $Char(\mathbb{F})$: Característica do corpo $\mathbb{F}$.
- $sgn(\sigma)$: Sinal da permutação $\sigma$.

# Sumário

# Introdução

As $\mathbb{F}$-álgebras são objetos de grande importância na Teoria de Anéis. Dentre elas, está a importante classe das $\mathbb{F}$-álgebras com identidades polinomiais, ou seja, as $\mathbb{F}$-álgebras que satisfazem polinômios não nulos em variáveis não comutativas, também denominadas PI-álgebras. Essa classe de álgebras foi considerada inicialmente por M. Dehn no artigo [5], em 1922, motivado por problemas de Geometria Projetiva.

Em meados de 1937, no artigo [25], W. Wagner demonstrou que o polinômio

$$f(x_1, x_2, x_3) = (x_1x_2 - x_2x_1)^2x_3 - x_3(x_1x_2 - x_2x_1)^2$$

é uma identidade polinomial para a álgebra de matrizes $M_2(\mathbb{F})$ ($\mathbb{F}$ denotando um corpo). Em 1950, Amitsur e Levitzki, no artigo [3], demonstraram que o polinômio standard de grau $2n$ é uma identidade polinomial de grau mínimo para a álgebra de matrizes $M_n(\mathbb{F})$. A partir daí um dos principais objetivos da PI-teoria se tornou a descrição das identidades polinomiais satisfeitas por determinadas $\mathbb{F}$-álgebras.

Nos últimos 50 anos, várias generalizações do conceito de identidades polinomiais vêm sendo estudadas. Em 1969, Amitsur demonstrou em [2] que uma $\mathbb{F}$-álgebra satisfazendo uma identidade com involução é uma PI-álgebra, impulsionando assim o estudo dessas identidades, também chamadas de $*$-identidades polinomiais. Nesse contexto, iremos abordar nesta dissertação um importante problema na descrição de $*$-identidades polinomiais de $(M_{2m}(\mathbb{F}), s)$: o problema de se determinar o grau mínimo da identidade polinomial em variáveis simétricas da álgebra de matrizes com a involução simplética $s$. Esse problema já foi resolvido, para os casos em que $m = 1, 2$ através dos resultados de D'Amour e Racine, feitos em [6]. Para $m = 3$ o mesmo foi resolvido por Racine e Rashkova nos artigos [17, 18], respectivamente. Entretanto, quando $m > 3$, esse problema permanece em aberto sendo apenas conhecidas a cota inferior e a cota superior para o grau deste tipo de identidade. A cota inferior dada por $2m+2$ foi estabelecida em [8], por Drensky e Giambruno. Já a cota superior, que será estudada de forma detalhada nessa dissertação, é dada por $4m - 3$ e foi obtida por J.D Hill, em [11].

Quando $\mathbb{F}$ é um corpo de característica zero o estudo das identidades polinomiais ($*$-

identidades) satisfeitas por uma $\mathbb{F}$-álgebra pode ser reduzido ao estudo dos polinômios multilineares (ou $*$-polinômios multilineares), o que é bastante vantajoso principalmente pelo fato de que para verificar se um polinômio multilinear é ou não uma identidade de uma $F$-álgebra de dimensão finita, basta aplicá-lo nos elementos de uma base dessa álgebra. Desse modo, a fim de se encontrar $*$-identidades polinomiais para $\mathbb{F}$-álgebras de dimensão finita, se torna interessante procurar bases para essas $\mathbb{F}$-álgebras com boas características. Nessa dissertação vamos expor a construção de uma base, feita em [14], para $(M_{2^m}(\mathbb{C}), s)$ que tem a surpreendente propriedade de que todos os seus elementos são invertíveis e são simétricos ou antissimétricos com relação a involução simplética. Mais ainda, os elementos dessa base que são simétricos formam uma base para $(M_{2^m}(\mathbb{C}), s)^+$ e os elementos que são antissimétricos formam uma base para $(M_{2^m}(\mathbb{C}), s)^-$.

No primeiro capítulo, definiremos alguns conceitos básicos e estabeleceremos resultados importantes dentro da teoria de $R$-módulos e $\mathbb{F}$-álgebras. Veremos que a álgebra de grupo de um grupo finito sobre um corpo de característica zero é semissimples e que suas componentes podem ser vistas como anéis de matrizes sobre anéis de divisão. Nesse sentido, iremos estudar a classificação dos chamados grupos extra-especiais com o intuito de decompor a álgebra de grupo de um 2-grupo extra-especial sobre os números complexos. Isso será importante para a construção da base supracitada.

No segundo capítulo, iremos definir PI-álgebras e expor o processo de multilinearização com o intuito de demonstrar que o ideal de identidades polinomiais de uma PI-álgebra $A$ sobre um corpo de característica zero é gerado por identidades multilineares de A. Ainda nesse capítulo, serão estudadas as identidades de traço, estáveis e alternadas que serão importantes para a compreensão do resultado de Hill. Ao final do capítulo, demonstraremos que para uma $\mathbb{F}$-álgebra $A$, com $\dim_{\mathbb{F}} A = n < \infty$, o polinômio

$$St_{n+1}(x_1, \ldots, x_{n+1}) = \sum_{\sigma \in S_{n+1}} sgn(\sigma)\ x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n+1)}$$

é uma identidade polinomial para $A$, com o intuito de concluir que os polinômios $St_m(x_1, \ldots, x_m)$, com $m \geq n^2 + 1$, são identidades polinomiais para $M_n(\mathbb{F})$.

No terceiro capítulo, vamos definir e dar exemplos de álgebras com involução, entre eles iremos apresentar a álgebra de matrizes com involução simplética, cujo o estudo das suas $*$-identidades (que serão definidas neste mesmo capítulo) de grau mínimo é o principal objeto de estudo dessa dissertação. Além disso, ao longo do capítulo serão caracterizadas as involuções da álgebra de matrizes $n \times n$ sobre um corpo $\mathbb{F}$ de característica zero. Por fim, demonstraremos para o caso em que $\mathbb{F}$ é um corpo algebricamente fechado que o $T^*$-ideal de $(M_n(\mathbb{F}), *)$ é tal que $Id(M_n(\mathbb{F}), *) = Id(M_n(\mathbb{F}), t)$ ou $Id(M_n(\mathbb{F}), *) = Id(M_n(\mathbb{F}), s)$, onde $t$ é a involução transposta e $s$ a involução simplética.

No quarto capítulo, baseando-se no artigo [11], iremos detalhar a demonstração do resultado que constrói para um inteiro $m > 1$ e $\mathbb{F}$ um corpo qualquer, uma identidade multilinear de grau $4m - 3$ para $(M_{2m}(\mathbb{F}), s)^+$, esse resultado estabelece uma cota superior para o grau minimo de uma identidade polinomial em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$. Iremos ainda expor a construção e a implementação da base, feita em [14], no software livre GAP [23], que tem propriedades interessantes de serem estudadas no contexto da involução simplética de $M_{2^m}(\mathbb{C})$.

# Capítulo 1

# Conceitos básicos

Nesse capítulo estamos interessados em definir alguns conceitos básicos. Além disso, ao longo do mesmo, teremos como objetivo principal a compreensão da decomposição da álgebra de grupo de um 2-grupo extra especial. Atentamos ainda para o fato de que nas duas primeiras seções desse capítulo não iremos fazer nenhuma restrição sobre o corpo $\mathbb{F}$ com o qual estaremos trabalhando, porém em um certo ponto da terceira seção será exigido que $\mathbb{F} = \mathbb{C}$, isto é, iremos trabalhar sobre o corpo dos números complexos.

## 1.1 $R$-Módulos e $\mathbb{F}$-álgebras

Nessa seção iremos elucidar alguns conceitos relativos a estrutura de $R$-módulos e $\mathbb{F}$-álgebras com a finalidade de garantir que a álgebra de grupo de um grupo finito sobre um corpo de característica zero é uma álgebra semissimples, cujas componentes simples podem ser vistas como álgebras de matrizes sobre anéis de divisão.

**Definição 1.1.** *Seja $R$ um anel. Um grupo abeliano $M$ (aditivo) é chamado um $R$-módulo à esquerda sobre $R$ se, para cada elemento $r \in R$ e $m \in M$, temos definido um produto $rm \in M$ tal que:*

*(i)* $(r+s)m = rm + sm$,

*(ii)* $(rs)m = r(sm)$,

*(iii)* $r(m_1 + m_2) = rm_1 + rm_2$,

*(iv)* $1.m = m$, *se $R$ possui unidade.*

*para todo $r, s \in R$ e $m, m_1, m_2 \in M$.*

Podemos definir analogamente um $R$-módulo à direita. Neste trabalho utilizaremos o termo $R$-módulo como uma abreviação para $R$-módulo à esquerda. Claramente, um anel

$R$ é um módulo sobre si mesmo, além disso, se $I$ é um ideal à esquerda de um anel $R$ então $I$ é também um $R$-módulo. Notemos ainda que, se $R = \mathbb{F}$ é um corpo, o conceito de $\mathbb{F}$-módulo coincide com a noção de espaço vetorial sobre $\mathbb{F}$. Assim, o espaço $\mathbb{F}^n$, dos vetores coluna com suas $n$ coordenadas em $\mathbb{F}$ e o espaço $M_n(\mathbb{F})$, das matrizes $n \times n$ com entradas em $\mathbb{F}$, com as operações usuais, são exemplos de $\mathbb{F}$-módulos.

**Exemplo 1.2.** *Dado qualquer automorfismo $\sigma$ de $M_n(\mathbb{F})$, o grupo abeliano $\mathbb{F}^n$ pode ser visto como um $M_n(\mathbb{F})$-módulo, com o produto definido por*

$$M_n(\mathbb{F}) \times \mathbb{F}^n \longrightarrow \mathbb{F}^n$$
$$(X, v) \longmapsto \sigma(X).v$$

*onde $\cdot$ denota a multiplicação usual de matrizes. Nesse caso, dizemos que $\mathbb{F}^n$ é um $M_n(\mathbb{F})$-módulo com o produto induzido por $\sigma$.*

**Definição 1.3.** *Sejam $R$ um anel e $M$ um $R$-módulo. Um subconjunto não vazio $N \subseteq M$ é chamado um $R$-submódulo de $M$ se as seguintes propriedades são satisfeitas:*

*(i)* $n_1 + n_2 \in N$,

*(ii)* $rn \in N$,

*para todos $n_1, n_2, n \in N$ e $r \in R$.*

Se $V$ é um espaço vetorial sobre um corpo $\mathbb{F}$, então os $\mathbb{F}$-submódulos de $V$ são precisamente seus subespaços vetoriais. Em geral, todo módulo não nulo $M$ contém pelos menos dois submódulos, $M$ e $\{0\}$, os quais são chamados triviais.

**Definição 1.4.** *Seja $R$ um anel unitário. Um $R$-módulo $M$ é chamado simples se $M \neq \{0\}$ e seus únicos $R$-submódulos são os triviais.*

Observe que $\mathbb{F}^n$ não é um $\mathbb{F}$-módulo simples, já que todo subespaço de $\mathbb{F}^n$ é um $\mathbb{F}$-submódulo. No entanto, veremos no próximo exemplo que $\mathbb{F}^n$, com o produto induzido por qualquer automorfismo $\sigma$ de $M_n(\mathbb{F})$, é um $M_n(\mathbb{F})$-módulo simples.

**Exemplo 1.5.** *Sejam $\mathbb{F}$ um corpo e $\sigma$ um automorfismo de $M_n(\mathbb{F})$. O módulo $\mathbb{F}^n$ com o produto induzido por $\sigma$ é um $M_n(\mathbb{F})$-módulo simples.*

*De fato, sendo $N \neq \{0\}$ um $M_n(\mathbb{F})$-submódulo de $\mathbb{F}^n$. Então $N$ contém um elemento $v$ não nulo. Assim, tomando $\alpha \in \mathbb{F}$ e considerando $v_i$ uma coordenada não-nula de $v$, por $\sigma$ ser um automorfismo de $M_n(\mathbb{F})$ temos que, para cada $j \in \{1, \ldots, n\}$, existe uma matriz $A_j$ tal que*

$$\sigma(A_j) = \frac{\alpha}{v_i} e_{ji},$$

*onde $e_{ji}$ denota a matriz elementar com 1 na (j,i)-entrada e 0 nas demais entradas.*

*Desse modo,*

$$\begin{aligned} A_j v &= \sigma(A_j)v \\ &= \frac{\alpha}{v_i} e_{ji} v \\ &= \frac{\alpha}{v_i} v_i e_j \\ &= \alpha e_j. \end{aligned}$$

*Agora, pelo fato de $\alpha$ ter sido escolhido arbitrariamente e $N$ ser um $M_n(\mathbb{F})$-submódulo, segue que $\alpha e_j \in N$, para todo $\alpha \in \mathbb{F}$ e $j \in \{1, \ldots, n\}$. Logo $N = \mathbb{F}^n$.*

**Exemplo 1.6.** *Sejam $\mathbb{F}$ um corpo e $j \in \{1, \cdots, n\}$. O ideal (à esquerda) de matrizes colunas*

$$L_j = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1j} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nj} & 0 & \cdots & 0 \end{pmatrix} ; a_{ij} \in \mathbb{F}, \forall\, i \in \{1, \ldots, n\} \right\}$$

*é um $M_n(\mathbb{F})$-módulo simples com a operação usual.*

*De fato, suponha que $J \subseteq L_j$ é um $M_n(\mathbb{F})$-submódulo não-nulo, então existe*

$$a = b_{1j}e_{1j} + b_{2j}e_{2j} + \ldots b_{nj}e_{nj} \in J,$$

*com algum $b_{ij} \neq 0$.*

*Observe que, $e_{1i}a = b_{ij}e_{1j}$, $e_{2i}a = b_{ij}e_{2j}$, $\ldots$, $e_{ni}a = b_{ij}e_{nj}$, portanto $b_{ij}e_{kj} \in J$, $\forall\ k \in \{1, \ldots, n\}$.*

*Desse modo,*

$$\left(\frac{1}{b_{ij}} e_{kk}\right)\left(b_{ij}e_{kj}\right) = e_{kj} \in J \quad \forall\ k \in \{1, \ldots, n\}$$

*logo,*

$$(a_{kj}e_{kk})\,(e_{kj}) = a_{kj}e_{kj} \in J \quad \forall\ k \in \{1, \ldots, n\}.$$

*Portanto, $L_j \subseteq J$ e, consequentemente, $L_j$ é simples.*

**Definição 1.7.** *Sejam $M$ e $N$ dois módulos sobre um anel $R$. Uma aplicação $f : M \to N$ é um homomorfismo de $R$-módulos, se $f$ é um homomorfismo de grupos aditivos e*

$$f(rm) = rf(m),$$

*para todo $r \in R$ e $m \in M$. No caso em que $f$ for também uma bijeção dizemos que $f$ é um isomorfismo e que $M$ e $N$ são $R$-módulos isomorfos.*

**Exemplo 1.8.** *Sejam $L_i$ e $L_j$ dois ideais de matrizes colunas com $i, j \in \{1, \cdots, n\}$ e $\mathbb{F}$ um corpo. A aplicação $f : L_i \to L_j$ definida por:*

$$\begin{array}{ccc} \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix} & \mapsto & \begin{pmatrix} 0 & \cdots & 0 & a_{1j} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nj} & 0 & \cdots & 0 \end{pmatrix} \\ \hookrightarrow i\text{-ésima coluna} & & \hookrightarrow j\text{-ésima coluna} \end{array}$$

*é claramente um isomorfismo de $M_n(\mathbb{F})$-módulos.*

Podemos ver então que $L_i$ e $L_j$ são $M_n(\mathbb{F})$-módulos simples e isomorfos para todo $i, j \in \{1, \cdots, n\}$. Em geral temos o seguinte resultado.

**Proposição 1.9.** *Se $\mathbb{F}$ é um corpo, então todos os $M_n(\mathbb{F})$-módulos simples são isomorfos.*

**Demonstração.** Seja $N$ um $R$-módulo simples, onde $R = M_n(\mathbb{F})$. Do que foi comentado acima, basta provar que existe $i \in \{1, \cdots, n\}$ tal que $N$ é isomorfo ao ideal de matrizes colunas $L_i$. Desde que $N = 1N \subseteq RN \subseteq N$, temos pela simplicidade de N, $RN = N$. Como $R = \sum_{i=1}^{n} L_i$ e $N \neq \{0\}$, existe $i \in \{1, \cdots, n\}$ tal que $L_i N \neq 0$. Portanto, existe $n \in N$ tal que $\widetilde{l_i} n \neq 0$ para algum $\widetilde{l_i} \in L_i$. Consideremos, então, a aplicação

$$\begin{array}{rcccl} f & : & L_i & \to & N \\ & & l_i & \mapsto & l_i n. \end{array}$$

Claramente, $f$ é um homomorfismo de grupos aditivos com conjunto imagem $f(L_i) \neq \{0\}$ e satisfaz $f(rl_i) = rf(l_i)$, para todo $r \in R$ e $l_i \in L_i$. Como $f(L_i)$ é um $R$-submódulo de $N$ e $N$ é um $R$-módulo simples, então $f(L_i) = N$. Por outro lado, como o núcleo $\mathrm{Ker}(f)$ é um $R$-submódulo de $L_i$ tal que $\mathrm{Ker}(f) \neq L_i$ e $L_i$ é um $R$-módulo simples, então $\mathrm{Ker}(f) = \{0\}$. Portanto, $f$ é um isomorfismo de $R$-módulos.

■

**Definição 1.10.** *Seja $A$ um espaço vetorial sobre um corpo $\mathbb{F}$. Dizemos que $A$ é uma $\mathbb{F}$-álgebra associativa, se $A$ for um anel associativo tal que*

$$\alpha(ab) = (\alpha a)b = a(\alpha b) \quad \forall\, a, b \in A \text{ e } \alpha \in \mathbb{F}.$$

Dizemos que $A$ é uma $\mathbb{F}$-álgebra comutativa, quando $A$ for um anel comutativo. No caso em que $A$ for um anel com unidade, dizemos que $A$ é uma $\mathbb{F}$-álgebra com unidade, e nesse caso pode-se observar o subanel $\mathbb{F}.1_A$ (que é isomorfo a $\mathbb{F}$) está contido no centro de $A$.

Definiremos a dimensão de uma $\mathbb{F}$-álgebra $A$ como sendo a dimensão de $A$ como espaço vetorial sobre $\mathbb{F}$. Desse modo, dizemos que $A$ é uma $\mathbb{F}$-álgebra de dimensão finita se $A$ for um espaço vetorial sobre $\mathbb{F}$ de dimensão finita.

Por fim, uma $\mathbb{F}$-álgebra $A$ é gerada como álgebra por um subconjunto $S$, se todo elemento de $A$ pode ser escrito como combinação linear de produtos da forma $s_{i_1}s_{i_2}\ldots s_{i_k}$ onde $s_{ij} \in S$. Nesse caso, escrevemos $A = \langle S \rangle$.

A seguir vamos dar alguns exemplos de álgebras associativas. Entre elas, iremos definir as álgebras de grupos e as álgebras livres associativas unitárias, que são álgebras de extrema importância para o desenvolvimento dessa dissertação.

**Exemplo 1.11.** *A álgebra das matrizes $n \times n$ com entradas em $\mathbb{F}$, denotada por $M_n(\mathbb{F})$, é unitária e não comutativa para todo $n \geq 2$. Além disso, $M_n(\mathbb{F})$ é uma álgebra de dimensão finita com dimensão igual a $n^2$.*

**Exemplo 1.12.** *Seja $\mathbb{F}$ um corpo, $G$ um grupo finito e $g_1, g_2, \ldots, g_n$ seus elementos. O conjunto de todas as somas formais*

$$\sum_{i=1}^{n} \lambda_i g_i \quad \text{com } \lambda_i \in \mathbb{F},$$

*munido com as operações de adição e multiplicação por escalar, definidas por*

$$u + v = \sum_{i=1}^{n} (\lambda_i + \alpha_i) g_i \quad e \quad \lambda u = \sum_{i=1}^{n} \lambda \lambda_i g_i,$$

*onde $u = \sum_{i=1}^{n} \lambda_i g_i$ e $v = \sum_{i=1}^{n} \alpha_i g_i$.*

*É um espaço vetorial sobre $\mathbb{F}$ de dimensão $n$, denotado por $\mathbb{F}G$. Os elementos $g_1, g_2, \ldots, g_n$ formam uma base para $\mathbb{F}G$, chamada de base natural.*

*Agora, munindo o espaço $\mathbb{F}G$ com a multiplicação, definida por*

$$\left( \sum_{g \in G} \lambda_g g \right) \cdot \left( \sum_{h \in G} \mu_h h \right) = \left( \sum_{g,h \in G} \lambda_g \mu_h (gh) \right), \qquad \text{com } \lambda_g, \mu_h \in \mathbb{C}$$

*pode-se observar que obtemos uma $\mathbb{F}$-álgebra, denominada a álgebra de grupo de $G$ sobre $\mathbb{F}$.*

**Exemplo 1.13.** *Seja $X = \{x_1, x_2, \ldots\}$ um conjunto enumerável de elementos não comutativos. Uma palavra em $X$ é definida como sendo uma sequência de variáveis $x_{i_1}x_{i_2}\ldots x_{i_n}$, onde $x_{i_j} \in X$ e $n \in \mathbb{N}$. No caso em que $n = 0$ temos uma palavra, denominada vazia e denotada por $1$.*

*Seja* $\mathbb{F}\langle X\rangle$ *o espaço vetorial tendo como base todas as palavras de* $X$*, incluindo a palavra* $1$*. O produto de um escalar de* $\mathbb{F}$ *com uma palavra será denominado um monômio e os elementos de* $\mathbb{F}\Big\langle X\Big\rangle$ *serão chamados polinômios, além disso, se* $f \in \mathbb{F}\Big\langle X\Big\rangle$ *escrevemos* $f = f(x_1, x_2, \ldots, x_n)$ *para indicar que* $x_1, x_2, \ldots, x_n$ *são as únicas variáveis que aparecem em* $f$*.*

*Por fim, definimos o produto de dois monômios* $\alpha x_{i_1}x_{i_2}\ldots x_{i_n}$ *e* $\beta x_{j_1}x_{j_2},\ldots,x_{j_n}$ *em* $\mathbb{F}\Big\langle X\Big\rangle$ *por justaposição, isto é,*

$$(\alpha x_{i_1}x_{i_2}\ldots x_{i_n}).(\beta x_{j_1}x_{j_2}\ldots x_{j_m}) = \alpha\beta x_{i_1}x_{i_2}\ldots x_{i_n}x_{j_1}x_{j_2}\ldots x_{j_m}.$$

*Com esse produto definido em* $\mathbb{F}\Big\langle X\Big\rangle$ *obtemos a álgebra unitária associativa livre gerada por* $X$*.*

**Definição 1.14.** *Dizemos que um subespaço vetorial* $B$ *de* $A$ *é uma subálgebra de* $A$ *se* $B$ *for um subanel de* $A$*.*

Por exemplo, a $\mathbb{F}$-álgebra das matrizes triangulares superiores $UT_n(\mathbb{F})$ é uma subálgebra da álgebra de matrizes $M_n(\mathbb{F})$.

**Definição 1.15.** *Uma aplicação linear* $\phi : A_1 \longrightarrow A_2$ *entre duas* $\mathbb{F}$*-álgebras* $A_1$ *e* $A_2$ *é um homomorfismo de F-álgebras, se para quaisquer* $a, b \in A_1$ *vale a seguinte propriedade:*

$$\phi(ab) = \phi(a)\phi(b).$$

Dizemos que $\phi$ é um isomorfismo se $\phi$ for um homomorfismo bijetor. Nesse caso, dizemos que $A_1$ e $A_2$ são isomorfas e escrevemos $A_1 \cong A_2$.

Destacamos abaixo alguns fatos importantes sobre homomorfismos de álgebras:

- $\phi$ é injetor se, e somente se, $Ker(\phi) = \{0\}$.
- Seja $\phi : A \longrightarrow B$ um homomorfismo de $\mathbb{F}$-álgebras. É fácil ver que $Ker(\phi)$ é um ideal de $A$ e $Im(\phi)$ é uma $\mathbb{F}$-subálgebra de $B$.
- Pode-se provar que $A/Ker(\phi) \cong Im(\phi)$. Este resultado é conhecido como o Teorema do isomorfismo para álgebras.

**Definição 1.16.** *Sejam* $I_1, I_2, \ldots I_k$ *ideais à esquerda de uma F-álgebra* $A$*. Escrevemos*

$$A = I_1 \oplus I_2 \oplus \cdots \oplus I_k$$

*e dizemos que* $A$ *é a soma direta de* $I_1, I_2, \ldots I_k$*, como* $A$*-módulos, se:*

- $A = I_1 + I_2 + \cdots + I_k$,
- $I_i \bigcap \sum_{\substack{j=1 \\ j \neq i}}^{k} I_j = \{0\}$, *para todo* $i \in \{1, \ldots, k\}$.

**Definição 1.17.** *Sejam* $A_1, A_2, \ldots A_k$ *subálgebras de uma* $F$*-álgebra* $A$*. Escrevemos*

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_k$$

*e dizemos que* $A$ *é a soma direta de* $A_1, A_2, \ldots A_k$*, como álgebra, se:*

- $A = A_1 + A_2 + \cdots + A_k$,
- $A_i \bigcap \sum_{\substack{j=1 \\ j \neq i}}^{k} A_j = \{0\}$, *para todo* $i \in \{1, \ldots, k\}$,
- $A_i A_j = 0$, *para todo* $i, j \in \{1, \ldots, k\}$, *com* $i \neq j$.

**Definição 1.18.** *Seja* $A$ *uma* $\mathbb{F}$*-álgebra, dizemos que*

1. $A$ *é simples, se* $A^2 \neq \{0\}$ *e esta não possui ideais bilaterais.*
2. $A$ *é semissimples, se pode ser escrita como a soma direta (não necessariamente finita) de* $A$*-módulos simples, isto é, ideias à esquerda minimais.*
3. $A$ *é nilpotente, se existe* $n \in \mathbb{N} - \{0\}$ *tal que* $A^n = \{0\}$*. O menor natural positivo* $n$ *com essa propriedade é chamado de índice de nilpotência de* $A$*.*

**Exemplo 1.19.** *Pode-se verificar que a álgebra de matrizes* $n \times n$ *estritamente triangulares superiores, é uma álgebra nilpotente com índice de nilpotência* $n$*.*

*O Teorema de Maschke, enunciado a seguir, estabelece que a álgebra* $\mathbb{F}G$ *discutida no Exemplo 1.12 é uma álgebra semissimples, quando* $\mathbb{F}$ *é um corpo de característica zero.*

**Teorema 1.20.** *(Maschke) Seja* $G$ *um grupo finito e* $\mathbb{F}$ *um corpo. Então a álgebra de grupo* $\mathbb{F}G$ *é semissimples se, e somente se, a característica de* $\mathbb{F}$ *não divide a ordem do grupo* $G$*.*

**Demonstração.**

Ver([16], pg.140).

■

Seja $A$ uma $\mathbb{F}$-álgebra semissimples de dimensão finita. O teorema que enunciaremos a seguir é devido a Joseph Wedderburn e Emil Artin, e nos diz que sob essas condições a

$\mathbb{F}$-álgebra $A$ é isomorfa à uma soma direta, de um número finito, de álgebras de matrizes com coeficientes sobre anéis de divisão, classificando dessa forma todas as $\mathbb{F}$-álgebras semissimples de dimensão finita. Para uma melhor compreensão deste teorema iremos, antes de enunciá-lo, provar o seguinte resultado:

**Proposição 1.21.** *Sejam $n$ um inteiro positivo e $D$ um anel de divisão. Então a álgebra de matrizes $M_n(D)$ é uma álgebra simples.*

**Demonstração.** Seja $I$ um ideal de $M_n(D)$. Vamos mostrar que se $I \neq \{0\}$, então $I = M_n(D)$.

De fato, se $I \neq 0$ então existe $A = (a_{ij}) \in I$ com pelo menos uma entrada $a_{hk}$ de $A$ não-nula. Defina $B_i = e_{ih}Ae_{ki}$, um cálculo direto mostra que as entradas de $B_i$ são todas iguais a 0, exceto a entrada $(i,i)$ que é igual à $a_{hk}$, isto é, $B_i = a_{hk}e_{ii}$.

Sendo $I \triangleleft M_n(D)$, temos pela definição de $B_i$ que $B = B_1 + B_2 + \ldots B_n \in I$ e, pelo o que foi observado acima, $B$ é uma matriz diagonal com todas as suas entradas na diagonal iguais à $a_{hk} \neq 0$. Portanto, $B \in I$ é invertível e, consequentemente, $I = M_n(D)$.

∎

**Teorema 1.22.** *(Teorema de Wedderburn-Artin). Seja $A$ uma $\mathbb{F}$-álgebra semissimples de dimensão finita. Então, $A$ é isomorfa a uma soma direta, de um número finito, de álgebras de matrizes com coeficientes sobre anéis de divisão, ou seja:*

$$A \cong \oplus_{i=1}^{k} M_{n_i}(D_i)$$

*onde cada $D_i$ é um anel de divisão.*

*Em particular, se $\mathbb{F}$ é um corpo algebricamente fechado, pode-se mostrar que $D_i \cong \mathbb{F}$, para todo $i \in \{1, \ldots k\}$, além disso,*

$$A \cong \oplus_{i=1}^{k} M_{n_i}(\mathbb{F}).$$

## 1.2 Grupos extra-especiais

Nessa seção iremos definir e expor a classificação dos grupos extra-especiais.

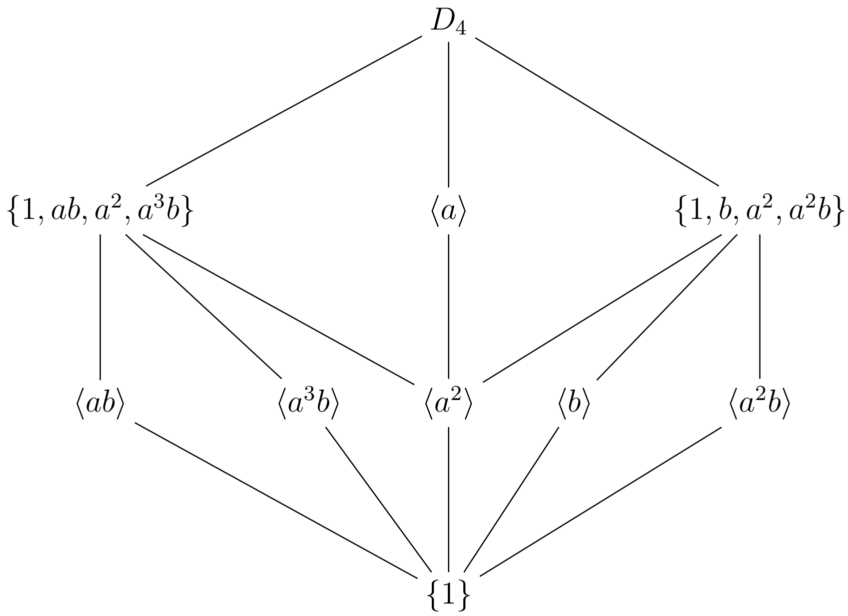
**Definição 1.23.** *Um $p$-grupo finito não abeliano $G$ é dito extra-especial se satisfaz:*

1. $Z(G) = G'$

2. $|Z(G)| = p$.

**Exemplo 1.24.** *O grupo diedral de ordem 8*

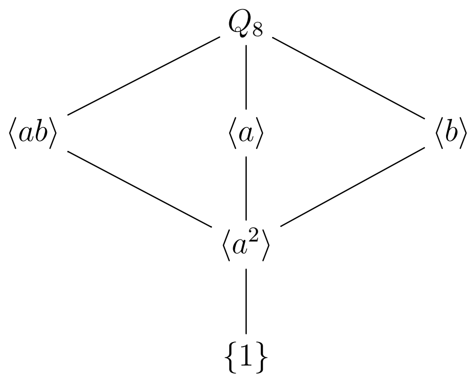
$$D_4 = \left\langle a, b \mid a^4 = b^2 = 1;\ bab^{-1} = a^{-1} \right\rangle$$




*é extra-especial, pois é um 2-grupo não abeliano com* $Z(D_4) = D_4' = \langle a^2 \rangle$ *e* $|Z(D_4)| = 2$.

**Exemplo 1.25.** *O grupo dos quatérnios*

$$Q_8 = \left\langle a, b \mid a^4 = 1;\ a^2 = b^2;\ bab^{-1} = a^{-1} \right\rangle$$




*é também extra-especial, pois é um 2-grupo não abeliano, com* $Z(Q_8) = Q_8' = \langle a^2 \rangle$ *e* $|Z(Q_8)| = 2$.

Observe que tanto $D_4$ quanto $Q_8$ têm ordem $2^3$. Além disso, pelo o que vimos acima, ambos são extra-especiais. Em geral, todo grupo não abeliano de ordem $p^3$ é extra-especial, como veremos na proposição a seguir.

**Proposição 1.26.** *Todo grupo não abeliano de ordem $p^3$ é extra-especial.*

**Demonstração.** Seja $G$ um grupo não abeliano de ordem $p^3$. Sabemos que todo $p$-grupo tem centro não-trivial, portanto as únicas possibilidades para a ordem do centro de $G$ são $|Z(G)| = p^2$ ou $|Z(G)| = p$. Suponhamos por absurdo que $|Z(G)| = p^2$, então pelo teorema de Lagrange, $|G/Z(G)| = p$ e, consequentemente, $G/Z(G)$ é um grupo cíclico, o que é uma contradição, pois nesse caso teríamos como consequência que $G$ é abeliano. Assim, concluímos que $|Z(G)| = p$.

Agora, como $|Z(G)| = p$ obtemos que $|G/Z(G)| = p^2$, logo $G/Z(G)$ é abeliano e $G' \leq Z(G)$. Então, por $G$ ser não abeliano $G' = Z(G)$.

■

Os grupos de ordem $p^3$ serão essenciais para a classificação dos grupos extra-especiais, por esse motivo é essencial conhecermos primeiro esses grupos. Observe que acima já foram estudados todos os grupos extra-especiais de ordem $2^3$, então nos resta caracterizar todos os grupos não-abelianos de ordem $p^3$, para $p$ um primo ímpar.

**Definição 1.27.** *Sejam $G$ e $H$ dois grupos e $\theta : H \longrightarrow Aut(G)$ um homomorfismo de grupos. O produto semi-direto de $G$ por $H$, denotado por $G \rtimes_\theta H$ (ou simplesmente $G \rtimes H$, quando o automorfismo $\theta$ estiver subentendido) é o conjunto*

$$G \times H = \big\{(g, h)|\ g \in G \quad e \quad h \in H\big\},$$

*munido com a operação:*

$$(g_1, h_1).(g_2, h_2) = (g_1.\theta(h_1)(g_2), h_1.h_2).$$

Observe que com a operação definida acima o produto semi-direto de $G$ por $H$ é um grupo e, com exceção ao caso em que $\theta$ for o homomorfismo trivial, esse grupo será não-abeliano.

A partir dessa observação podemos construir, para $p$ um primo ímpar, dois $p$-grupos não-abelianos de ordem $p^3$. Começamos considerando os grupos cíclicos $G = C_{p^2} = \langle x \rangle$, $H = C_p = \langle y \rangle$ e o automorfismo

$$\begin{aligned} \theta : H &\longrightarrow Aut(G) \\ y &\longmapsto \theta(y) : G \longrightarrow G \\ &\qquad\qquad\quad x \longmapsto x^{p+1}. \end{aligned}$$

O grupo $\mathcal{N} = C_{p^2} \rtimes_\theta C_p$ tem ordem $p^3$ e o homomorfismo $\theta$ é não trivial. Portanto $\mathcal{N}$ é um $p$-grupo extra-especial, ao qual podemos dar a seguinte apresentação:

$$\mathcal{N} = \left\langle x, y \middle| \; x^{p^2} = 1; y^p = 1; x^y = x^{p+1} \right\rangle .$$

Considere agora os grupos $G = C_p \times C_p = \langle x \rangle \times \langle z \rangle$ , $H = C_p = \langle y \rangle$ e o automorfismo

$$\begin{aligned} \psi : H &\longrightarrow Aut(G) \\ y &\longmapsto \theta(y) : G \longrightarrow G \\ & \qquad\qquad\quad x \longmapsto zx \\ & \qquad\qquad\quad z \longmapsto z. \end{aligned}$$

O grupo $\mathcal{M} = (C_p \times C_p) \rtimes_\psi C_p$ tem ordem $p^3$ e o homomorfismo $\psi$ é não trivial. Assim, $\mathcal{M}$ também é um $p$-grupo extra-especial, com apresentação:

$$\mathcal{M} = \left\langle x, y, z \middle| \; x^p = y^p = z^p = 1; [x, y] = z; [x, z] = [y, z] = 1 \right\rangle .$$

Veremos a seguir que na verdade os grupos $D_4, Q_8, \mathcal{N}$ e $\mathcal{M}$ são, a menos de isomorfismo, os únicos $p$-grupos não-abelianos de ordem $p^3$.

**Definição 1.28.** *Um $p$-grupo abeliano $G$ é dito abeliano elementar, se todos os seus elementos diferentes da identidade tem ordem igual à $p$.*

**Proposição 1.29.** *Seja $G$ um $p$-grupo extra-especial. Então $G/Z(G)$ é um grupo abeliano elementar.*

**Demonstração.** Queremos mostrar que $G/Z(G)$ é um grupo abeliano elementar, para tanto devemos mostrar que $x^p \in Z(G)$, para todo $x \in G$.

Com efeito, usando a identidade de comutadores $[ab, c] = [a, c]^b[b, c]$, obtemos que $[x^2, y] = x^{-2}y^{-1}x^2y = [x, y]^x[x, y]$. Agora, por $Z(G) = G'$, que $[x^2, y] = [x, y]^2$. Seguindo os mesmos passos, por indução, temos que $[x^n, y] = [x, y]^n$, para todo $n \in \mathbb{N}$.

Então, por $|G'| = |Z(G)| = p$, $[x^p, y] = [x, y]^p = 1$, para todo $x, y \in G$, isto é, $x^p \in Z(G) \; \forall \; x \in G$.

■

**Lema 1.30.** *Seja $G$ um $p$-grupo extra-especial com $Z(G) = \langle z \rangle$ e $z = [x, y]$ para $x, y \in G$. Então, para todo inteiro $k$, temos que*

*(i)* $x^k y = z^k y x^k$.

*(ii)* $(yx)^k = z^{\frac{1}{2}(k-1)k} y^k x^k$.

**Demonstração.**

(i) Sendo $[x,y] = z$, temos que $y^{-1}xy = xz = zx$. Desse modo, para todo inteiro $k$, obtemos $(y^{-1}xy)^k = z^k x^k$ . Consequentemente, $y^{-1}x^k y = z^k x^k$, ou seja, $x^k y = z^k y x^k$.

(ii) A demonstração do resultado será feita por indução.

Observe que, para $k = 1$ a igualdade se verifica. Suponhamos que a igualdade se verifica para $k-1$ e vamos mostrar que se verifica para k. Como

$$\begin{aligned} (yx)^k &= (yx)^{k-1}(yx) \\ &= z^{\frac{1}{2}(k-2)k-1} y^{k-1} x^{k-1} yx \qquad \text{(por hipótese de indução)}, \end{aligned}$$

pelo o que foi provado acima, temos que $(yx)^k = z^{\frac{1}{2}(k-2)(k-1)} y^{k-1} z^{k-1} y x^{k-1} x = z^{\frac{1}{2}(k-1)k} y^k x^k$. Dessa maneira, a igualdade é válida para $k$ e o resultado segue do princípio de indução matemática.

■

**Teorema 1.31.** *Seja $G$ um grupo não-abeliano com $|G| = p^3$. Então*

1. *Se $p = 2$ temos*
$$G \cong D_4 \quad ou \quad G \cong Q_8.$$

2. *Se $p$ é ímpar, temos*
$$G \cong \mathcal{N} \quad ou \quad G \cong \mathcal{M}.$$

**Demonstração.** A demonstração será dividida em dois casos. Classificaremos primeiro os grupos que contém pelo menos um subgrupo cíclico de ordem $p^2$ e depois aqueles em que todo subgrupo cíclico não trivial tem ordem $p$.

**Caso 1.** Suponhamos que existe $x \in G$ tal que $H = \langle x \rangle$ tem ordem $p^2$. Então $H \triangleleft G$ e $G/H$ é cíclico de ordem $p$.

Consideremos inicialmente que $p$ é um primo ímpar e tomemos $u \in G \backslash H$. Pela Proposição 1.26 $G$ é um grupo extra-especial, então $z = [x,u]$ é tal que $z \in Z(G)$. Pela Proposição 1.29, temos que $x^p \in Z(G)$ e $Z(G) = \langle x^p \rangle$. Dessa forma, $x^p = z^i = [x,u]^i = [x,u^i]$, para algum $i \in \mathbb{N}$. Observe ainda que o elemento $u^i \notin H$, caso contrário ele comutaria com $x$ e então $x^p = [x,u]^i = [x,u^i] = 1$, o que é uma contradição. Fazendo $v = u^i$, temos $[x,v] = x^p$ e, consequentemente, $x^v = x^{p+1}$. Como $H$ é um subgrupo maximal de $G$, $x$ é um gerador de $H$ e $v \notin H$ é imediato que $G = \langle x,v \rangle$. Observe que

$v^p \in H$, uma vez que a Proposição 1.29 nos diz que, $v^p \in Z(G) = \langle x^p \rangle \subseteq \langle x \rangle = H$. Entretanto $v^p$ não gera $H$, caso contrário $G$ seria cíclico, o que é um absurdo. Logo, $v^p = x^{pk}$, para algum $k \in \mathbb{N}$.

Consideremos $y = vx^{-k}$. Como $p$ é ímpar e pelo Lema 1.30, temos que $y^p = z^{\frac{1}{2}(p-1)p} v^p x^{-kp} = 1$. Além disso, $x^y = x^{vx^{-k}} = x^v = x^{p+1}$. Dessa forma, concluímos que $G \cong \mathcal{N}$.

Se $p = 2$, então $|G| = 8$ e sendo $G$ um 2-grupo extra-especial, temos $Z(G) = \langle x^2 \rangle$. Consideremos $y \in G \backslash H$. Então $[x, y] = x^2$ e, por conseguinte, $x^y = x^{-1}$. Sendo $G/Z(G)$ um 2-grupo elementar, temos $y^2 \in Z(G)$ e portanto $y^2 = x^{2j}$, para algum $j \in \mathbb{N}$. Se $j$ for par, temos $y^2 = 1$ e desse modo $G \cong D_4$. Se $j$ for ímpar, temos $y^2 = x^2$ e portanto $G \cong Q_8$.

**Caso 2.** Agora vamos Supor que todo subgrupo cíclico de $G$ tem ordem $p$. Então, $x^p = 1 \ \forall \ \ x \in G$ e $p$ é um primo ímpar (caso contrário $G$ seria abeliano). Seja $H$ um subgrupo maximal de $G$. Então $|H| = p^2$, $H \lhd G$ e $H$ é um $p$-grupo abeliano elementar. Assim, $H \cap Z(G) \neq 1$ e portanto $Z(G) \subset H$. Tomando $y \in G \backslash H$, $x \in H \backslash Z(G)$ ($x$ e $y$ distintos) e $z = [x, y] \in G' = Z(G)$. Obtemos, $G = \langle x, y, z \rangle$ ; $x^p = y^p = z^p$; $z = [x, y]$ e $[x, z] = [y, z] = 1$, consequentemente, $G \cong \mathcal{M}$.

Concluímos dessa forma que $D_4, Q_8, \mathcal{N}$ e $\mathcal{M}$ são, a menos de isomorfismo, os únicos $p$-grupos não-abelianos de ordem $p^3$.

■

**Definição 1.32.** *Sejam $G$ um grupo finito e $G_1, G_2, \ldots, G_n$ subgrupos de $G$. Dizemos que $G$ é o produto central dos subgrupos $G_i$, com $1 \leq i \leq n$, e escrevemos $G = G_1 * G_2 * \cdots * G_n$, se*

*(i)* $G = \left\langle G_i \middle| \ 1 \leq i \leq n \right\rangle$, *com* $[G_i, G_j] = 1$ *para* $i \neq j$.

*(ii)* $Z(G) = Z(G_i) \quad \forall \quad 1 \leq i \leq n$.

**Proposição 1.33.** *Sejam $L$ e $H$ $p$-grupos extra-especiais. Então, o produto central*

$$G = L * H$$

*é um grupo extra-especial.*

**Demonstração.** De fato, $Z(G)$ tem ordem $p$, pois $Z(G) = Z(L) = Z(H)$ e como $L$ e $H$ são extra-especiais, segue que $|Z(G)| = |Z(L)| = |Z(H)| = p$. Além disso, como $[L, H] = 1$, então $G = L * H$ tem subgrupo derivado igual ao seu centro. Assim, concluímos que $G = L * H$ é um grupo extra-especial. ■

O teorema anterior nos deu a classificação para $p$-grupos de ordem $p^3$. Iremos a seguir enunciar o teorema que classifica os $p$-grupos extra-especiais de qualquer ordem. Na verdade, veremos que um $p$-grupo extra-especial nada mais é do que o produto central de grupos obtidos a partir dos grupos $D_4, Q_8, \mathcal{N}$ e $\mathcal{M}$.

**Teorema 1.34.** *Um $p$-grupo extra-especial $G$ é o produto central de $r \geq 1$ subgrupos não abelianos de ordem $p^3$. Além disso, se $p$ é ímpar então $G$ é isomorfo a $\mathcal{N}^k\mathcal{M}^{r-k}$, enquanto se $p = 2$, $G$ é isomorfo a $D_4^k Q_8^{r-k}$, para algum $k$, onde os produtos aqui considerados são centrais. Em ambos os casos $|G| = p^{2r+1}$.*

**Demonstração.**

Ver([22], pg 19)

■

Terminamos essa seção ressaltando que para se obter a classificação completa dos grupos extra-especiais, pode-se mostrar que $Q_8^2 \cong D_4^2$, $D_4^{r-1}Q_8 \ncong D_4^r$, $\mathcal{N}\mathcal{M}^{r-1} \ncong \mathcal{M}^r$ e $\mathcal{N}^2 \cong \mathcal{N}\mathcal{M}$. Portanto, quando $G$ é um 2-grupo extra-especial de ordem $2^{2r+1}$, temos que $G \cong D_4^r$ ou $G \cong D_4^{r-1}Q_8$, e quando $G$ é um $p$-grupo extra-especial de ordem $p^{2r+1}$, onde $p$ é um primo ímpar, temos que $G \cong \mathcal{M}^r$ ou $G \cong \mathcal{N}\mathcal{M}^{r-1}$ (Para detalhes dessa demonstração ver [22], pg.19).

## 1.3 A álgebra de um 2-grupo extra-especial.

Nessa seção iremos definir o conceito de idempotentes de uma $\mathbb{F}$-álgebra $A$ e relacionar esse conceito com o conceito de semissimplicidade de $\mathbb{F}$-álgebras. Iremos ainda estudar os idempotentes da álgebra de grupo $\mathbb{C}G$ de um grupo finito $G$, com a finalidade de usar as ferramentas obtidas a partir desse estudo para decompor a álgebra de grupo de um 2-grupo extra-especial sobre os complexos.

**Definição 1.35.** *Seja $A$ uma $\mathbb{F}$-álgebra. Um elemento $e \in A$ é dito um idempotente se $e^2 = e$.*

Observe que no caso em que $A$ é um $\mathbb{F}$-álgebra unitária, o elemento neutro aditivo 0 e a unidade 1 de A, são idempotentes e são chamados, idempotentes triviais. Além disso, dado qualquer idempotente $e \in A$, é facil verificar que $(1 - e)$ também é um idempotente de $A$.

**Definição 1.36.** *Um idempotente $e \in A$ é dito central se $e \in Z(A)$.*

Foi visto na Definição 1.18 que álgebras semissimples podem ser decompostas em uma soma de ideias minimais à esquerda. O próximo resultado relaciona o conceito de semissimplicidade de uma $\mathbb{F}$-álgebra com os seus idempotentes.

**Teorema 1.37.** *Uma $\mathbb{F}$-álgebra $A$ é semissimples se, e somente se, todo ideal à esquerda $I$ de $A$ for da forma $I = Ae$, para algum idempotente central $e \in A$. Além disso, no caso em que $A$ é semissimples e $\underline{e}$ é um idempotente central não trivial de $A$, temos que $A = Ae \oplus A(1 - e)$.*

**Demonstração.** Ver ([16], pg 96) . ∎

**Definição 1.38.** *Seja $e \in A$ um idempotente. Dizemos que $\underline{e}$ é um idempotente primitivo de $A$ se $\underline{e}$ não pode ser escrito como*

$$e = e_1 + e_2$$

*onde $e_1, e_2$ são idempotentes não nulos, tais que $e_1e_2 = e_2e_1 = 0$.*

Recordemos que, pelo Teorema de Maschke 1.20, no caso em que $G$ é um grupo finito e $\mathbb{F}$ é um corpo de característica zero, temos que a álgebra $\mathbb{F}G$ é semissimples. Assim, pelo Teorema 1.37, $\mathbb{F}G$ tem idempotentes centrais não triviais. Por tal motivo iremos por ora direcionar o nosso interesse nos idempotentes da $\mathbb{F}$-álgebra $\mathbb{F}G$, para G um grupo finito.

Seja $X$ um subconjunto do grupo finito $G$. Denotaremos por $\hat{X}$ o elemento de $\mathbb{F}G$ definido por

$$\hat{X} = \frac{1}{|X|}\sum_{x \in X} x.$$

**Lema 1.39.** *Seja $H \leq G$. Então $\hat{H}$ é um idempotente de $\mathbb{F}G$ e se $H \trianglelefteq G$, então $\hat{H}$ é central.*

**Demonstração.** Primeiro iremos mostrar que $\hat{H}$ é um idempotente. De fato,

$$\hat{H}\hat{H} = \left(\frac{1}{|H|}\sum_{h \in H} h\right)\hat{H} = \left(\frac{1}{|H|}\sum_{h \in H} h\hat{H}\right) = \left(\frac{1}{|\hat{H}|}\sum_{h \in H} \hat{H}\right) = \hat{H}.$$

Agora, suponhamos que $H \trianglelefteq G$, tomando $g \in G$ obtemos

$$\hat{H}^g = \frac{1}{|H|}\sum_{h \in H} h^g = \frac{1}{|H|}\sum_{\tilde{h} \in H} \tilde{h} = \hat{H}.$$

Dessa forma, $\hat{H}$ comuta com cada elemento da base de $\mathbb{F}G$ e, consequentemente, comuta com qualquer elemento de $\mathbb{F}G$, isto é, $\hat{H}$ é um idempotente central de $\mathbb{F}G$.

∎

Consideremos o conjunto $G\hat{H} = \{g\hat{H} \mid g \in G\} \subseteq \mathbb{F}G$, usando o resultado acima podemos mostrar que no caso em que $H \lhd G$, o conjunto $G\hat{H}$ com o produto definido por

$$g_1\hat{H}.g_2\hat{H} = g_1g_2\hat{H}$$

é um grupo.

**Teorema 1.40.** *Sejam $G$ um grupo e $H \lhd G$. Então, $\mathbb{F}G = \mathbb{F}G\hat{H} \oplus \mathbb{F}G(1-\hat{H})$ e $\mathbb{F}G\hat{H} \cong \mathbb{F}(G/H)$.*

**Demonstração.** Observe que, pelo Lema 1.39 e Teorema 1.37, temos que

$$\mathbb{F}G = \mathbb{F}G\hat{H} \oplus \mathbb{F}G(1-\hat{H}).$$

Afim de mostrarmos que $\mathbb{F}G\hat{H} \cong \mathbb{F}\big(G/H\big)$, vamos mostrar que $G\hat{H} \cong G/H$. Para tanto definimos

$$\begin{aligned} \varphi : G &\longrightarrow G\hat{H} \\ g &\longmapsto g\hat{H}. \end{aligned}$$

usando o fato de $\hat{H}$ ser um idempotente central é fácil mostrar que $\varphi$ é um homomorfismo de grupos. Por sua vez, se $h \in H$, então $\varphi(h) = h\hat{H} = \hat{H}$ o que implica em $H \subseteq ker\varphi$, a inclusão inversa segue do fato de $G$ ser uma base para $\mathbb{F}G$, portanto $Ker\varphi = H$. Agora, $\varphi$ é claramente sobrejetivo e, pelo teorema do isomorfismo, temos que $G/H \cong G\hat{H}$.

∎

O resultado a seguir nos diz que escolhendo $H = G^{'}$ no resultado anterior obtemos uma decomposição da nossa álgebra em duas componentes interessantes.

**Teorema 1.41.** *A álgebra de grupo $\mathbb{F}G$ pode ser decomposta como*

$$\mathbb{F}G = \mathbb{F}G\hat{G'} \oplus \mathbb{F}G(1-\hat{G'}),$$

*onde $\mathbb{F}G\hat{G'}$ é a soma de todas as componentes simples comutativas de $\mathbb{F}G$, e $\mathbb{F}G(1-\hat{G'})$ é a soma de todas as outras.*

**Demonstração.** Ver ( [16], pg.154). ∎

No que se segue nosso objetivo será determinar a componente comutativa $\mathbb{F}G\hat{G'}$ e a componente não comutativa $\mathbb{F}G(1-\hat{G'})$ de $\mathbb{F}G$, para o caso em que $\mathbb{F}=\mathbb{C}$ e $G$ é um 2-grupo extra-especial.

Seja $G$ um 2-grupo extra-especial de ordem $2^{2n+1}$, pela Proposição 1.29,

$$G/G^{'} = G/Z(G) \cong \underbrace{C_2 \times C_2 \times \cdots \times C_2}_{2^{2n} \text{ vezes}}$$

e pelo Teorema anterior $\mathbb{C}G\hat{G'} \cong \mathbb{C}G(C_2 \times C_2 \times \cdots \times C_2)$.

A seguir iremos mostrar que $\mathbb{C}G(C_2 \times C_2 \times \cdots \times C_2) \cong \overset{2^{2n}}{\oplus} \mathbb{C}$.

**Lema 1.42.** $\mathbb{C}C_p \cong \overset{p}{\oplus} \mathbb{C}$.

**Demonstração.** Seja $C_p = \langle g \rangle$. Observe que

$$\begin{aligned} \varphi : \mathbb{C}[x] &\longrightarrow \mathbb{C}C_p \\ f(x) &\longmapsto f(g) \end{aligned}$$

é um homomorfismo sobrejetor e que $x^p - 1 \in Ker\varphi$. Agora, por $\langle g \rangle$ ser uma base para $\mathbb{C}C_p$, $x^p-1$ é o polinômio de menor grau dentro do $ker\varphi$. Como $\mathbb{C}[x]$ é um domínio de ideais principais, então $Ker\varphi = \langle x^p - 1\rangle$.

Sendo

$$x^p - 1 = (x-1)(x-\xi)(x-\xi^2)\dots(x-\xi^{p-1}),$$

onde $\xi$ denota a $p$-ésima raiz da unidade, obtemos, pelo Teorema do Isomorfismo para álgebras e pelo Teorema Chinês do Resto [4], que

$$\mathbb{C}C_p \cong \mathbb{C}[x]/\left\langle x^p-1\right\rangle \cong \mathbb{C}[x]/\left\langle x-1\right\rangle \oplus \mathbb{C}[x]/\left\langle x-\xi\right\rangle \oplus \cdots \oplus \mathbb{C}[x]/\left\langle x-\xi^{p-1}\right\rangle,$$

portanto $\mathbb{C}C_p \cong \underbrace{\mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{p \text{ vezes}}$.

■

Usando o lema anterior, temos que

$$\mathbb{C}(C_p \times C_p) \cong \mathbb{C}C_p \otimes_{\mathbb{C}} \mathbb{C}C_p \cong \left(\overset{p}{\oplus}\mathbb{C}\right) \otimes_{\mathbb{C}} \left(\overset{p}{\oplus}\mathbb{C}\right) \cong \overset{p^2}{\oplus}\mathbb{C},$$

e, por indução, $\mathbb{C}G(\underbrace{C_p \times C_p \times \cdots \times C_p}_{n \text{ vezes}}) \cong \overset{p^n}{\oplus}\mathbb{C}$.

Desse modo, a decomposição da componente comutativa de $\mathbb{C}G$, para G um 2-grupo extra-especial, é dada por:

$$\mathbb{C}G\hat{G'} \cong \mathbb{C}G(C_2 \times C_2 \times \cdots \times C_2) \cong \overset{2^{2n}}{\oplus}\mathbb{C}.$$

Vamos agora analisar a componente não comutativa $\mathbb{C}G(1-\hat{G}')$. Na realidade, o que faremos a seguir é mostrar que a mesma é simples. Mas antes precisaremos de alguns resultados auxiliares:

**Lema 1.43.** *Sejam $G$ um 2-grupo extra-especial e $g \in G$. Se $g^{-1}Cl_G(g) \cap Z(G) \neq \{1\}$. Então $Z(G)$ contém um elemento $z$ de ordem 2, tal que $\widehat{Cl_G(g)}\hat{z} = \widehat{Cl_G(g)}$.*

**Demonstração.** Como $g^{-1}Cl_G(g) \cap Z(G) \neq \{1\}$, existe $z \in g^{-1}Cl_G(g) \cap Z(G)$ tal que $z = g^{-1}(h^{-1}gh) \neq 1$, para algum $h \in G$. Agora, $z$ tem ordem 2, pois $G$ é um 2-grupo extra-especial. Vamos mostrar que $Cl_G(g)\langle z\rangle = Cl_G(g)$:

Inicialmente observe que a partir de $z \in Z(G)$ e $gz = h^{-1}gh$, podê-se mostrar por indução que $gz^n = h^{-n}gh^n$ para todo $n \in \mathbb{N}$. Logo, $g^x z^n = (gz^n)^x = (h^{-n}gh^n)^x$ para todo $x \in G$ e $n \in \mathbb{N}$, portanto $g^x z^n \in Cl_G(g)$, ou seja, $Cl_G(g)\langle z\rangle \subseteq Cl_G(g)$ e, imediatamente, $Cl_G(g)\langle z\rangle = Cl_G(g)$. Dessa forma, podemos concluir que $\widehat{Cl_G(g)}\widehat{\langle z\rangle} = \widehat{Cl_G(g)}$.

■

Seja $\alpha \in \mathbb{C}G$. O suporte de $\alpha$, denotado por $Supp(\alpha)$, é o subconjunto de $G$ formado pelos elementos $g \in G$ que possuem coeficientes não nulos em $\alpha$, ou seja,

$$Supp(\alpha) = \{g \in G \mid \alpha_g \neq 0\}.$$

**Lema 1.44.** *Sejam $G$ um 2-grupo extra-especial e $\alpha \in Z(\mathbb{C}G(1-\hat{G}'))$. Então*

$$supp(\alpha) \subseteq Z(G).$$

**Demonstração.** Sendo $G$ um 2-grupo extra-especial, temos que $G' = Z(G) = \langle c\rangle$, onde $c$ é um elemento de ordem 2. Além disso, pelo o fato do centro de $G$ ser normal em $G$, decorre-se do Teorema 1.40 que

$$\mathbb{C}G \cong \mathbb{C}G\widehat{\langle c\rangle} \oplus \mathbb{C}G(1-\widehat{\langle c\rangle}).$$

Como $\alpha \in Z(\mathbb{C}G(1-\hat{c}))$, temos que $\alpha \in Z(\mathbb{C}G)$ (pois a outra componente de $\mathbb{C}G$ é comutativa). Em particular, $\alpha g = g\alpha \ \forall\ g \in G$, isto é, $g^{-1}\alpha g = \alpha \ \forall\ g \in G$, logo os elementos de uma mesma classe de conjugação de $G$ tem a mesma componente em $\alpha$. Podemos então escrever $\alpha$ na forma

$$\alpha = \sum_{g \in Z(G)} \alpha_g g + \sum_{g \notin Z(G)} \alpha_g^{'} \widehat{Cl_G(g)}.$$

Observe entretanto que $\alpha = \lambda(1-\widehat{\langle c\rangle})$ com $\lambda \in \mathbb{C}G$, logo $\alpha(1-\widehat{\langle c\rangle}) = \lambda(1-\widehat{\langle c\rangle})^2 = \lambda(1-\widehat{\langle c\rangle}) = \alpha$. Desse modo,

$$\alpha = \sum_{g \in Z(G)} \alpha_g g(1 - \langle \hat{c} \rangle) + \sum_{g \notin Z(G)} \alpha_g{}' \widehat{Cl_G(g)}(1 - \langle \hat{c} \rangle).$$

Por outro lado, para cada $g \notin Z(G)$, existe $h \in G$ tal que

$$1 \neq [g, h] \in g^{-1} Cl_G(g) \cap Z(G).$$

Então, pelo lema anterior, existe $z \in Z(G)$ de ordem 2 tal que $\widehat{Cl_G(g)}\hat{z} = \widehat{Cl_G(g)}$. Como $\langle z \rangle = \langle c \rangle$, temos que $\widehat{Cl_G(g)}\langle \hat{c} \rangle = \widehat{Cl_G(g)}$.

Desse modo,

$$\alpha = \sum_{g \in Z(G)} \alpha_g (1 - \langle \hat{c} \rangle) g + \sum_{g \notin Z(G)} \alpha_g' \widehat{Cl_G(g)} \langle \hat{c} \rangle (1 - \langle \hat{c} \rangle) = \sum_{g \in Z(G)} \alpha_g (1 - \langle \hat{c} \rangle) g,$$

isto é, $Supp(\alpha) \subseteq Z(G)$.

■

Como consequência imediata do lema acima, temos o seguinte resultado:

**Corolário 1.45.** *Seja $G$ um 2-grupo extra-especial. Então*

$$Z(\mathbb{C}G(1 - \hat{G}')) = \mathbb{C}Z(G)(1 - \hat{G}').$$

Agora temos todas as ferramentas necessárias para demonstrar que $\mathbb{C}G(1 - \hat{G}')$ é simples.

**Proposição 1.46.** *Seja $G$ um 2-grupo extra-especial. Então $\mathbb{C}G(1 - \hat{G}')$ é simples.*

**Demonstração.** Seja $\alpha$ um idempotente central em $\mathbb{C}G(1 - \hat{G}')$ segue, do corolário anterior, que $\alpha \in \mathbb{C}Z(G)(1 - \hat{G}')$.

Sendo $G$ um 2-grupo extra-especial, temos que

$$\mathbb{C}Z(G) = \mathbb{C}G' \cong \mathbb{C}C_2 \cong \mathbb{C} \oplus \mathbb{C}. \tag{1.1}$$

Por outro lado,

$$\mathbb{C}Z(G) = \mathbb{C}Z(G)\widehat{Z(G)} \oplus \mathbb{C}Z(G)(1 - \widehat{Z(G)}) = \mathbb{C}Z(G)\hat{G}' \oplus \mathbb{C}Z(G)(1 - \hat{G}'). \tag{1.2}$$

Então, de 1.1 e 1.2, decorre-se imediatamente que $\mathbb{C}Z(G)(1 - \hat{G}') \cong \mathbb{C}$. Como $\mathbb{C}$ é uma $\mathbb{C}$-álgebra simples, temos que $\alpha$ é nulo e, consequentemente, $\mathbb{C}G(1 - \hat{G}')$ é simples.

■

A partir das análises das componentes de $\mathbb{C}G$, $G$ um 2-grupo extra-especial de ordem $2^{2n+1}$, e do Teorema de Wedderburn-Artin 1.22, temos que a decomposição da $\mathbb{C}$-álgebra $\mathbb{C}G$ em componentes simples é dada por

$$\mathbb{C}G \cong \overset{2^{2n}}{\oplus} \mathbb{C} \oplus M_{2^n}(\mathbb{C}).$$

**Exemplo 1.47.** *Consideremos* $E_m$ $(m \geq 1)$ *o grupo extra-especial de ordem* $2^{2m+1}$ *dado pelo produto de* $m$ *grupos* $D^1, D^2, \ldots, D^m$, *onde para cada* $j \in \{1, \ldots, m\}$, *temos* $D^j \cong D_4$.

*Sabemos, por tudo o que foi discutido na seção anterior e nessa seção, que*

- $Z(E_m) = E_m^{'}$
- $|Z(E_m| = 2$
- $E_m/E_m^{'} \cong \overset{2^{2m}}{\oplus}\ \mathbb{C}$.

*Além disso, sabemos que a álgebra de grupo* $\mathbb{C}E_m$ *tem uma decomposição em uma componente comutativa e outra não comutativa, denotadas respectivamente, por* $\mathbb{C}\big(E_m/E_m^{'}\big)$ *e* $\Delta(E_m, E_m^{'})$.

*Sendo*

$$\mathbb{C}\big(E_m/E_m^{'}\big) \cong \mathbb{C}E_m\left(\frac{1+s}{2}\right) \cong \overset{2^{2m}}{\oplus}\ \mathbb{C} \qquad \text{onde} \quad E_m^{'} = \langle s \rangle$$

*e* $\Delta(E_m, E_m^{'}) = \mathbb{C}E_m\left(\dfrac{1-s}{2}\right)$, *temos que* $|E_m| = 2^{2m} + dim_{\mathbb{C}}(\Delta(E_m, E_m^{'}))$, *donde segue que* $dim_{\mathbb{C}}(\Delta(E_m, E_m^{'})) = 2^{2m}$ *e portanto*

$$\mathbb{C}E_m \cong \overset{2^{2m}}{\oplus}\ \mathbb{C} \oplus M_{2^m}(\mathbb{C}).$$

Usaremos esse exemplo no Capítulo 4 para a construção, através de representações do grupo $E_m$, de uma base para a álgebra das matrizes $2^m \times 2^m$ sobre $\mathbb{C}$, cujas matrizes são simétricas ou antissimétricas com relação a involução simplética (definida no Capítulo 3).

# Capítulo 2

# PI-álgebras

Nesse capítulo estaremos interessados em estudar as chamadas PI-álgebras, isto é, as $\mathbb{F}$-álgebras que satisfazem uma identidade polinomial não nula. Observando que o estudo das identidades polinomiais multilineares está diretamente ligado ao objetivo principal dessa dissertação, iremos expor o processo de multilinearização a fim de demonstrar que o T-ideal de identidades polinomiais de uma PI-álgebra $A$ sobre um corpo de característica zero é em algum sentido gerado por identidades multilineares. Vamos ainda estudar as identidades de traço, as identidades estáveis e as identidades alternadas. A definição dessas identidades bem como os exemplos de algumas delas que serão dados ao longo do capítulo serão essenciais para o desenvolvimento dos próximos capítulos.

## 2.1 Identidades polinomiais

Nessa seção iremos definir e apresentar alguns exemplos de PI-álgebras.

Consideremos $X = \{x_1, x_2, \ldots, \}$ um conjunto enumerável de variáveis não comutativas e $\mathbb{F}\langle X\rangle$ a álgebra livre associativa unitária gerada por $X$, definida em 1.13.

**Definição 2.1.** *Sejam $A$ uma $\mathbb{F}$-álgebra e $f = f(x_1, x_2, \ldots, x_n) \in \mathbb{F}\langle X\rangle$. Dizemos que $f$ é uma identidade polinomial para a álgebra $A$, se*

$$f(a_1, a_2, \ldots, a_n) = 0,$$

*para quaisquer $a_1, a_2, \ldots, a_n \in A$. Nesse caso, escrevemos $f \equiv 0$.*

Observe que o polinômio $f = 0$ é uma identidade polinomial para qualquer $\mathbb{F}$-álgebra $A$. Essa identidade polinomial é denominada a identidade trivial.

**Definição 2.2.** *Uma $\mathbb{F}$-álgebra $A$ é chamada uma álgebra com identidade polinomial, ou PI-álgebra, se $A$ satisfaz uma identidade polinomial não-trivial.*

Daremos a seguir alguns exemplos de PI-álgebras. Para tanto definimos os chamados comutadores de Lie de peso $n$. Começamos definindo o comutador de Lie de peso 2 dado por

$$[a, b] = ab - ba$$

e indutivamente definimos o comutador de Lie de peso $n \geq 3$ por

$$[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$

**Exemplo 2.3.** *Seja $A$ uma $\mathbb{F}$-álgebra comutativa e considere $f = f(x_1, x_2) = [x_1, x_2]$. Como $ab = ba$, para quaisquer $a, b \in A$, temos que $f$ é uma identidade polinomial para $A$. Dessa forma, toda $\mathbb{F}$-álgebra comutativa $A$ é uma PI-álgebra.*

**Exemplo 2.4.** *Seja $A$ um $\mathbb{F}$-álgebra nilpotente com índice de nilpotência $n$. Então $A$ é uma PI-álgebra. De fato, considerando o polinômio $f = f(x_1, x_2, \ldots, x_n) = x_1x_2 \ldots x_n$. Como o índice de nilpotência de $A$ é $n$, temos pela Definição 1.18, que $f$ é uma identidade polinomial para $A$ e portanto $A$ é uma PI-álgebra.*

**Exemplo 2.5.** *A álgebra $UT_n(\mathbb{F})$ é uma PI-álgebra, para qual uma identidade polinomial é $f = f(x_1, x_2, \ldots, x_{2n}) = [x_1, x_2][x_3, x_4] \ldots [x_{2n-1}, x_{2n}]$. De fato, sejam $A, B \in UT_n(\mathbb{F})$. Sabemos que os elementos da diagonal principal de $AB$ são iguais aos da diagonal principal de $BA$. Assim, a matriz $C = [A, B]$ é uma matriz triangular estritamente superior, portanto pelo o que foi enunciado no Exemplo* 1.19, *temos que $f(A_1, A_2, \ldots, A_{2n}) = 0$, para quaisquer $A_1, A_2, \ldots, A_{2n} \in UT_n(\mathbb{F})$.*

**Exemplo 2.6.** *Sejam $A, B$ e $C \in M_2(\mathbb{F})$. Afirmamos que $[[A, B]^2, C] = 0$.*
*Com efeito, considere $D \in M_2(\mathbb{F})$. A expressão matricial do polinômio característico associado a $D$ é:*

$$p(x) = x^2 - tr(D)x + det(D)I_2.$$

*Sendo $D = [A, B]$, temos que $tr(D) = 0$ e pelo Teorema de Cayley- Hamilton, segue que*

$$D^2 = -det(D).I_2$$

*logo,*

$$[[A, B]^2, C] = [D^2, C] = [-det(D).I_2, C] = 0.$$

*Desse modo, $M_2(\mathbb{F})$ é uma PI-álgebra para qual $f(x_1, x_2, x_3) = [[x_1, x_2]^2, x_3]$ é uma identidade polinomial.*

**Definição 2.7.** *Dada uma $\mathbb{F}$-álgebra $A$, definimos*

$$Id(A) = \{f \in \mathbb{F}\langle X\rangle |\ f \equiv 0 \ em\ A\}$$

*como sendo o conjunto das identidades polinomiais de $A$.*

É fácil ver que $Id(A)$ é um ideal de $\mathbb{F}\langle X\rangle$. Além disso, se $f = f(x_1, x_2, \ldots, x_n)$ é um polinômio qualquer em $Id(A)$ e $g_1, \ldots g_n$ são polinômios arbitrários em $\mathbb{F}\langle X\rangle$, então $f(g_1, g_2, \ldots, g_n) \in Id(A)$.

Uma vez que, qualquer endomorfismo de $\mathbb{F}\langle X\rangle$ é unicamente determinado mapeando-se cada variável $x \in \mathbb{F}\langle X\rangle$ em um polinômio $g \in \mathbb{F}\langle X\rangle$, segue do que foi observado acima, que $Id(A)$ é invariante sobre todos os endomorfismos de $\mathbb{F}\langle X\rangle$. Ideais com essa propriedade são denominados $T$-ideais.

**Definição 2.8.** *Um ideal $I$ de $\mathbb{F}\langle X\rangle$ é dito um $T$-ideal, se $\varphi(I) \subseteq I$ para todo endomorfismo $\varphi$ de $\mathbb{F}\langle X\rangle$.*

A proposição a seguir caracteriza todos os $T$-ideais de $\mathbb{F}\langle X\rangle$ como sendo ideais de identidades polinomiais.

**Proposição 2.9.** *Seja $I$ um $T$-ideal de $\mathbb{F}\langle X\rangle$. Então $Id\big(\mathbb{F}\langle X\rangle/I\big) = I$.*

**Demonstração.** Dado $f(x_1, \ldots, x_n) \in I$. Para quaisquer $g_1 + I, \ldots, g_n + I \in \mathbb{F}\langle X\rangle/I$, temos, por $I$ ser um T-ideal,

$$f(g_1 + I, \ldots, g_n + I) = f(g_1, \ldots, g_n) + I = 0 + I.$$

Portanto, $I \subseteq Id\big(\mathbb{F}\langle X\rangle/I\big)$.

Reciprocamente, consideremos $h(x_1, \ldots, x_n) + I \in Id\big(\mathbb{F}\langle X\rangle/I\big)$. Como

$$h(x_1 + I, \ldots, x_n + I) = 0 + I,$$

segue que $f(x_1, \ldots, x_n) + I = 0 + I$, isto é, $f(x_1, \ldots, x_n) \in I$. O que nos mostra por fim que $I = Id\big(\mathbb{F}\langle X\rangle/I\big)$. ∎

Um $T$-ideal é gerado, como $T$-ideal, por um conjunto $S \subset \mathbb{F}\langle X\rangle$ se todo elemento de $I$ pode ser escrito como uma $\mathbb{F}$-combinação linear de elementos da forma:

$$h_1 f(g_1, \ldots, g_n) h_2$$

onde os polinômios $h_1, h_2, g_1, \ldots g_n \in \mathbb{F}\langle X\rangle$ e $f \in S$. Nesse caso, escrevemos $I = \langle S\rangle_T$.

Dois conjuntos $S_1$ e $S_2$ são ditos equivalentes se $\langle S_1 \rangle_T = \langle S_2 \rangle_T$. Além disso, dizemos que um polinômio $f$ é uma consequência de polinômios em um conjunto $S \subset \mathbb{F}\langle X \rangle$, se $f \in \langle S \rangle_T$.

Em 1950, Specht conjecturou que todo $T$-ideal $I$ sobre um corpo de característica 0 é finitamente gerado, ou seja, existe um conjunto $S \subset \mathbb{F}\langle X \rangle$ finito, tal que $I = \langle S \rangle_T$. Essa conjectura foi provada mais tarde, em [12], por Kemer.

## 2.2 Processo de multilinearização

Nessa seção iremos expor o processo de multilinearização, com o objetivo de concluirmos que todo $T$-ideal de $\mathbb{F}\langle X \rangle$, em que $\mathbb{F}$ é um corpo de característica zero, é gerado como $T$-ideal por um número finito de polinômios multilineares.

**Definição 2.10.** *Sejam $u = \alpha x_{i_1} \dots x_{i_k}$ um monômio e $f(x_1, x_2, \dots, x_n)$ um polinômio, ambos em $\mathbb{F}\langle X \rangle$.*

*i) O grau de $x_i$ em $u$, denotado por $gr_{x_i}(u)$, é definido como sendo o número de ocorrências das variáveis $x_i$ em $u$.*

*ii) O grau de $x_i$ em $f$, denotado por $gr_{x_i}(f)$, é definido como o maior $gr_{x_i}(u)$ dentre todos os monômios de $f$.*

*iii) O grau de um monômio $u$, denotado por $gr(u)$, é definido como sendo*

$$gr(u) = \sum_{j=1}^{k} gr_{x_{i_j}}(u)$$

.

*iv) O grau de $f$, denotado por $gr(f)$ é definido como sendo o maior valor de $gr(u)$ dentre todos os monômios de $f$.*

**Exemplo 2.11.** *Considere,*

$$f = f(x_1, x_2, x_3 x_4) = x_3 x_2^2 x_1 x_4 - x_3 x_4 x_3^2 x_1 + x_1 x_3 x_4 x_2 x_4$$

*então $gr(f) = 5$; $gr_{x_1}(f) = 1$; $gr_{x_2}(f) = 2$; $gr_{x_3}(f) = 3$ e $gr_{x_4}(f) = 2$.*

**Definição 2.12.** *Seja $f$ um polinômio. Com base na definição anterior:*

*i) Dizemos que $f$ é um polinômio homogêneo na variável $x_i$ quando $gr_{x_i}(u)$ é igual para todo monômio $u$ de $f$.*

*ii) Dizemos que $f$ é um polinômio multihomogêneo quando é homogêneo em cada uma das suas variáveis.*

*iii) Dizemos que $f$ é um polinômio linear na variável $x_i$ quando $gr_{x_i}(u) = 1$ para todo monômio $u$ de $f$.*

*iv) Dizemos que $f$ é um polinômio multilinear quando é linear em cada uma das suas variáveis.*

**Exemplo 2.13.** *O polinômio*

$$g(x_1, x_2, x_3) = x_1^2 x_2 x_3 + 4x_2 x_1 x_3 x_1 - 3x_1 x_3 x_2 x_1$$

*é multihomogêneo, mas não é multilinear. Já o polinômio*

$$h(x_1, x_2, x_3, x_4) = x_1 x_4 x_3 x_2 + 2x_3 x_2 x_1 x_4 - 7x_4 x_2 x_1 x_3 + x_2 x_4 x_1 x_3$$

*é multilinear.*

Seja $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}\langle X \rangle$, podemos escrever $f = f(x_1, x_2, \ldots, x_n)$ na forma

$$f = \sum_{i_1 \geq 0, \ldots, i_n \geq 0} f^{(i_1, \ldots, i_n)},$$

onde $f^{(i_1, \ldots, i_n)}$ é a soma de todos os monômios em $f$ em que $x_1, \ldots, x_n$ tem grau $i_1, \ldots, i_n$, respectivamente. Os polinômios $f^{(i_1, \ldots, i_n)}$ que são não-nulos, são chamados as componentes multihomogêneas de $f$.

**Teorema 2.14.** *Seja $\mathbb{F}$ um corpo infinito. Se $f = f(x_1, x_2, \ldots, x_n)$ é uma identidade polinomial para uma $\mathbb{F}$-álgebra $A$, então toda componente multihomogênea de $f$ também é uma identidade polinomial para $A$.*

**Demonstração.** Observe que para cada variável $x_t$ de $f(x_1, x_2, \ldots, x_n)$ $(1 \leq t \leq n)$, podemos escrever $f$ na forma

$$f = \sum_{i=0}^{m} f_i,$$

onde $f_i$ é a soma de todos os monômios de $f$ nos quais $x_t$ tem grau $i$ e $m = gr_{x_t}(f)$ é o grau de $x_t$ em $f$.

Por um argumento de indução é suficiente demonstrar que, para toda variável $x_i$ de $f(x_1, x_2, \ldots, x_n)$, $f_i$ é uma identidade polinomial de $f$.

Sejam $\alpha_0, \alpha_1, \ldots, \alpha_m$ elementos distintos de $\mathbb{F}$. Sendo $f$ uma identidade polinomial de $A$, temos que para qualquer $\alpha \in A$, $f(x_1, \ldots, \alpha x_t, \ldots, x_n)$ também é uma identidade para $A$. Como

$$f(x_1, \ldots, \alpha x_t, \ldots, x_n) = \sum_{i=0}^{m} \alpha^i f_i(x_1, \ldots, x_t, \ldots x_n),$$

então para cada $j \in \{0, \ldots m\}$,

$$f(x_1, \ldots, \alpha_j x_t, \ldots, x_n) = \sum_{i=0}^{m} {\alpha_j}^i f_i(x_1, \ldots, x_t, \ldots x_n).$$

Assim, para quaisquer $a_1, \ldots, a_n \in A$, escrevemos $f_i(a_1, \ldots, a_n) = \bar{f}_i$ e, por $f$ ser uma identidade polinomial de $A$, obtemos o sistema

$$\begin{cases} \bar{f}_0 + \alpha_0 \bar{f}_1 + \cdots + \alpha_0^m \bar{f}_m = 0 \\ \bar{f}_0 + \alpha_1 \bar{f}_1 + \cdots + \alpha_1^m \bar{f}_m = 0 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \bar{f}_0 + \alpha_m \bar{f}_1 + \cdots + \alpha_m^m \bar{f}_m = 0 \end{cases}.$$

Como a matriz associada ao sistema,

$$\Delta = \begin{bmatrix} 1 & \alpha_0 & \ldots & \alpha_0^m \\ 1 & \alpha_1 & \ldots & \alpha_1^m \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_m & \ldots & \alpha_m^m \end{bmatrix} \qquad \text{matriz de Vandermonde}$$

é tal que $det(\Delta) = \prod_{0 \leq i < j \leq m} (\alpha_j - \alpha_i) \neq 0$. Concluímos que $(\bar{f}_0, \ldots, \bar{f}_m) = (0, \ldots, 0)$ e, por conseguinte, $\bar{f}_0, \ldots, \bar{f}_m$ são identidades polinomiais de $A$. ∎

Segue imediatamente do resultado acima que qualquer $T$-ideal sobre um corpo infinito é gerado por polinômios multihomogêneos.

Entre os polinômios multihomogêneos, um papel importante é desempenhado pelos polinômios multilineares. Em um polinômio multilinear $f(x_1, x_2, \ldots, x_n)$ cada variável aparece em cada monômio com grau igual a exatamente 1, portanto está claro que esse polinômio é sempre da forma

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \ldots x_{\sigma(n)}, \qquad \text{onde } \alpha_\sigma \in \mathbb{F}.$$

Note que, se $f(x_1, x_2, \ldots, x_n)$ é um polinômio linear em uma variável, digamos $x_1$, então

$$f(\sum \alpha_i y_i, x_2, \ldots, x_n) = \alpha_i \sum f(y_i, x_2, \ldots, x_n), \qquad \forall\ \alpha_i \in \mathbb{F} \text{ e } y_i \in \mathbb{F}\langle X \rangle.$$

Essa propriedade tem diversas aplicações, entre elas, a proposição à seguir:

**Proposição 2.15.** *Seja $A$ uma $\mathbb{F}$-álgebra gerada linearmente sobre $\mathbb{F}$ pelo conjunto $B$. Se um polinômio multilinear $f$ se anula sobre todas as avaliações tomadas no conjunto $B$, então $f$ é uma identidade polinomial de $A$.*

**Demonstração.** Sejam $a_1, \ldots, a_n$ elementos de $A$. Como $A$ é gerada linearmente por $B$ sobre $\mathbb{F}$, temos que $a_1 = \sum \alpha_{1i_1} u_{i_1}, \ldots, a_n = \sum \alpha_{ni_n} u_{i_n}$, onde os $u_{i_k}{}'s$ são elementos de $B$. Então, como $f(x_1, x_2, \ldots, x_n)$ é um polinômio multilinear, temos que

$$\begin{aligned} f(a_1, \ldots, a_n) &= f(\sum \alpha_{1i_1} u_{i_1}, \ldots, \sum \alpha_{ni_n} u_{i_n}) \\ &= \sum \alpha_{1i_1} \alpha_{2i_2} \ldots \alpha_{ni_n} f(u_{i_1}, u_{i_2}, \ldots, u_{i_n}) \\ &= 0 \end{aligned}$$

e portanto $f(x_1, x_2, \ldots, x_n)$ é uma identidade polinomial para $A$.

■

Seja A uma $\mathbb{F}$-álgebra, onde $\mathbb{F}$ é um corpo infinito de característica diferente de 2. O próximo teorema mostra que a partir de uma identidade polinomial de grau $k$ para $A$, é possível obter uma identidade multilinear para $A$ de grau menor ou igual a $k$.

**Teorema 2.16.** *(Processo de Multilinearização) Sejam $\mathbb{F}$ um corpo infinito de característica diferente de 2 e $f(x_1, x_2, \ldots, x_n)$ uma identidade polinomial de uma $\mathbb{F}$-álgebra $A$ de grau $k$. Então, existe uma identidade polinomial multilinear $h$ de $A$ cujo o grau é menor ou igual à $k$.*

**Demonstração.** Suponhamos inicialmente que $gr_{x_i}(f) \leq 1$ para todo $i \in \{1, \ldots, n\}$. Decompomos $f$ na soma de seus monômios

$$f = \sum_{j=1}^{m} \alpha_j u_j, \qquad onde \alpha_j \in \mathbb{F} \backslash \{0\}.$$

No caso em que $gr_{x_i} u_j = 1$, para todo $i \in \{1, \ldots n\}$ e $j \in \{1, \ldots, m\}$, temos que $f$ já é um polinômio multilinear, então obviamente o resultado se verifica. Suponhamos que $f$ não é um polinômio multilinear, ou seja, existem $i \in \{1, \ldots, n\}$ e $j, l \in \{1, \ldots, m\}$ tais que

$gr_{x_i}u_j = 0$ e $gr_{x_i}u_l = 1$. Seja $x_{i_1}$ uma variável de $f$ com essa propriedade, e consideremos o endomorfismo de $\mathbb{F}\langle X\rangle$ definido por

$$\begin{aligned} \phi_{i_1} : \mathbb{F}\langle X\rangle &\longrightarrow \mathbb{F}\langle X\rangle \\ x_j &\longmapsto 0 \qquad \text{caso } j = i_1 \\ x_j &\longmapsto x_j \qquad \text{caso contrário,} \end{aligned}$$

temos que $\phi_{i_1}(f)$ é uma identidade de $A$, onde a variável $x_{i_1}$ não aparece. Caso o polinômio resultante $\phi_{i_1}(f)$ for multilinear, concluímos a demonstração para esse primeiro caso. Caso contrário, existe uma variável $x_{i_2}$ em $\phi_{i_1}(f)$ com a mesma propriedade que $x_{i_1}$ tinha em $f$. Assim, construímos novamente um endomorfismo $\phi_{i_2}(\phi_{i_1}(f))$ de $\mathbb{F}\langle X\rangle$ que associa $x_{i_2}$ a 0 e mantém as outras variáveis de $\phi_{i_1}(f)$ fixas. Caso $\phi_{i_2}(\phi_{i_1}(f))$ seja multilinear, terminamos a demonstração. Caso contrário, repetimos o procedimento anterior. Como o número de variáveis de $f$ é finito, esse processo será interrompido em alguma etapa e assim iremos obter, a partir de $f$, uma identidade multilinear.

Consideraremos agora o caso em que $gr_{x_i}(f(x_1, \dots, x_i, \dots, x_n)) = d > 1$, para algum $i \in \{1, \dots, n\}$. Veremos que é possível obter uma identidade $h$ de $A$, em que

$$gr_{y_i}(h(x_1, \dots, \underbrace{y_i, y_{i+1}}_{\hat{x}_i}, \dots, x_n)) = gr_{y_{i+1}}(h(x_1, \dots, \underbrace{y_i, y_{i+1}}_{\hat{x}_i}, \dots, x_n)) = d - 1.$$

Observe que nessa notação, a $i$-ésima variável de $h$ é omitida e surgem as variáveis $y_i$ e $y_{i+1}$. A fim de simplificar a demonstração, iremos supor que $gr_{x_1}(f(x_1, \dots, x_i, \dots, x_n)) = d > 1$. Desse modo, considere o polinômio:

$$h(y_1, y_2, x_2, \dots, x_n) = f(y_1 + y_2, x_2, \dots, x_n) - f(y_1, x_2, \dots, x_n) - f(y_2, x_2, \dots, x_n). \quad (2.1)$$

Note que $h$ é uma identidade polinomial de $A$. Além disso observe que,

$$gr_{y_1}(f(y_1 + y_2, x_2, \dots, x_n)) = gr_{y_2}(f(y_1 + y_2, x_2, \dots, x_n)) = d$$

$$gr_{y_1}(f(y_1, x_2, \dots, x_n)) = gr_{y_2}(f(y_2, x_2, \dots, x_n)) = d$$

$$gr_{y_1}(h(y_1, y_2, x_2, \dots, x_n)) = gr_{y_2}(h(y_1, y_2, x_2, \dots, x_n)) = d - 1.$$

Substituindo, $y_1$ e $y_2$ por $x_1$ em 2.1 obtemos

$$h(x_1, x_1, x_2, \dots, x_n) = f(2x_1, x_2, \dots, x_n) - 2f(x_1, x_2, \dots, x_n).$$

Vamos verificar que $h$ é um polinômio não nulo. Seja $f_i$ a componente de $f$ de grau $i$ na variável $x_1$. Assim,

$$f(2x_1, x_2, \ldots, x_n) = \sum_{i=0}^{d} 2^i f_i$$

Suponhamos por absurdo que

$$\sum_{i=0}^{d} 2^i f_i = 2\bigg(\sum_{i=0}^{d} f_i\bigg),$$

então $-f_0 + (2^2 - 2)f_2 + (2^3 - 2)f_3 + \cdots + (2^d - 2)f_d = 0$. Logo,

$$f_0 = (2^2 - 2)f_2 + (2^3 - 2)f_3 + \cdots + (2^d - 2)f_d.$$

Sabemos que $gr_{x_1}(f_0) = 0$, mas por outro lado

$$gr_{x_1}((2^2 - 2)f_2 + \cdots + (2^d - 2)f_d) = d > 1,$$

o que é um absurdo. Desse modo, $h$ é uma identidade multilinear não nula de $A$ com a propriedade desejada.

Sendo $\mathbb{F}$ um corpo infinito, podemos considerar, pelo Teorema 2.14, $f(x_1, x_2, \ldots, x_n)$ multihomogêneo. Caso $f$ obedeça as hipóteses do primeiro caso, basta aplicar o algoritmo desenvolvido neste. Caso isso não aconteça, então $gr_{x_i}(f) > 1$ para algum $i \in \{1, \ldots n\}$. Realizando uma indução no grau de $x_i$, construímos a partir do caso anterior, uma identidade $g$ de $A$ com $gr_{y_i}(g) = 1$. Repetindo esse procedimento, se necessário, para as outras variáveis de $h$, obtemos uma identidade $h(z_1, \ldots, z_m)$ com $gr_{z_i}(h) = 1$ para todo $i \in \{1, \ldots n\}$. ■

Como consequência do processo de multilinearização, obtemos o seguinte resultado.

**Teorema 2.17.** *Sejam $\mathbb{F}$ um corpo de característica zero e $f \in \mathbb{F}\langle X \rangle$ um polinômio qualquer. Então $f(x_1, x_2, \ldots, x_n)$ é uma consequência de uma quantidade finita de polinômios multilineares.*

**Demonstração.** Seja $I = \langle f \rangle_T$ o $T$-ideal gerado por $f$. Sabemos que, pela proposição 2.9, existe uma $\mathbb{F}$-álgebra $A$ tal que $Id(A) = I$. Vimos no Teorema 2.14 que $f$ é consequência de polinômios multihomogêneos. Então vamos considerar $f$ multihomogêneo e aplicar no mesmo o processo de multilinearização:

Se $gr_{x_1} f = d > 1$, então escrevemos

$$h = f(y_1 + y_2, x_2, \ldots, x_n) = \sum_{i=0}^{d} g_i(y_1, y_2, x_2, \ldots, x_n)$$

onde $gr_{y_1}g_i = i, gr_{y_2}g_i = d - i$ e $gr_{x_t}g_i = gr_{x_t}f$ para todo $t \in \{2, \ldots, n\}$. Como $f$ é uma identidade polinomial de $A$, temos que $h$ também é uma identidade polinomial de $A$. Sendo $g_0, \ldots, g_d$ componentes multihomogêneas de $h$, segue do Teorema 2.14 que cada uma dessas componentes pertencem à $Id(A)$. Dessa forma, $\langle g_0, \ldots, g_d \rangle \subseteq Id(A) = \langle f \rangle_T$. Por outro lado, note que para todo $i \in \{0, \ldots, d\}$ temos

$$g_i(y_1, y_1, x_2, \ldots, x_n) = \binom{d}{i} f(y_1, x_2, \ldots, x_n).$$

Como $Char(\mathbb{F}) = 0$, temos que $\binom{d}{i} \neq 0$ e portanto, $\langle g_0, \ldots, g_d \rangle = \langle f \rangle_T$.

O restante da demonstração segue por indução.

■

A partir desse resultado e pelo o que foi conjecturado em 1950 por Specht, e mais tarde demonstrado em [12] por Kemer, obtemos o seguinte resultado:

**Corolário 2.18.** *Se $Char(\mathbb{F}) = 0$, então todo $T$-ideal de $\mathbb{F}\langle X \rangle$ é gerado como $T$-ideal por um número finito de polinômios multilineares.*

## 2.3 Identidades de traço

Nessa seção iremos definir e estudar algumas propriedades do conceito de traço no contexto da álgebra $\mathbb{F}\langle X \rangle$, com o intuito de definir as identidades de traço para uma $\mathbb{F}$-álgebra.

**Definição 2.19.** *Seja $A$ uma $\mathbb{F}$-álgebra. Uma função traço é uma aplicação $\mathbb{F}$-linear*

$$tr : A \longrightarrow \mathbb{F}$$

*satisfazendo:*

*1) $tr(ab) = tr(ba)$*

*2) $tr(aTr(b)) = tr(a).tr(b)$*

*para quaisquer $a, b \in A$.*

Observe ainda que, pela definição acima,

$$tr(a_1 \ldots a_{n-1}a_n) = tr((a_1 \ldots a_{n-1})a_n) = tr(a_n a_1 \ldots a_{n-1})$$

para todo $n \in \mathbb{N}$.

**Definição 2.20.** *No caso em que $A = \mathbb{F}\langle X \rangle$, iremos definir o traço como sendo um símbolo formal, linear sobre $\mathbb{F}$, e que satisfaz:*

*(i)* $tr(x_{i_1}x_{i_2}\dots x_{i_n}) = tr(x_{i_n}x_{i_1}\dots x_{i_{n-1}})$

*(ii)* $tr(f)x_i = x_i tr(f)$

*(iii)* $tr(ftr(g)) = tr(f)tr(g)$,

*para toda variável* $x_i \in X$ *e* $f, g \in \mathbb{F}\langle X \rangle$.

A seguir vamos estabelecer algumas nomenclaturas, que serão importantes para o entendimento do Capítulo 4 dessa dissertação.

**Definição 2.21.** *Um monômio de traço simples é definido como sendo uma expressão da forma*

$$tr(x_{i_1}x_{i_2}\dots x_{i_t}).$$

*Um traço puramente monomial é um produto de monômios de traços simples, ou seja, é da forma*

$$tr(x_{i_1}x_{i_2}\dots x_{i_{t_1}})tr(x_{j_1}x_{j_2}\dots x_{j_{t_2}})\dots tr(x_{k_1}x_{k_2}\dots x_{k_{t_n}}).$$

*Um monômio de traço é o produto de um monômio de* $\mathbb{F}\langle X \rangle$ *com um número arbitrário de traços puramente monomiais, ou seja, um monômio de traço é da forma:*

$$x_{i_1}x_{i_2}\dots x_{i_t}tr(x_{j_1}x_{j_2}\dots x_{j_{t_1}})tr(x_{k_1}x_{k_2}\dots x_{k_{t_2}})\dots tr(x_{l_1}x_{l_2}\dots x_{l_{t_n}}).$$

**Definição 2.22.** *O grau de uma variável* $x_i \in X$*, denotado por* $gr_{x_i}h$*, de um monômio de traço* $h$ *é computado contando-se as ocorrências de* $x_i$ *em* $h$*, independentemente se ela aparece no interior ou fora do símbolo* $tr$.

**Definição 2.23.** *A álgebra livre com traço* $\mathbb{F}\langle T' \rangle$ *é a álgebra gerada pelos monômios de traço com a multiplicação dada por justaposição e satisfazendo* $(i), (ii)$ *e* $(iii)$ *da Definição 2.20. Seus elementos são chamados de polinômios de traço.*

*A álgebra de polinômios puramente de traço* $\mathbb{F}\langle X \rangle$*, é a subálgebra de* $\mathbb{F}\langle T' \rangle$ *gerada por mônomios de traço simples.*

Observe que a definição acima nos diz que os elementos de $\mathbb{F}\langle T' \rangle$ serão escritos como $\mathbb{F}$-combinações lineares de elementos da forma

$$w_1 tr(w_2)\dots tr(w_k) \qquad \text{ou} \qquad tr(w_1)\dots tr(w_k),$$

onde $w_1, w_2, \dots, w_k$ são palavras em $x_i \in X$ permitindo a palavra vazia 1.

É fácil ver que a álgebra $\mathbb{F}\langle T' \rangle$ é uma álgebra associativa na qual $tr$ age linearmente e

$$tr(w_1 tr(w_2)\dots tr(w_k)) = tr(w_1)tr(w_2)\dots tr(w_k).$$

Iremos ainda definir um polinômio de traço homogêneo e multilinear, de acordo com os graus dos seus monômios obtidos desconsiderando-se o traço e seguindo as definições estabelecidas em 2.12 do caso ordinário.

**Exemplo 2.24.** *O polinômio*

$$f = f(x_1, x_2, x_3) = tr(x_1x_2)tr(x_1x_3^2) - tr(x_1^2x_2x_3^2)$$

*é um polinômio puramente de traço homogêneo e o polinômio*

$$g = g(x_1, x_2, x_3) = tr(x_1x_2)tr(x_3) - tr(x_1x_2x_3)$$

*é um polinômio multilinear puramente de traço.*

**Definição 2.25.** *Seja $A$ uma $\mathbb{F}$-álgebra sobre a qual se tem definida uma função de traço. Uma identidade de traço de $A$, é um polinômio de traço que se anula sobre $A$, sempre que substituímos as variáveis $x_i$'s que aparecem nesse polinômio por elementos de $A$ e o traço $tr$ definido em $\mathbb{F}\langle T' \rangle$ pela função de traço $tr$ definida em $A$.*

Sobre essa definição é imprescindível observar que, quando $\mathbb{F}$ é um corpo infinito de característica diferente de 2, podemos multilinearizar identidades de traço, aplicando-se o mesmo processo de multilinearização dado no Teorema 2.16.

## 2.4 Identidades polinomiais alternadas e estáveis

Nessa seção iremos definir as identidades polinomiais alternadas e estáveis que serão importantes para a compreensão de alguns resultados do nosso trabalho. Além disso, ao falar de identidades polinomiais alternadas vamos definir o polinômio standard e apresentar o famoso Teorema de Amitsur e Levitzki [3] que estabelece, que o polinômio standard de grau $2n$ é uma identidade polinomial de grau minímo para $M_n(\mathbb{F})$.

**Definição 2.26.** *Seja $f$ uma identidade polinomial para a $\mathbb{F}$-álgebra $A$. Dizemos que $f$ é uma identidade estável para $A$, se $f$ for uma identidade polinomial para a $\mathbb{F}$-álgebra $A \otimes_{\mathbb{F}} C$, para toda $\mathbb{F}$-álgebra comutativa $C$.*

O resultado a seguir estabelece que no caso em que $\mathbb{F}$ é um corpo infinito podemos afirmar que toda identidade de uma $\mathbb{F}$-álgebra $A$ é estável, ou seja, toda identidade polinomial de $A$ é uma identidade polinomial de $A \otimes_{\mathbb{F}} C$.

**Proposição 2.27.** *Seja $\mathbb{F}$ um corpo infinito e $A$ uma $\mathbb{F}$-álgebra, então toda identidade polinomial de $A$ é estável.*

**Demonstração.** Sejam $f = f(x_1, x_2, \ldots, x_n)$ uma identidade polinomial para $A$, $C$ uma álgebra comutativa sobre $\mathbb{F}$ e $\bar{A} = A \otimes_{\mathbb{F}} C$. Pelo Teorema 2.14 podemos assumir que $f$ é um polinômio multihomogêneo com $gr_{x_i}(f) = m_i$, $1 \leq i \leq n$.

Dados $\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n} \in \bar{A}$, precisamos mostrar que $f(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n}) = 0$.

Suponhamos primeiramente que $\bar{a_1} = a_1 \otimes c_1, \bar{a_2} = a_2 \otimes c_2, \ldots, \bar{a_n} = a_n \otimes c_n$, então

$$f(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n}) = f(a_1, a_2, \ldots, a_n) \otimes c_1^{m_1} c_2^{m_2} \ldots_n^{m_n} = 0.$$

Agora, suponhamos que $\bar{a_1} = b_1 \otimes d_1 + b_2 \otimes d_2, \bar{a_2} = a_2 \otimes c_2, \ldots, \bar{a_n} = a_n \otimes c_n$, então

$$\begin{aligned} f(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n}) = {} & f(b_1 \otimes d_1, a_2 \otimes c_2, \ldots, a_n \otimes c_n) + f(b_2 \otimes d_2, a_2 \otimes c_2, \ldots, a_n \otimes c_n) \\ & + \sum_{i=1}^{m_1 - 1} f_i(b_1 \otimes d_1, b_2 \otimes d_2, a_2 \otimes c_2, \ldots, a_n \otimes c_n), \end{aligned}$$

já que

$$f(x_1 + y_1, x_2, \ldots, x_n) - f(x_1, x_2, \ldots, x_n) - f(y_1, x_2, \ldots, x_n) = \sum_{i=1}^{m_1 - 1} f_i(x_1, y_1, x_2, \ldots, x_n)$$

e $gr_{x_1}(f_i) = i$. Uma vez que todos os polinômios $f_i$ acima são multihomogêneos, temos pelo primeiro caso que $f(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n}) = 0$.

Por fim, generalizamos o argumento acima para o caso em que

$$\bar{a_1} = \sum a_{1i} \otimes c_{1i}, \ldots, \bar{a_n} = \sum a_{ni} \otimes c_{ni} \in \bar{A}.$$

Escrevemos $f(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n})$ como a soma de expressões da forma

$$\bar{g} = g(a_{i_1 j_1} \otimes c_{i_1 j_1}, \ldots, a_{i_k j_k} \otimes c_{i_k j_k}),$$

onde $g = g(x_1, \ldots, x_k)$ é multihomogêneo e é consequência de $f$. Novamente, pela primeira parte da demonstração, temos que todas as expressões $\bar{g}$ são nulas, por conseguinte, $f(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n}) = 0$

■

Observe que a partir desse resultado, temos que para $\mathbb{F}$ um corpo infinito o $T$-ideal de uma $\mathbb{F}$-álgebra $A$ é igual ao $T$-ideal da $\mathbb{K}$-álgebra $A \otimes_{\mathbb{F}} \mathbb{K}$, onde $\mathbb{K}$ denota o fecho algébrico de $\mathbb{F}$.

**Definição 2.28.** *Seja $f = f(x_1, \ldots, x_n, y_1, \ldots, y_t)$ um polinômio linear nas variáveis $x_1, \ldots, x_n$. Dizemos que $f$ é um polinômio alternado nas variáveis $x_1, \ldots, x_n$ se, para quaisquer $1 \leq i < j \leq n$, o polinômio $f$ se anula ao substituirmos $x_i$ por $x_j$.*

**Exemplo 2.29.** *O polinômio $f(x_1, x_2) = [x_1, x_2]$ é alternado nas variaveis $x_1$ e $x_2$.*

Veja que podemos definir uma ação de $S_n$ nos polinômios alternados nas variáveis $x_1, \ldots, x_n$ definindo

$$\sigma f(x_1, \ldots, x_n, y_1, \ldots, y_t) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}, y_1, \ldots, y_t) \quad \forall\ \sigma \in S_n.$$

**Proposição 2.30.** *Sejam $f$ um polinômio alternado nas variáveis $x_1, \ldots, x_n$ e $\varsigma \in S_n$ uma transposição, então $f = -\varsigma f$, ou seja,*

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, y_t) = -f(x_1, \ldots, x_j, \ldots, x_i, \ldots, y_t),$$

*onde $\varsigma = (ij)$.*

**Demonstração.** Suponhamos que $\varsigma = (ij)$. Então,

$$f + \varsigma f = f(x_1, \ldots, x_i, \ldots, x_j, \ldots, y_t) + f(x_1, \ldots, x_j, \ldots, x_i, \ldots y_t)$$

e pela linearidade de $f$ nas variáveis $x_1, \ldots, x_n$ podemos reescrever a equação acima na forma

$$\begin{aligned} f + \varsigma f = f(x_1, \ldots, x_i + x_j, \ldots, x_j + x_i, \ldots, y_t) - f(x_1, \ldots, x_i, \ldots, x_i, \ldots, y_t) \\ -f(x_1, \ldots, x_j, \ldots, x_j, \ldots y_t). \end{aligned}$$

Mas $f$ é um polinômio alternado, então por definição todas as parcelas acima são nulas e, por conseguinte, $f + \varsigma f = 0$, isto é, $f = -\varsigma f$.

■

Quando a característica de $\mathbb{F}$ é diferente de 2, a Definição 2.28 é equivalente a proposição acima, ou seja, se $f(x_1, \ldots, x_i, \ldots, x_j, \ldots y_t) = -f(x_1, \ldots, x_j, \ldots, x_i, \ldots, y_t)$, para todo $1 \leq i < j \leq n$ e $f$ é linear nas variáveis $x_1, \ldots, x_n$, então $f$ é alternado nas variáveis $x_1, \ldots, x_n$. Além disso, como qualquer permutação $\sigma \in S_n$ pode ser escrita como um produto de transposições, temos pelo resultado acima que

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(i)}, \ldots, x_{\sigma(j)}, \ldots, x_{\sigma(n)}, y_1, \ldots, y_t) = sgn(\sigma)\ f(x_1, \ldots x_n, y_1, \ldots, y_t).$$

**Observação 2.31.** *No caso em que $f$ for alternado em todas as suas variáveis, diremos simplesmente que $f$ é alternado.*

**Proposição 2.32.** *Sejam $f(x_1, \ldots, x_n, y_1, \ldots, y_t)$ um polinômio alternado nas variáveis $x_1, \ldots, x_n$ e $A$ uma $\mathbb{F}$-álgebra. Se $a_1, \ldots, a_n \in A$ são linearmente dependentes sobre $\mathbb{F}$, então*

$$f(a_1, \ldots, a_n, b_1, \ldots, b_t) = 0, \qquad \forall\ b_1, \ldots, b_t \in A.$$

**Demonstração.** Sendo os $a_i^{'}$s linearmente dependentes, sem perda de generalidade podemos supor que $a_1 = \sum_{i=2}^{n} \beta_i a_i$, com $\beta_i \in \mathbb{F}$. Assim, pelo o fato de $f$ ser linear nas variáveis $x_1, \ldots, x_n$, temos

$$f(a_1, \ldots, a_n, b_1, \ldots, b_t) = \sum_{i=2}^{n} \beta_i f(a_i, a_2, \ldots, a_n, b_1, \ldots, b_t).$$

Como em cada termo dois argumentos $a_i$ repetem nas variáveis $x_1, \ldots, x_n$ do polinômio $f$, o resultado segue do fato de $f$ ser alternado nas variáveis $x_1, \ldots, x_n$. ∎

**Definição 2.33.** *O polinômio*

$$St_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} sgn(\sigma)\ x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)}$$

*é chamado o polinômio standard de grau $n$.*

A seguir iremos expor algumas propriedades básicas do polinômio standard, com o objetivo de demonstrar que para uma $\mathbb{F}$-álgebra $A$ de dimensão $m$, qualquer polinômio standard de grau $> m$ é uma identidade polinomial para $A$.

Adotaremos a convenção de colocar o símbolo $\hat{}$ para denotar a omissão de uma variável, ou seja, $f(x_1, \ldots, \hat{x}_i, \ldots x_n)$ é um polinômio no qual a variável $x_i$ não aparece.

**Proposição 2.34.**

*(1) Se $f(x_1, x_2, \ldots, x_n)$ é um polinômio multilinear alternado de grau $n$, então $f = \alpha St_n(x_1, \ldots, x_n)$, para algum $\alpha \in \mathbb{F}$.*

*(2) $St_{n+1}(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{n+1} (-1)^{i+1} x_i St_n(x_1, \ldots, \hat{x}_i, \ldots, x_{n+1})$. Então se, $St_n$ é uma identidade polinomial para uma $\mathbb{F}$-álgebra $A$, temos que $St_{n+1}$ também é uma identidade polinomial para $A$.*

**Demonstração.**

(1) Sejam $\beta x_{i_1} x_{i_2} \ldots x_{i_n}$ um monômio não-nulo de $f$ e $\varsigma \in S_n$ uma transposição. Sendo $f$ um polinômio alternado, temos pela Proposição 2.30 que $f = -\varsigma f$ e, consequentemente, $\varsigma(\beta x_{i_1} x_{i_2} \ldots x_{i_n})$ aparece no polinômio $f$ com coeficiente $-\beta$. Então, como toda permutação $\sigma \in S_n$ pode ser escrita como um produto de transposições e sabemos que $\sigma f = sgn(\sigma) f$, temos que $\sigma(\beta x_{i_1} x_{i_2} \ldots x_{i_n})$ aparece em $f$ com coeficiente $sgn(\sigma)\beta \quad \forall\ \sigma \in S_n$. Portanto, o polinômio $St_n(x_1, \ldots, x_n)$ é um somando de $f$. Agora, como o mesmo acontece para todo monômio de $f$, temos que

$$f(x_1, x_2, \ldots, x_n) = \alpha St_n(x_1, \ldots, x_n), \qquad \text{onde } \alpha \in \mathbb{F}.$$

(2) Observe que podemos escrever $St_{m+1}$ na forma

$$St_{n+1}(x_1, \dots, x_{n+1}) = x_1 f_1 + \cdots + x_{n+1} f_{n+1},$$

onde $f_i = f_i(x_1, \dots, \hat{x_i}, \dots, x_{n+1})$ é um polinômio multilinear alternado de grau $n$. Então, pela parte 1, temos $f_i = \beta_i St_n(x_1, \dots, \hat{x_i}, \dots, x_{n+1})$ e comparando os monômios que aparecem em $St_{n+1}$ com os de cada $f_i'$ pode-se observar que $\beta_i = (-1)^{i+1}$.

■

**Teorema 2.35.** *Seja $A$ uma $\mathbb{F}$-álgebra com $dim_{\mathbb{F}} A = n < \infty$, então $St_{n+1}$ é uma identidade polinomial para $A$.*

**Demonstração.** Uma vez que o polinômio $St_{n+1}$ é multilinear, então, pela Proposição 2.15, basta garantirmos que $St_{n+1}$ se anula sobre todas as avaliações feitas a partir de uma base de $A$. Como $dim_{\mathbb{F}} A = n$ e $St_{n+1}$ é alternado em $n+1$ variáveis, o resultado segue imediatamente da Proposição 2.32. ■

Observe que a partir do resultado acima o polinômio standard $St_{n^2+1}$ é uma identidade polinomial para $M_n(\mathbb{F})$. Além disso, segue da Proposição 2.34 que os polinômios $St_m$ com grau $m \geq n^2+1$ são todos identidades polinomiais de $M_n(\mathbb{F})$. Desse modo, uma pergunta relevante a ser feita é: qual o menor valor de $m$ para o qual $St_m$ é uma identidade polinomial para $M_n(\mathbb{F})$?.

Nesse sentido, podemos observar que $M_n(\mathbb{F})$ não satisfaz nenhuma identidade polinomial de grau $< 2n$. De fato, suponhamos que $f$ é uma identidade polinomial para $M_n(\mathbb{F})$ de grau $< 2n$. Pelo o processo de multilinearização 2.16, podemos assumir que $f$ é multilinear. Além disso, multiplicando $f$ à direita por novas variáveis e então renomeando as variáveis de $f$ obtemos um novo polinômio que também é uma identidade polinomial para $M_n(\mathbb{F})$. Assim, podemos assumir que $gr(f) = 2n-1$ e escrever

$$f(x_1, \dots, x_{2n-1}) = \sum_{\sigma \in S_{2n-1}} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(2n-1)}$$

com $\alpha_1 \neq 0$. Então, computamos $f(e_{11}, e_{12}, e_{22}, \dots, e_{n-1n}, e_{nn}) = \alpha_1 e_{1n} \neq 0$ e concluímos que $f$ não é uma identidade polinomial para $M_n(\mathbb{F})$, o que é uma contradição. Dessa forma, concluímos que realmente $M_n(\mathbb{F})$ não satisfaz nenhuma identidade polinomial de grau $< 2n$.

Entretanto, para identidades polinomiais de grau $2n$, o famoso resultado de Amitsur e Levitzki, que será enunciado a seguir, estabelece que o polinômio standard de grau $2n$ é uma identidade polinomial para $M_n(\mathbb{F})$ e pelo o que foi observado acima ela é a identidade de menor grau para $M_n(\mathbb{F})$.

**Teorema 2.36.** *(Amitsur e Levitzki, [3]) O polinômio standard de grau $2n$*

$$St_{2n}(x_1, \ldots, x_{2n}) = \sum_{\sigma \in S_{2n}} sgn(\sigma) x_{\sigma(1)} \ldots x_{\sigma(2n)}$$

*é uma identidade polinomial para a álgebra de matrizes $M_n(\mathbb{F})$, e $M_n(\mathbb{F})$ não satisfaz nenhum polinômio de grau menor que $2n$. Além disso, se $Char(\mathbb{F}) > 2$ ou $n > 2$, então, a menos de um múltiplo escalar, $St_{2n}$ é a única identidade multilinear de grau $2n$ satisfeita por $M_n(\mathbb{F})$.*

Terminamos este capítulo ressaltando que o $T$-ideal da álgebra de matrizes $M_n(\mathbb{F})$ não é totalmente conhecido. Drensky, em [7], provou que

$$Id(M_2(\mathbb{F})) = \left\langle [[x_1, x_2]^2, x_3], St_4(x_1, x_2, x_3, x_4) \right\rangle_T .$$

Porém, ainda não são conhecidos os geradores de $Id(M_n(\mathbb{F}))$, para todo $n \geq 3$.

# Capítulo 3

# $*$-Identidades polinomiais

Nesse capítulo iremos definir as álgebras com involução e apresentar alguns exemplos, entre eles, apresentaremos a álgebra de matrizes com involução simplética, cujo estudo das suas $*$-identidades (que definiremos ao longo do capítulo) é o objetivo principal dessa dissertação. A fim de explicitar a importância desse estudo iremos também caracterizar as involuções da álgebra de matrizes $n \times n$. Em todo o capítulo, $\mathbb{F}$ denotará um corpo com característica 0.

## 3.1 Álgebras com involução

Nessa seção faremos um breve estudo das álgebras com involução e daremos alguns exemplos importantes para o desenvolvimento dos principais resultados do capítulo.

**Definição 3.1.** *Seja $A$ uma $\mathbb{F}$-álgebra. Uma aplicação $* : A \longrightarrow A$ é dita uma involução de $A$, se para quaisquer $a, b \in A$ e $\lambda \in \mathbb{F}$, temos:*
*i_* $(a+b)^* = a^* + b^*$
*ii_* $(\lambda a)^* = \lambda a^*$
*iii_* $(ab)^* = b^* a^*$
*iv_* $(a^*)^* = a.$

Denotaremos uma $\mathbb{F}$-álgebra $A$ com involução $*$ por $(A, *)$ e omitiremos a involução quando não houver dúvidas sobre a involução considerada.

Observe, ainda que se a $\mathbb{F}$-álgebra $A$ com involução tem unidade, então $1^*a = (a^*1)^* = a$ e $a = (a^*)^* = (1.a^*)^* = a1^*$, ou seja, $1^* = 1$.

**Exemplo 3.2.** *Seja $A$ uma $\mathbb{F}$-álgebra comutativa. A aplicação identidade definida em $A$ satisfaz as condições da Definição 3.1 e portanto é uma involução de $A$. Observe ainda* *que a aplicação identidade é uma involução apenas para as álgebras comutativas e é usualmente denominada a involução trivial.*

**Exemplo 3.3.** *Seja $D = F \oplus F$. Definindo*

$$\begin{aligned} * : A &\longrightarrow A \\ (x, y) &\longmapsto (y, x) \end{aligned}$$

*podemos observar que $*$ satisfaz as condições da Definição 3.1. Portanto, $F \oplus F$ é uma álgebra comutativa com involução diferente da involução trivial.*

**Exemplo 3.4.** *Seja $M_n(\mathbb{F})$ a álgebra de Matrizes $n \times n$ sobre $\mathbb{F}$. Definindo a transposta por*

$$\begin{aligned} t : M_n(\mathbb{F}) &\longrightarrow M_n(\mathbb{F}) \\ (x_{ij}) &\longmapsto (x_{ji}) \end{aligned}$$

*podemos observar que $t$ satisfaz as condições da Definição 3.1. Portanto, $M_n(\mathbb{F})$ é uma álgebra com involução transposta.*

**Definição 3.5.** *Sejam $(A_1, *)$ e $(A_2, j)$ duas álgebras com involução. Um homomorfismo com involução é um homomorfismo de $\mathbb{F}$-álgebras $\varphi : (A_1, *) \longrightarrow (A_2, j)$ que satisfaz $\varphi(a^*) = \varphi(a)^j$.*

Veremos a seguir que a partir de uma involução $*$ de uma álgebra $A$ podemos construir uma nova involução para $A$. Usando essa construção iremos obter para a álgebra $M_{2m}(\mathbb{F})$, $m \leq 1$, a partir da involução transposta, uma nova involução chamada de **involução simplética canônica**, que é a involução com a qual estamos interessados em trabalhar.

**Proposição 3.6.** *Seja $(A, *)$ com unidade e $u \in U(A)$, tal que $u \in A^+ \cup A^-$. Então a aplicação $j$ definida por*

$$\begin{aligned} j : A &\longrightarrow A \\ a &\longmapsto ua^*u^{-1} \end{aligned}$$

*é uma involução.*

**Demonstração.** É fácil ver que a aplicação j satisfaz as condições da Definição 3.1 e portanto $j$ é de fato uma involução.

■

Observe que dada uma matriz $M \in M_{2m}(\mathbb{F})$ podemos escrevê-la na forma

$$M = \begin{pmatrix} R & S \\ P & Q \end{pmatrix}, \qquad \text{onde} \quad R, S, P, Q \in M_m(\mathbb{F}).$$

Mantendo essa partição em mente, consideramos $U = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$ (em que $I_m$ denota a matriz identidade $m \times m$) e definimos, usando a involução transposta $t$, a aplicação

$$\begin{aligned} s : & M_{2m}(\mathbb{F}) \longrightarrow M_{2m}(\mathbb{F}) \\ & M \longmapsto UM^tU^{-1} \end{aligned}$$

que pela proposição anterior é uma involução. Essa involução é usualmente denominada por **involução simplética canônica**, entretanto iremos nos referir a ela apenas por **involução simplética** e trabalharemos com essa involução usando a sua forma explícita dada pela fórmula:

$$\begin{pmatrix} R & S \\ P & Q \end{pmatrix}^s = \begin{pmatrix} Q^t & -S^t \\ -P^t & R^t \end{pmatrix}, \qquad \text{onde} \quad R, S, P, Q \in M_m(\mathbb{F}).$$

É importante observar que a involução simplética está definida somente para matrizes de ordem par.

**Definição 3.7.** *Seja $(A, *)$ uma $\mathbb{F}$-álgebra com involução. Dizemos que $a \in A$ é um elemento simétrico se $a^* = a$ e que é antissimétrico se $a^* = -a$.*

Denotaremos o conjunto dos elementos simétricos de $A$ por $(A, *)^+ = \{a \in A |\ a^* = a\}$ e o conjuntos dos elementos antissimétricos por $(A, *)^- = \{a \in A |\ a^* = -a\}$ (omitiremos a involução na notação quando não houver possibilidade de confusão ).

Observe que os conjuntos definidos acima são na verdade subespaços vetoriais de $A$ e que, $A^+ \cap A^- = \{0\}$. Além disso, temos que para todo $a \in A$

$$a = \frac{a + a^*}{2} + \frac{a - a^*}{2}$$

e portanto $A = A^+ \dot{+} A^-$.

**Exemplo 3.8.** *Para as $\mathbb{F}$-álgebras com involução $(M_n(\mathbb{F}), t)$ e $(M_{2m}(\mathbb{F}), s)$, temos que:*

*Para $(M_n(\mathbb{F}), t)$:*

- *$M_n(\mathbb{F})^+$ é um subespaço de dimensão $\frac{1}{2}n(n+1)$ com base*

$$\{e_{ij} + e_{ji} | 1 \leq i < j \leq n\} \cup \{e_{ii} | 1 \leq i \leq n\}.$$

- $M_n(\mathbb{F})^-$ *é um subespaço de dimensão* $\frac{1}{2}n(n-1)$ *com base*

$$\{e_{ij} - e_{ji} | 1 \leq i < j \leq n\}.$$

*Por outro lado, para a* $\mathbb{F}$*-álgebra* $(M_{2m}(\mathbb{F}), s)$*, temos que:*

- $M_{2m}(\mathbb{F})^+$ *é um subespaço de dimensão* $m(2m-1)$ *com base*

  $\{e_{i,j} + e_{j+m,i+m} | 1 \leq i, j \leq m\} \cup \{e_{i,j+m} - e_{j,i+m} | 1 \leq i < j \leq m\} \cup$
  $\{e_{i+m,j} - e_{j+m,i} | 1 \leq i < j \leq m\}$

- $M_{2m}(\mathbb{F})^-$ *é um subespaço de dimensão* $m(2m+1)$ *com base*

  $\{e_{i,j} - e_{j+m,i+m} | 1 \leq i, j \leq m\} \cup \{e_{i,j+m} + e_{j,i+m} | 1 \leq i < j \leq m\} \cup \{e_{i,i+m} | 1 \leq i \leq m\} \cup$
  $\{e_{i+m,j} + e_{j+m,i} | 1 \leq i < j \leq m\} \cup \{e_{j+m,j} | 1 \leq j \leq m\}.$

Observe que apesar da involução simplética de $M_{2m}(\mathbb{F})$ ser obtida através da involução transposta de $M_{2m}(\mathbb{F})$, os espaços de elementos simétricos e antissimétricos com relação a involução simplética são diferentes dos mesmos espaços obtidos com relação a involução transposta.

## 3.2 Caracterização das involuções de $M_n(\mathbb{F})$

Nessa seção iremos restringir o nosso estudo das involuções para as involuções da álgebra de matrizes $M_n(\mathbb{F})$ com o intuito de caracterizar todas as involuções dessa álgebra.

Dado uma $\mathbb{F}$-álgebra $A$ com unidade e $u \in U(A)$, definimos o automorfismo interno de $A$ induzido por $u$ como sendo

$$\begin{aligned} Int(u) : A &\longrightarrow A \\ a &\longmapsto u^{-1}au. \end{aligned}$$

Na Proposição 3.6, vimos que dada uma involução $*$, para todo $u \in U(A)$ tal que $u \in A^+ \cup A^-$, $j = Int(u^{-1}) \circ *$ é uma involução. A seguir vamos mostrar que a recíproca dessa proposição é válida quando a álgebra considerada é a álgebra de matrizes $M_n(\mathbb{F})$.

**Definição 3.9.** *Sejam* $A$ *uma* $\mathbb{F}$*-álgebra e* $\sigma$ *um automorfismo de* $A$*. Dizemos que* $\sigma$ *é um automorfismo interno de* $A$ *se* $\sigma = Int(u)$*, para algum* $u \in U(A)$*.*

**Teorema 3.10.** *Todo $\mathbb{F}$-automorfismo $\sigma$ de $M_n(\mathbb{F})$ é interno.*

**Demonstração.** Considere $\mathbb{F}^n$ o $M_n(\mathbb{F})$-módulo sob ação natural

$$M_n(\mathbb{F})\times\mathbb{F}^n \longrightarrow \mathbb{F}^n$$

$$(X,v) \longmapsto X.v$$

e $\mathbb{F}^n$ o $M_n(\mathbb{F})$-módulo com o produto induzido pelo automorfismo $\sigma : M_n(\mathbb{F}) \longrightarrow M_n(\mathbb{F})$

$$M_n(\mathbb{F})\times\mathbb{F}^n \longrightarrow \mathbb{F}^n$$

$$(X,v) \longmapsto \sigma(X).v.$$

Como vimos no Exemplo 1.5, os $M_n(\mathbb{F})$-módulos $\mathbb{F}^n$, com as ações assim definidas, são simples e, pela Proposição 1.9, são também isomorfos, ou seja, existe um $M_n(\mathbb{F})$-isomorfismo $\varphi : \mathbb{F}^n \longrightarrow \mathbb{F}^n$. Considerando a matriz $Y \in GL_n(\mathbb{F})$ que representa esse isomorfismo, obtemos

$$Y.X.v = \varphi(X.v) = \sigma(X)\varphi(v) = \sigma(X).Y.v \quad \forall\ v \in \mathbb{F}^n$$

e, consequentemente, $\sigma(X) = Y^{-1}XY \quad \forall\ X \in M_n(\mathbb{F})$.

■

**Lema 3.11.** *Sejam $*$ e $j$ duas involuções de $M_n(\mathbb{F})$. Se $* = Int(U)\circ j$, com $U \in GL_n(\mathbb{F})$, então $U^* = U^j = \pm U$.*

**Demonstração.** Observe que

$$* = Int(U) \circ j \Leftrightarrow * \circ j = Int(U) \Leftrightarrow j = * \circ Int(U).$$

Por outro lado,

$$* \circ Int(U)\ (X) = (U^{-1}XU)^* = U^*X^*(U^{-1})^* = Int(U^{-1^*}) \circ *\ (X) \quad \forall\ X \in M_n(\mathbb{F}).$$

Logo, $* \circ Int(U) = Int((U^*)^{-1}) \circ *$ e retornando na primeira equação, obtemos

$$j = * \circ Int(U) = Int((U^*)^{-1}) \circ * = Int((U^*)^{-1}) \circ Int(U) \circ j \Rightarrow Int((U^*)^{-1}) \circ Int(U) = id.$$

Portanto, $Int(U(U^{-1})^*) = id$ e, por conseguinte, $U(U^{-1})^* \in Z(M_n(\mathbb{F}))$, isto é, $U^* = zU$, para algum $z \in Z(M_n(\mathbb{F}))$. Desse modo,

$$U = (U^*)^* = (zU)^* = U^*z^* = zUz^* = Uzz^*,$$

como $Z(M_n(\mathbb{F})) = \{\lambda I_n \mid \lambda \in \mathbb{F}\}$, temos que $U = Uz^2$ e portanto $z = I$ ou $z = -I$, ou seja, $U^* = \pm U$. Agora, de $j = Int(U) \circ *$, segue que $U^j = U^* = \pm U$.

■

**Teorema 3.12.** *Sejam $*$ e $j$ duas involuções quaisquer de $M_n(\mathbb{F})$. Então, existe $U \in GL_n(\mathbb{F})$ tal que $* = Int(U) \circ j$ e $U^* = \pm U$ .*

**Demonstração.** Sendo $*$ e $j$ involuções de $M_n(\mathbb{F})$, temos que $* \circ j$ é um $\mathbb{F}$-automorfismo de $M_n(\mathbb{F})$. Então, pelo Teorema 1.9, temos que $* \circ j = Int(U)$, para algum $U \in U(M_n(\mathbb{F}))$. Então, $* = Int(U) \circ j$, para algum $U \in U(M_n(\mathbb{F}))$ e, pelo lema anterior, $U^* = \pm U$, donde segue o resultado.

∎

Denotaremos por $Inv(M_n(\mathbb{F}))$ o conjunto de todas as involuções de $M_n(\mathbb{F})$. Em $Inv(M_n(\mathbb{F}))$ definiremos uma relação $([21], pg - 168)$ da seguinte maneira:

Sejam $*$, $j \in Inv(M_n(\mathbb{F}))$. Dizemos que $*$ e $j$ são equivalentes, e denotamos por $* \sim j$, se $* = Int(r) \circ j$ para algum $r \in (M_n(\mathbb{F}), *)^+ \cap GL_n(\mathbb{F})$.

**Proposição 3.13.** *A relação definida acima é uma relação de equivalência em $Inv(M_n(\mathbb{F}))$.*

**Demonstração.** De fato, A relação é reflexiva, uma vez que $* = int(1) \circ *$; a relação é simétrica, já que $* = int(u) \circ j \Rightarrow j = int(u^{-1}) \circ *$ e temos $u, u^{-1} \in (M_n(\mathbb{F}), *)^+$; a relação é transitiva, pois se $* = int(u_1) \circ j$ e $j = int(u_2) \circ k$, com $u_1 \in (M_n(\mathbb{F}), *)^+$ e $u_2 \in (M_n(\mathbb{F}), j)^+$, então $* = int(u_2 u_1) \circ k$ e $(u_2 u_1)^* = u_1^* u_2^* = u_1 u_2^{int(u_1) \circ j} = u_1 (u_1)^{-1} u_2^j u_1 = u_2 u_1$. Desse modo, concluímos que a relação é realmente uma relação de equivalência.

∎

**Teorema 3.14.**

1. *A relação de equivalência definida acima em $Inv(M_n(\mathbb{F}))$ determina no máximo duas classes de equivelência.*

2. *Se $*, j \in Inv(M_n(\mathbb{F}))$ e $* = Int(Y) \circ j$, para algum $Y \in (M_n(\mathbb{F}), *)^- \cap GL_n(\mathbb{F})$, então $*$ e $j$ não são equivalentes.*

**Demonstração.** A fim de provar o primeiro item consideremos $j_1, j_2, j_3 \in Inv(M_n(\mathbb{F}))$. Afirmamos que duas delas são equivalentes.

De fato, pelo Teorema 3.11, existem $U_1, U_2 \in GL_n(\mathbb{F})$ tais que

$$j_1 = Int(U_1) \circ j_2; \;\; j_2 = Int(U_2) \circ j_3 \;\text{ e }\; U_i^{j_i} = \pm U, \text{ para } i = 1, 2.$$

. Assim temos os seguintes casos:

- Caso $U_1^{j_1} = U_1$ então, pela definição da relação de equivalência, $j_1 \sim j_2$.

- Caso $U_2^{j_2} = U_2$ então, pela definição da relação de equivalência, $j_2 \sim j_3$.

- Caso $U_1^{j_1} = -U_1$ e $U_2^{j_2} = -U_2$. Segue de $j_1 = Int(U_1) \circ j_2$ e $j_2 = Int(U_2) \circ j_3$ que

$$j_1 = Int(U_1) \circ Int(U_2) \circ j_3 = Int(U_2U_1) \circ j_3.$$

Por outro lado, $U_2^{j_2} = -U_2$ e $j_1 = Int(U_1) \circ j_2$ implica em

$$U_2^{j_1} = U_1^{-1}U_2^{j_2}U_1 = -U_1^{-1}U_2U_1,$$

então $(U_2U_1)^{j_1} = U_1^{j_1}U_2^{j_1} = (-U_1)(-U_1^{-1}U_2U_1) = U_2U_1$.

Portanto, $j_1 \sim j_3$.

Concluímos que dadas $j_1, j_2, j_3 \in Inv(M_n(\mathbb{F}))$ duas delas são sempre equivalentes, logo temos no máximo duas classes de equivalência em $Inv(M_n(\mathbb{F}))$.

Agora, para provar o segundo item consideremos $*, j \in Inv(M_n(\mathbb{F}))$ tais que $* = Int(Y) \circ j$, para algum $Y \in (M_n(\mathbb{F}), *)^- \cap GL_n(\mathbb{F})$. Suponhamos por absurdo que $* \sim j$, então existe $U \in (M_n(\mathbb{F}), *)^+ \cap GL_n(\mathbb{F})$ tal que $* = Int(U) \circ j$. Desse modo, $Int(Y) \circ j = Int(U) \circ j$ e portanto $Int(YU^{-1}) = id$. Obtemos assim, $YU^{-1} \in Z(M_n(\mathbb{F})) \cong \mathbb{F}$ e em particular

$$(YU^{-1})Y = Y(YU^{-1}) \Rightarrow Y(U^{-1}Y - YU^{-1}) = 0 \Rightarrow U^{-1}Y - YU^{-1} = 0 \Rightarrow U^{-1}Y = YU^{-1},$$

então

$$(YU^{-1})^* = U^{-1*}Y^* = U^{-1}Y^* = -U^{-1}Y = -YU^{-1},$$

o que contradiz o fato de $YU^{-1} \in Z(M_n(\mathbb{F})) \cong \mathbb{F}$. Assim, concluímos que $*$ e $j$ não são equivalentes.

■

**Corolário 3.15.** *As involuções transposta e simplética, definidas na seção anterior, de $M_{2m}(F)$ não são equivalentes.*

**Demonstração.** Segue do teorema anterior, pois $s = Int(U) \circ t$, onde $U = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ e $U \in (M_{2m}(\mathbb{F}), s)^- \cap GL_{2m}(\mathbb{F})$. ■

**Corolário 3.16.** *$Inv(M_n(\mathbb{F}))$ tem duas classes de equivalência quando $n$ for par e apenas uma quando $n$ for ímpar.*

**Demonstração.** Pelo teorema anterior, $M_n(\mathbb{F})$ tem, no máximo, duas classes de equivalência.

Quando $n$ for par, pelo corolário anterior $M_n(\mathbb{F})$ tem exatamente duas classes de equivalência determinadas por $t$ e $s$.

Quando $n$ for ímpar, como $(M_n(\mathbb{F}), t)^- \cap GL_n((\mathbb{F}) = \emptyset$. Então, pelos Teoremas 3.11 e 3.12, temos que $M_n(\mathbb{F})$ tem apenas uma classe de equivalência.

■

Desse modo, toda involução de $M_n(\mathbb{F})$ ou é equivalente a involução transposta, ou é equivalente a involução simplética e assim obtemos a caracterização das involuções de $M_n(\mathbb{F})$.

## 3.3 $*$-Identidades de uma $\mathbb{F}$-álgebra

Nessa seção iremos apresentar a $\mathbb{F}$-álgebra livre associativa unitária com involução e caracterizar o conjunto das $*$-identidades de $(M_n(\mathbb{F}), *)$, a fim de evidenciar a importância do estudo das $*$-identidades polinomiais de $(M_n(\mathbb{F}), s)$, que é o objetivo principal dessa dissertação.

Seja $X = \{x_1, x_2, ...\}$ um conjunto infinito e enumerável de variáveis não comutativas. Denotamos por $\mathbb{F}\langle X, *\rangle$ a álgebra associativa unitária com involução livremente gerada por $Z = \{x_1, x_1^*, x_2, x_2^*, \dots\}$, onde a involução $*$ em $\mathbb{F}\langle X, *\rangle$ é definida como sendo a extensão linear da aplicação:

$$
\begin{aligned}
* : \mathbb{F}\langle X, *\rangle &\longrightarrow \mathbb{F}\langle X, *\rangle \\
x_i &\longmapsto x_i^* \\
x_i^* &\longmapsto x_i
\end{aligned}
$$

tal que para $k \geq 2 \quad (x_{i_1}^{\alpha_{i_1}} x_{i_2}^{\alpha_{i_2}} \dots x_{i_k}^{\alpha_{i_k}})^* = (x_{i_k}^{\alpha_{i_k}})^* (x_{i_2}^{\alpha_{i_2}})^* \dots (x_{i_1}^{\alpha_{i_1}})^*, \quad$ em que $\alpha_{i_j} \in \{1, *\}$.

Os elementos de $\mathbb{F}\langle X, *\rangle$ usualmente são denominados $*$-polinômios e podem ser escritos da forma

$$
f(x_1, x_1^*, x_2, x_2^*, \dots, x_n, x_n^*) = \sum_{j,\alpha} \beta_{j,\alpha}\ x_{j_1}^{\alpha_1} x_{j_2}^{\alpha_2} \dots x_{j_m}^{\alpha_m},
$$

onde $\beta_{j,\alpha} \in \mathbb{F}$ e $\alpha_i \in \{1, *\}$.

Se $f \in \mathbb{F}\langle X, *\rangle$ vamos escrever $f = f(x_1, x_1^*, x_2, x_2^*, \dots, x_n, x_n^*)$ indicando que $x_1, x_2, \dots x_n$ são as únicas variáveis que aparecem em $f$ com involução ou não.

**Definição 3.17.** *Seja* $f = f(x_1, x_1^*, x_2, x_2^*, \dots, x_n, x_n^*) \in \mathbb{F}\langle X, *\rangle$.

*i) Seja* $h$ *um* $*$*-monômio de* $f$. *Definimos o grau de* $x_i$ *em* $h$, *denotado por* $deg_{x_i}(h)$, *como sendo o número de ocorrências das variáveis* $x_i^{\alpha_i}$ *em* $h$ *onde* $\alpha_i \in \{1, *\}$.

*ii) O grau de* $x_i$ *em f, denotado por* $deg_{x_i}(f)$, *é definido como o maior* $deg_{x_i}(h)$ *dentre todos os* $*$*-monômios de* $f$.

*iii) O grau de um* $*$*-monômio* $h$, *denotado por* $deg(h)$, *é definido como sendo*

$$deg(h) = \sum_{i=1}^{n} deg_{x_i}(h)$$

.

*iv) O grau de* $f$, *denotado por* $deg(f)$, *é definido como sendo o maior valor de* $deg(h)$ *dentre todos os* $*$*-monômios de* $f$.

**Exemplo 3.18.** *Consideremos os* $*$*-polinômios:*

$$f = f(x_1, x_1^*, x_2, x_2^*, x_3, x_3^*) = 2x_1^2 x_3 {x_1^*}^4 x_2 x_1 + 3x_1 {x_2^*}^3 x_1^* x_3 x_2$$

$$g = g(x_1, x_1^*, x_2, x_2^*, x_3, x_3^*) = x_1 x_2^* x_3 + x_1 x_2 x_3^* + x_1 x_2 x_3$$

$$l = l(x_1, x_1^*, x_2, x_2^*, x_3, x_3^*) = {x_1^*}^3 {x_2^*}^2 x_1 x_3 + x_1 x_2 x_3^* x_1^2 x_1^* x_2$$

*temos que* $deg_{x_1}(f) = 7$; $deg_{x_2}(g) = 4$; $deg_{x_3}(l) = 1$; $deg(f) = 9$; $deg(g) = 3$; $deg(l) = 7$.

**Definição 3.19.** *Seja* $f$ *um* $*$*-polinômio. Com base na definição anterior:*

*i) Dizemos que* $f$ *é um polinômio homogêneo na variável* $x_i$ *quando* $deg_{x_i}(h)$ *é igual para todo* $*$*-monômio* $h$ *de* $f$.

*ii) Dizemos que* $f$ *é um polinômio multihomogêneo quando é homogêneo em cada uma das suas variáveis.*

*iii) Dizemos que* $f$ *é um polinômio linear na variável* $x_i$ *quando* $deg_{x_i}(h) = 1$ *para todo* $*$*-monômio* $h$ *de* $f$.

*iv) Dizemos que* $f$ *é um polinômio multilinear quando é linear em cada uma das suas variáveis.*

Analisando os polinômios do exemplo anterior podemos observar que o polinômio $f$ é linear na variável $x_3$, o polinômio $g$ é multilinear e o polinômio $l$ é multihomogêneo.

**Observação 3.20.** *Dado $f(x_1, x_1^*, \ldots, x_n, x_n^*)$ um $*$-polinômio qualquer, podemos sempre supor que $f$ é um polinômio em variáveis simétricas ou antissimétricas. Para tanto, basta observarmos que caso apareça em $f$ uma variável ${x_i}^{\alpha_i}$ ($\alpha_i \in \{1, *\}$) que não é simétrica ou antissimétrica, então podemos reescrevê-la na forma*

$$x_i^{\alpha_i} = \frac{y_i + z_i}{2},$$

*em que $y_i = {x_i}^{\alpha_i} + ({x_i}^{\alpha_i})^*$ é a parte simétrica de ${x_i}^{\alpha_i}$ e $z_i = {x_i}^{\alpha_i} - ({x_i}^{\alpha_i})^*$ é a parte antissimétrica de ${x_i}^{\alpha_i}$. Fazendo isso para todas as variáveis de $f$, obtemos $f$ como um polinômio nas variáveis $y_1, \ldots, y_n, z_1, \ldots z_n$, isto é, obtemos $f$ como um polinômio em variáveis simétricas ou antissimétricas. Desse modo, podemos ver $\mathbb{F}\big\langle X, *\big\rangle$ como sendo gerada por variáveis simétricas e antissimétricas, isto é, $\mathbb{F}\big\langle X, *\big\rangle = \mathbb{F}\langle Y \cup Z\rangle$. Nesse caso, as noções de polinômios multihomogêneos e multilineares são dadas da mesma forma que no caso ordinário, considerando, para cada $i \geq 1$, $y_i$ e $z_i$ como sendo variáveis distintas.*

**Definição 3.21.** *Dados $(A, *)$ e $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in \mathbb{F}\big\langle X, *\big\rangle$. Dizemos que $f$ é uma $*$-identidade de $A$, se*

$$f(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m) = 0,$$

*para quaisquer $a_1, a_2, \ldots, a_n \in A^+$ e $b_1, b_2, \ldots, b_m \in A^-$.*

**Exemplo 3.22.** *Os polinômios $f(y_1, z_2, z_3) = [z_2 z_3, y_1]$ e $g(z_1, z_2) = [z_1, z_2]$ são $*$-identidades para $(M_2(\mathbb{F}), t)$. Enquanto que o polinômio $h(y_1, z_2) = [y_1, z_2]$ é uma $*$-identidade para $(M_2(\mathbb{F}), s)$.*

**Definição 3.23.** *Dada uma $\mathbb{F}$-álgebra com involução $(A, *)$ definimos*

$$id(A, *) = \{f \in \mathbb{F}\big\langle X, *\big\rangle | f \text{ é uma} *\text{-identidade de } A\}$$

*como sendo o conjunto das $*$-identidades de $A$.*

Definimos no segundo capítulo o conceito de $T$-ideais e vimos que o ideal das identidades polinomiais de uma $\mathbb{F}$-álgebra são $T$-ideais. Podemos estender esse conceito para as $\mathbb{F}$-álgebras com involução através dos $T^*$-ideias, que são os ideais da álgebra livre $\mathbb{F}\big\langle X, *\big\rangle$ invariantes sob todos os $*$-endomorfismos de $\mathbb{F}\big\langle X, *\big\rangle$. A partir dessa definição podemos ver que o conjunto $id(A, *)$ de uma $\mathbb{F}$-álgebra $A$ é um $T^*$-ideal de $\mathbb{F}\big\langle X, *\big\rangle$ e, reciprocamente, todo $T^*$-ideal de $\mathbb{F}\big\langle X, *\big\rangle$ é um conjunto de $*$-identidades para alguma álgebra com involução.

A seguir iremos caracterizar os $T^*$- ideais das $\mathbb{F}$-álgebras de matrizes com involução. Apesar de, pela Proposição 2.27, não precisarmos exigir que o corpo $\mathbb{F}$ seja algebricamente fechado para que os resultados a seguir sejam válidos, vamos fazer essa restrição a fim de simplificar os mesmos.

**Lema 3.24.** *Seja $\mathbb{F}$ um corpo algebricamente fechado. Se $U \in GL_n(F)$, então existe $p(x) \in \mathbb{F}[x]$ tal que $U = p(U)^2$.*

**Demonstração.**

Ver $([21], pg - 169)$.

■

**Teorema 3.25.** *Seja $* \in Inv(M_n(\mathbb{F}))$ uma involução equivalente a involução transposta (resp. simplética). Então $(M_n(\mathbb{F}), *) \cong (M_n(\mathbb{F}), t)$ $(resp.(M_n(\mathbb{F}), *) \cong (M_n(\mathbb{F}), s))$.*

**Demonstração.** Suponhamos que $*$ é equivalente a involução transposta, então $* = Int(U) \circ t$, para algum $U \in (M_n(\mathbb{F}), s)^+ \cap GL_n(\mathbb{F})$. Observe que, $U^* = U^t = U$ e, pelo lema anterior, existe $p(x) \in \mathbb{F}[x]$ tal que $U = p(U)^2$. Denotando $U_0 = p(U)$ segue, das primeiras observações, que $U_0^* = U_0^t = U_0$. Definindo o $\mathbb{F}$-isomorfismo de álgebras

$$\begin{aligned} \varphi : (M_n(\mathbb{F}), t) &\longrightarrow (M_n(\mathbb{F}), *) \\ X &\longmapsto U_0^{-1} X U_0, \end{aligned}$$

temos que

$$\begin{aligned} \varphi(X^t) &= U_0^{-1} X^t U_0 \\ &= U_0^{-1} U X^* U^{-1} U_0 \\ &= U_0^{-1} U_0^2 X^* (U_0^{-1})^2 U_0 \\ &= U_0 X^* U_0^{-1} \\ &= (U_0^{-1} X U_0)^* \\ &= \varphi(X)^*, \end{aligned}$$

isto é, $\varphi$ é um $*$-isomorfismo, o que encerra a demonstração.

Caso $*$ seja equivalente a involução simplética a demonstração segue de forma análoga.

■

**Corolário 3.26.** *Seja* $\mathbb{F}$ *um corpo algebricamente fechado e* $Id(M_n(\mathbb{F}), *)$ *o* $T^*$*-ideal de* $(M_n(\mathbb{F}), *)$*. Então* $Id(M_n(\mathbb{F}), *) = Id(M_n(\mathbb{F}), t)$ *ou* $Id(M_n(\mathbb{F}), *) = Id(M_n(\mathbb{F}), s)$*.*

**Demonstração.** Sabemos pelo o que foi discutido na seção anterior que $*$ ou é equivalente a involução transposta, ou é equivalente a involução simplética. Dessa forma, pelo teorema anterior, $(M_n(\mathbb{F}), *) \cong (M_n(\mathbb{F}), t)$ ou $(M_n(\mathbb{F}), *) \cong (M_n(\mathbb{F}), s)$, logo $Id(M_n(\mathbb{F}), *) = Id(M_n(\mathbb{F}), t)$ ou $Id(M_n(\mathbb{F}), *) = Id(M_n(\mathbb{F}), s)$. ∎

Concluímos com as últimas duas seções, que para estudarmos as identidades polinomiais de $(M_n(\mathbb{F}), *)$, com $*$ uma involução qualquer, é suficiente estudarmos as identidades polinomiais de $(M_n(\mathbb{F}), s)$ e $(M_n(\mathbb{F}), t)$. Deixando evidente a importância do estudo desses dois casos.

# Capítulo 4

# As $*$-identidades de grau mínimo para $(M_{2m}(\mathbb{F}), s)^+$

No capítulo anterior vimos a importância de se conhecer as $*$-identidades de $(M_n(\mathbb{F}), s)$. Nas duas primeiras seções desse capítulo iremos estudar, baseando-se no artigo [11], as $*$-identidades de $(M_n(\mathbb{F}), s)$ em variáveis simétricas, concentrando-se no problema de se encontrar $*$-identidades em variáveis simétricas de grau mínimo, problema esse que já se encontra completamente resolvido para $m = 1, 2$ e 3, porém permanece em aberto para $m > 3$. Nas últimas seções iremos expor a construção de uma base, feita em [14], que tem propriedades interessantes de serem estudadas no contexto da involução simplética de $M_{2^m}(\mathbb{C})$.

## 4.1 Resultados conhecidos

Nessa seção iremos estabelecer as cotas conhecidas para o grau de uma $*$-identidade em variáveis simétricas de $(M_{2m}(\mathbb{F}), s)$ .

No Teorema 2.35 vimos que pelo fato de $M_n(\mathbb{F})$ ser uma $\mathbb{F}$-álgebra de dimensão $n^2$, $M_n(\mathbb{F})$ satisfaz uma identidade polinomial de grau $n^2+1$. Então, em particular $(M_n(\mathbb{F}), s)$ também satisfaz uma $*$-identidade em variáveis simétricas de grau $n^2 + 1$.

Ainda no Capítulo 2, vimos o teorema de Amitsur-Levitzki que estabelece o grau mínimo de uma identidade polinomial para $M_n(\mathbb{F})$. Por esse teorema, temos que $St_{4m}$ é uma identidade para $M_{2m}(\mathbb{F})$. Entretanto, observe que apesar de esse ser o grau mínimo para uma identidade polinomial de $M_{2m}(\mathbb{F})$, o mesmo não pode ser dito para o grau mínimo de uma $*$-identidade em variáveis simétricas satisfeita por $(M_{2m}(\mathbb{F}), s)$. De fato, veremos a seguir que esse grau pode ser melhorado com o resultado estabelecido por Rowen, em [19].

**Teorema 4.1.** *Seja $m$ um inteiro positivo. Então, $St_{4m-2}(y_1, \ldots, y_{4m-2})$ é uma $*$- identidade polinomial para $(M_{2m}(\mathbb{F}), s)$.*

Para provar esse teorema, Rowen usou uma $*$-identidade polinomial de $(M_{2m}(\mathbb{F}), s)$ ([21], pg.139), denominada o polinômio mínimo genérico e definido por:

$$Y^m + \sum_{k=1}^{m} (-1)^k \mu_k Y^{m-k},$$

onde $\mu_k$ é obtido indutivamente por

$$\mu_0 = 1 \qquad \mu_k = \frac{1}{k} \sum_{i=1}^{k} (-1)^{i-1} \mu_{k-i} T(Y^i)$$

e $T$ denota $\frac{1}{2}tr$ (em que $tr$ é o traço definido em 2.20).

Observe que através do resultado acima temos, até o momento, uma cota superior para o grau de $*$-identidades polinomiais em variáveis simétricas satisfeitas por $(M_{2m}(\mathbb{F}), s)$. O resultado a seguir estabelecido em [8], nos fornece uma cota inferior para esse grau quando $m > 2$.

**Teorema 4.2.** *Se $f$ é uma $*$-identidade polinomial em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$ e $m > 2$, então $gr(f) \geq 2m + 2$.*

Desse modo, temos até o momento que o grau de uma $*$-identidade $f$ em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$, com $m > 2$, é tal que $2m + 2 \leq \mathrm{gr}(f) \leq 4m - 2$.

A seguir vamos enunciar o teorema, devido a D'Amour e Racine em [6], que resolve o problema de se encontrar $*$-identidades em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$ de grau mínimo, para os casos $m = 1, 2$. Ressaltamos que as identidades dadas abaixo valem em geral, mas a unicidade das mesmas exigem a restrição que será feita na característica do corpo $\mathbb{F}$. Usaremos a notação $y_1 \circ y_2 = y_1y_2 + y_2y_1 = y_1V_{y_2} = y_2V_{y_1}$.

**Teorema 4.3.** *Seja $Char(\mathbb{F}) = 0$, então $St_2(y_1, y_2) = [y_1, y_2]$ é uma $*$-identidade polinomial para $M_2(\mathbb{F}, s)$. Além disso, $M_2(\mathbb{F}, s)$ não satisfaz nenhuma $*$-identidade polinomial em variáveis simétricas de grau menor que 2 e qualquer $*$-identidade em variáveis simétricas de grau 2 é consequência de $St_2(y_1, y_2) = [y_1, y_2]$.*

*Também temos que*

$$p_4(y_1, y_2, y_3, y_4, y_5) = [[y_1, y_2] \circ [y_3, y_4] + [y_1, y_4] \circ [y_3, y_2], y_5] e$$

$$\begin{aligned} r_5(y_1, y_2, y_3, y_4, y_5) &= (y_4 \circ y_5) St_3(V_{y_1}, V_{y_2}, V_{y_3}) - (y_4 St_3(V_{y_1}, V_{y_2}, V_{y_3})) \circ y_5 \\ &- (y_5 St_3(V_{y_1}, V_{y_2}, V_{y_3})) \circ y_4 \end{aligned}$$

*são $*$-identidades polinomiais em variáveis simétricas para $M_4(\mathbb{F}, s)$ e $M_4(\mathbb{F}, s)$ não satisfaz uma $*$-identidade em variáveis simétricas com grau menor que 5. Mais ainda, qualquer$*$-identidade em variáveis simétricas para $M_4(\mathbb{F}, s)$ de grau 5 é consequência do conjunto $\{p_4, r_5\}$.*

Os teoremas abaixo resolvem o problema para o caso $m = 3$. O primeiro se deve a Racine, feito em [17] , e estabelece uma $*$-identidade em variáveis simétricas para $M_6(\mathbb{F}, s)$, enquanto o segundo, devido a Rashkova e feito em [18], prova a minimalidade dessa identidade.

**Teorema 4.4.** *O polinômio*

$$St_3([y_1^3, y_2], [y_1^2, y_2], [y_1, y_2])$$

*é uma $*$-identidade polinomial em variáveis simétricas para $M_6(\mathbb{F}, s)$ de grau 9.*

**Teorema 4.5.** *$M_6(\mathbb{F}, s)$ não satisfaz uma $*$-identidade em variáveis simétricas de grau menor que 9.*

Observe que a partir dos casos $m = 2, 3$ pode-se conjecturar que para $m > 1$, $(M_{2m}(\mathbb{F}), s)$ satisfaz uma $*$-identidade polinomial em variáveis simétricas de grau $4m-3$. O artigo [11], no qual se baseia a próxima seção, tem como objetivo principal demonstrar essa conjectura.

## 4.2 Identidade multilinear de grau $4m - 3$

Nessa seção iremos expor o resultado devido a J.D.Hill, feito em [11], que nos diz que para um inteiro $m > 1$ e $\mathbb{F}$ um corpo qualquer, $(M_{2m}(\mathbb{F}), s)$ satisfaz uma $*$-identidade multilinear de grau $4m - 3$ em variáveis simétricas. Desse modo, iremos obter uma nova cota superior para o grau minímo de uma $*$-identidade polinomial em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$.

**Definição 4.6.** *Seja $n$ um número inteiro positivo. Definimos,*

$$\begin{aligned} \phi : F\big\langle y_1, y_2, \ldots, y_n, \boldsymbol{y}\big\rangle &\longrightarrow F\big\langle y_1, y_2, \ldots, y_n, \boldsymbol{y}\big\rangle \\ f(y_1, \ldots, y_n, \boldsymbol{y}) &\longmapsto \sum_{\sigma \in S_n} sgn(\sigma) f(y_{\sigma(1)}, \ldots, y_{\sigma(n)}, \boldsymbol{y}) \end{aligned}$$

*e estendemos essa definição para polinômios de traço da forma natural.*

**Definição 4.7.** *Definimos para* $i = 1, 2, \ldots, n-1$

$$A_i^n := \phi(y_{j_1} \ldots y_{J_{i-1}} \boldsymbol{y} y_{j_i} \ldots y_{j_{n-1}}) = \sum_{\sigma \in S_{n-1}} sgn(\sigma) y_{\sigma(j_1)} \ldots y_{\sigma(j_{i-1})} \boldsymbol{y} y_{\sigma(j_i)} \ldots y_{\sigma(jn-1)},$$

*com* $1 \leq j_1 < j_2 \ldots j_{n-1} \leq n$. *Para* $i = n$ *definimos*

$$A_n^n := \phi(y_{j_1} \ldots y_{j_n-1} \boldsymbol{y}) = \sum_{\sigma \in S_{n-1}} sgn(\sigma) y_{\sigma(j_1)} \ldots y_{\sigma(J_n-1)} \boldsymbol{y}$$

*com* $1 \leq j_1 < j_2 \ldots j_{n-1} \leq n$.

Observe que na definição acima $n$ representa o número de variáveis e $i$ a posição da variável $y$ no monômio dentro de $\phi$.

**Exemplo 4.8.** *A fim de exemplificar o uso da notação estabelecida, consideremos*

$$\begin{aligned}
St_4(\boldsymbol{y}, y_1, y_2, y_3) &= \boldsymbol{y} y_1 y_2 y_3 - \boldsymbol{y} y_1 y_3 y_2 + \boldsymbol{y} y_2 y_3 y_1 - \boldsymbol{y} y_2 y_1 y_3 + \boldsymbol{y} y_3 y_1 y_2 - \boldsymbol{y} y_3 y_2 y_1 \\
&- y_1 \boldsymbol{y} y_2 y_3 + y_1 \boldsymbol{y} y_3 y_2 - y_2 \boldsymbol{y} y_3 y_1 + y_2 \boldsymbol{y} y_1 y_3 - y_3 \boldsymbol{y} y_1 y_2 + y_3 \boldsymbol{y} y_2 y_1 \\
&+ \cdots - y_1 y_2 y_3 \boldsymbol{y} + y_1 y_3 y_2 \boldsymbol{y} - y_2 y_3 y_1 \boldsymbol{y} + y_2 y_1 y_3 \boldsymbol{y} - y_3 y_1 y_2 \boldsymbol{y} + y_3 y_2 y_1 \boldsymbol{y} \\
&= \sum_{\sigma \in S_3} sgn(\sigma) \boldsymbol{y} y_{\sigma(1)} y_{\sigma(2)} y_{\sigma(3)} - \sum_{\sigma \in S_3} sgn(\sigma) y_{\sigma(1)} \boldsymbol{y} y_{\sigma(2)} y_{\sigma(3)} \\
&+ \ldots - \sum_{\sigma \in S_3} sgn(\sigma) y_{\sigma(1)} y_{\sigma(2)} y_{\sigma(3)} \boldsymbol{y} \\
&= A_1^4 - A_2^4 + A_3^4 - \cdots - A_4^4 \\
&= \sum_{i=1}^{4} (-1)^{i+1} A_i^4.
\end{aligned}$$

Vamos agora estabelecer alguns lemas técnicos necessários para a demonstração do teorema principal dessa seção.

**Lema 4.9.** *Seja* $\phi$ *o endomorfismo definido na Definição 4.6 e* $T = \frac{1}{2} tr$. *Então,*

$$\phi(T(\boldsymbol{y} y_2 y_3 + y_3 y_2 \boldsymbol{y})) = 0 = \phi(T((\boldsymbol{y} y_2 y_3 + y_3 y_2 \boldsymbol{y}) y_{i_1} y_{i_2} \ldots y_{i_k})),$$

*onde* $k$ *é um inteiro positivo e* $y_{i_1} y_{i_2} \ldots y_{i_k} = y_{\sigma(1)} y_{\sigma(4)} y_{\sigma(5)} \ldots y_{\sigma(k)}$, *em que* $\sigma$ *denota uma permutação de* $\{1, 4, 5, \ldots, k\}$.

**Demonstração.** Observe inicialmente que, pelas propriedades 2.20 da função traço, temos

$$\begin{aligned}
T(\mathbf{y} y_2 y_3 y_{i_1} \ldots y_{i_k} + y_3 y_2 \mathbf{y} y_{i_1} \ldots y_{i_k}) &= T(\mathbf{y} y_2 y_3 y_{i_1} y_{i_2} \ldots y_{i_k} + y_3 y_2 \mathbf{y} y_{i_1} y_{i_2} \ldots y_{i_k}) \\
&= T(\mathbf{y} y_2 y_3 y_{i_1} y_{i_2} \ldots y_{i_k}) \ + \ T(\mathbf{y} y_{i_1} y_{i_2} \ldots y_{i_k} y_3 y_2).
\end{aligned}$$

Como as permutações,

$$(2,3,i_1\dots,i_k)\longmapsto(2,3,i_1\dots,i_k)$$
$$(2,3,i_1\dots,i_k)\longmapsto(i_1\dots,i_k,3,2)$$

têm sinais opostos (veja que para obter a segunda permutação a partir da primeira é preciso realizar $2k+1$ transposições), então ao aplicar $\phi$ em $T$ obtemos

$$\begin{aligned}
\phi(T(\mathbf{y}y_2y_3y_{i_1}\dots y_{i_k}+y_3y_2\mathbf{y}y_{i_1}\dots y_{i_k})) &= T(\phi(\mathbf{y}y_2y_3y_{i_1}\dots y_{i_k}))\ +\ T(\phi(\mathbf{y}y_{i_1}\dots y_{i_k}y_3y_2))\\
&= T\Bigg(\sum_{\sigma\in S_k} sgn(\sigma)\mathbf{y}y_{\sigma(2)}y_{\sigma(3)}\dots y_{\sigma(i_k)}\Bigg)\\
&- T\Bigg(\sum_{\sigma\in S_k} sgn(\sigma)\mathbf{y}y_{\sigma(2)}y_{\sigma(3)}\dots y_{\sigma(i_k)}\Bigg)=0.
\end{aligned}$$

■

**Lema 4.10.** *[13] Seja $n$ um inteiro positivo. Então*

$$T(St_{2n}(y_1,\dots,y_{2n}))=0.$$

**Demonstração.** Seja $\mathcal{R}$ o subgrupo de $S_{2n}$ gerado pelo ciclo $\tau_1=(1\,2\,3\dots 2n)$ e $\mathcal{U}\subset S_{2n}$ o subgrupo cujos elementos são as permutações de $S_{2n}$ que deixam $2n$ fixo. Observe que $\mathcal{U}\cap\mathcal{R}=1$ e $S_{2n}=\mathcal{U}\mathcal{R}$ (igualdade como conjuntos) e portanto

$$\begin{aligned}
tr(St_{2n}(y_1,\dots,y_{2n})) &= tr\Bigg(\sum_{\alpha\in S_{2n}} sgn(\alpha)y_{\alpha(1)}\dots y_{\alpha(2n)}\Bigg)\\
&= tr\Bigg(\sum_{\sigma\tau\in\mathcal{U}\mathcal{R}} sgn(\tau\delta)y_{\tau\delta(1)}\dots y_{\tau\delta(2n)}\Bigg)\\
&= tr\Bigg(\sum_{\sigma\in\mathcal{U}} sgn(\sigma)\sum_{\tau\in\mathcal{R}} sgn(\tau)y_{\tau\sigma(1)}\dots y_{\tau\sigma(2n)}\Bigg)
\end{aligned}$$

como, pela a Definição 2.20, a função traço é invariante sob a ação de permutações cíclicas

$$tr(St_{2n}(y_1,\dots,y_{2n}))=tr\Bigg(\sum_{\sigma\in\mathcal{U}} sgn(\sigma)\sum_{\tau\in\mathcal{R}} sgn(\tau)y_{\sigma(1)}\dots y_{\sigma(2n)}\Bigg).$$

Agora, por $sgn(\tau_1)=-1$, temos que $sgn(\tau_1^{2j})=1$ e $sgn(\tau_1^{2j-1})=-1$, onde $1\leq j\leq n$. Desse modo,

$$tr(St_{2n}(y_1,\dots,y_{2n}))=tr\Bigg(\sum_{j=1}^{2n} sgn({\tau_1}^j)\sum_{\sigma\in\mathcal{U}} sgn(\sigma)y_{\sigma(1)}\dots y_{\sigma(2n)}\Bigg)=0.$$

■

**Lema 4.11.** *Seja* $A_k^{2l} = A_k^{2l}(y_1, \ldots, y_{2l-1}, \boldsymbol{y})$. *Então,*

*a.* $\dfrac{1}{(2l-1)!}\phi(A_k^{2l}(y_1, \ldots, y_{2l-1}, \boldsymbol{y} \circ y_{2l})) = (-1)^k(A_k^{2l+1} + A_{k+1}^{2l+1})$

*b.* $\dfrac{1}{(2l-1)!}\phi(A_k^{2l}(y_1, \ldots, y_{2l-1}, \boldsymbol{y}) \circ y_{2l}) = A_k^{2l+1} - A_{k+1}^{2l+1}$.

**Demonstração.** Pelas definições, temos

$$\begin{aligned}
&\frac{1}{(2l-1)!}\ \phi(A_k^{2l}(y_1, \ldots, y_{2l-1}, \mathbf{y} \circ y_{2l}))\\
&= \frac{1}{(2l-1)!}\phi\Bigg(\sum_{\sigma \in S_{2l-1}} sgn(\sigma) y_{\sigma(1)} \ldots y_{\sigma(k-1)}(\mathbf{y} \circ y_{2l}) y_{\sigma(k)} \ldots y_{\sigma(2l-1)}\Bigg)\\
&= \frac{1}{(2l-1)!}\phi\Bigg(\sum_{\sigma \in S_{2l-1}} sgn(\sigma) y_{\sigma(1)} \ldots y_{\sigma(k-1)}(\mathbf{y} \circ y_{\sigma(k)}) y_{\sigma(k+1)} \ldots y_{\sigma(2l-1)} y_{2l} (-1)^{2l-1-(k-1)}\Bigg).
\end{aligned}$$

Observe que a última igualdade se deve a definição de $\phi$ e ao fato de que para mover $y_{2l}$ até o final de cada monômio precisamos realizar $2l-1-(k-1)$ transposições e por esse motivo $(-1)^{2l-1-(k-1)}$ aparece na equação. Como $(-1)^{2l-1-(k-1)} = (-1)^k$ obtemos

$$\frac{(-1)^k}{(2l-1)!}\phi\Bigg(\sum_{\sigma \in S_{2l-1}} sgn(\sigma) y_{\sigma(1)} \ldots y_{\sigma(k-1)}(\mathbf{y} \circ y_{\sigma(k)}) y_{\sigma(k+1)} \ldots y_{\sigma(2l-1)} y_{2l}\Bigg).$$

Aplicando $\phi$ na equação acima e lembrando que $A_i^n := \phi(y_1 \ldots y_{i-1}\mathbf{y} y_i \ldots y_{n-1})$, resulta que

$$\frac{(-1)^k}{(2l-1)!}(2l-1)!(A_k^{2l+1} + A_{k+1}^{2l+1}) = (-1)^k(A_k^{2l+1} + A_{k+1}^{2l+1})$$

o que prova a primeira parte do lema. Para a segunda parte, temos

$$\begin{aligned}
&\frac{1}{(2l-1)!}\phi(A_k^{2l}(y_1, \ldots, y_{2l-1}, \mathbf{y}) \circ y_{2l})\\
&= \frac{1}{(2l-1)!}\phi\Bigg(\sum_{\sigma \in S_{2l-1}} sgn(\sigma)(y_{\sigma(1)} \ldots y_{\sigma(k-1)}\mathbf{y} y_{\sigma(k)} \ldots y_{\sigma(2l-1)}) \circ y_{2l}\Bigg)\\
&= \frac{1}{(2l-1)!}\phi\Bigg(\sum_{\sigma \in S_{2l-1}} sgn(\sigma) y_{\sigma(1)} \ldots y_{\sigma(k-1)}\mathbf{y} y_{\sigma(k)} \ldots y_{2l} + y_{2l} y_{\sigma(1)} \ldots y_{\sigma(k-1)}\mathbf{y} y_{\sigma(k)} \ldots y_{\sigma(2l-1)}\Bigg)
\end{aligned}$$

realizando $2l-1$ transposições, a fim de mover $y_{2l}$ para última posição, na equação acima obtemos,

$$\frac{1}{(2l-1)!}\phi\Bigg(\sum_{\sigma \in S_{2l-1}} sgn(\sigma) y_{\sigma(1)}, \ldots, y_{\sigma(k-1)}\mathbf{y} \ldots y_{2l} + (-1)^{2l-1} y_{\sigma(1)}, \ldots, y_{\sigma(k)}\mathbf{y} \ldots y_{2l}\Bigg).$$

Desse modo, temos

$$\frac{1}{(2l-1)!}(2l-1)!(A_k^{2l+1} - A_{k+1}^{2l+1}) = A_k^{2l+1} - A_{k+1}^{2l+1}.$$

■

**Lema 4.12.** *Seja* $A_k^{2l+1} = A_k^{2l+1}(y_1, \ldots, y_{2l}, \boldsymbol{y})$. *Então,*

*a.* $\dfrac{1}{(2l)!}\phi(A_k^{2l+1}(y_1, \ldots, y_{2l}, \boldsymbol{y} \circ y_{2l+1})) = (-1)^{k-1}(A_k^{2l+2} + A_{k+1}^{2l+2})$

*b.* $\dfrac{1}{(2l)!}\phi(A_k^{2l+1}(y_1, \ldots, y_{2l}, \boldsymbol{y}) \circ y_{2l+1}) = A_k^{2l+2} + A_{k+1}^{2l+2}$.

**Demonstração.**

A demonstração desse lema é análoga à dada no lema 4.11, exceto pelo fato de que na primeira parte moveremos $x_{2l+1}$, para tanto precisaremos realizar $2l-(k-1)$ transposições e por esse motivo $(-1)^{2l-(k-1)}$ aparecerá na equação, enquanto que na segunda parte moveremos também $y_{2l+1}$, mas para tanto precisaremos realizar $2l$ transposições e por esse motivo $(-1)^{2l} = 1$ aparecerá na equação.

■

**Teorema 4.13.** *Sejam* $\mathbb{F}$ *um corpo e* $m > 1$ *um inteiro positivo. Então,*

$$q_m(y_1, \ldots, y_{4m-4}; \boldsymbol{y}) := (m-1)\sum_{i=1}^{m} A_{4i-3}^{4m-3} - m\sum_{i=1}^{m-1} A_{4i-1}^{4m-3}$$

*é uma $*$-identidade polinomial multilinear em variáveis simétricas para* $(M_{2m}(\mathbb{F}), s)$ *de grau* $4m-3$.

Note que como um primo $p$ não pode dividir simultaneamente $m$ e $m-1$, assim $q_m$ é um polinômio não-nulo em $\mathbb{F}$, tendo $\mathbb{F}$ característica zero ou não.

**Demonstração.** Começamos observando que apesar do resultado acima não depender da característica do corpo $\mathbb{F}$ será suficiente demonstrarmos o resultado para o caso $Char(\mathbb{F}) = 0$. Uma vez que, tendo demonstrado esse caso especial teremos que o polinômio $q_m$ se anula em todas as substituições tomadas à partir de alguma base de $(M_{2m}(\mathbb{F}), s)^+$, em particular $q_m$ se anula em todas as substituições tomadas na base dada no Exemplo 3.8. Por sua vez note que as entradas das matrizes dessa base são dadas apenas pelos elementos 0 e $\pm 1$, portanto essa base é ainda uma base para $(M_{2m}(\mathbb{F}), s)^+$ com $\mathbb{F}$ um corpo com característica prima. Desse modo, pelo Teorema 2.35, $q_m$ é uma $*$-identidade polinomial independentemente da característica considerada para o corpo $\mathbb{F}$.

Estabelecendo então que $Char\mathbb{F} = 0$, consideremos a seguinte $*$-identidade polinomial de traço para $(M_{2m}(\mathbb{F}), s)$ (Ver [21], pg.139), denominada o polinômio genérico mínimo, que é definido por

$$Y^m + \sum_{k=1}^{m} (-1)^k \mu_k Y^{m-k},$$

onde $\mu_k$ é obtido indutivamente por

$$\mu_0 = 1 \qquad \mu_k = \frac{1}{k}\sum_{i=1}^{k}(-1)^{i-1}\mu_{k-i}T(Y^i)$$

.

Multilinearizando-se em $Y$ a identidade polinomial de traço acima, obtemos pelo Teorema 2.16 uma $*$-identidade polinomial de traço multilinear para $(M_{2m}(\mathbb{F}),s)$. Escrevendo-se essa identidade multilinear na forma,

$$\sum_{\sigma\in S_m} Y_{\sigma(1)}Y_{\sigma(2)}\dots Y_{\sigma(m)} + (\text{parte de traço})$$

e então substituindo-se $Y_1$ por $\{\mathbf{y},y_2,y_3\} = \mathbf{y}y_2y_3 + y_3y_2\mathbf{y}$, $Y_2$ por $y_1$ e $Y_i$ $(i>2)$ por $Q_i = \frac{1}{2}(y_{4(i-2)}y_{4(i-2)+1}y_{4(i-2)+2}y_{4(i-2)+3} + y_{4(i-2)+3}y_{4(i-2)+2}y_{4(i-2)+1}y_{4(i-2)})$ obtém-se a seguinte identidade polinomial de traço para $(M_n(\mathbb{F}),s)^+$:

$$\{\mathbf{y},y_2,y_3\}y_1Q_3Q_4\dots Q_m + \dots Q_m\dots Q_4Q_3y_1\{\mathbf{y},y_2,y_3\} + \text{parte de traço}. \tag{4.1}$$

Nosso objetivo será usar a parte livre de traço, da identidade acima, para "gerar"o polinômio $q_m(y_1,\dots,y_{4m-4};\mathbf{y})$ e provar que (após as transformações realizadas para se obter $q_m$) a parte de traço será nula.

Dessa forma, consideremos a parte livre de traço da Equação (4.1)

$$\{\mathbf{y},y_2,y_3\}y_1Q_3Q_4\dots Q_m + \dots + Q_m\dots Q_4Q_3y_1\{\mathbf{y},y_2,y_3\} \tag{4.2}$$

e apliquemos à ela o endomorfismo $\phi$ definido na Definição 4.6. Obtemos pela notação estabelicida em 4.7,

$$\begin{aligned}&(m-2)!(m-1)\big(A_1^{4m-4} - A_3^{4m-4}\big) + (m-2)!(1)\big(A_2^{4m-4} - A_4^{4m-4}\big)\\ &+ (m-2)!(m-2)\big(A_5^{4m-4} - A_7^{4m-4}\big) + (m-2)!(2)\big(A_6^{4m-4} - A_8^{4m-4}\big)\\ &+ \dots + (m-2)!(1)\big(A_{4m-7}^{4m-4} - A_{4m-5}^{4m-4}\big) + (m-2)!(m-1)\big(A_{4m-6}^{4m-4} - A_{4m-4}^{4m-4}\big),\end{aligned}$$

ou seja,

$$(m-2)!\sum_{r=1}^{m-1}\Big[(m-r)\big(A_{4(r-1)+1}^{4m-4} - A_{4(r-1)+3}^{4m-4}\big) + r\big(A_{4(r-1)+2}^{4m-4} - A_{4(r-1)+4}^{4m-4}\big)\Big]. \tag{4.3}$$

Para ver isso considere por exemplo o coeficiente do termo $\left(A_6^{4m-4} - A_8^{4m-4}\right)$ e perceba que para tanto consideramos em (4.1) apenas aquelas permutações de $\{\mathbf{y}, y_2, y_3\}, y_1$ e $Q_j$'s que tem $\{\mathbf{y}, y_2, y_3\}$ na terceira posição e $y_1$ à esquerda de $\{\mathbf{y}, y_2, y_3\}$. Aplicando-se $\phi$ a esses termos, temos que $(m-2)!$ aparecerá no coeficiente devido à permutação dos $m-2$ $Q_j's$ e o número 2 devido ao número de posições possíveis, à esquerda de $\{\mathbf{y}, y_2, y_3\}$, para $y_1$. Finalmente, note que as permutações de $Q_1, \ldots, Q_m$ e $y_1$ correspondem a permutações pares de $\{1, 4, 5, 6, \ldots, 4m-5\}$, portanto o único sinal negativo em $\left(A_6^{4m-4} - A_8^{4m-4}\right)$ se deve ao sinal da permutação de $\{2, 3\}$, advindo do fator $\{\mathbf{y}, y_2, y_3\}$, e portanto aparece na frente de $A_8^{4m-4}$.

Agora iremos transformar a Equação (4.3) de duas maneiras:

Primeiro substituímos $\mathbf{y}$ por $\mathbf{y} \circ y_{4m-4}$ (em 4.3) e aplicamos $\frac{1}{(4m-5)!}\phi$. Então, usando a primeira parte do Lema 4.11, obtemos

$$\begin{aligned}(m-2)! \sum_{r=1}^{m-1} (m-r)\big(-A_{4(r-1)+1}^{4m-3} - A_{4(r-1)+2}^{4m-3} + A_{4(r-1)+3}^{4m-3} + A_{4(r-1)+4}^{4m-3}\big) \\ + r\big(A_{4(r-1)+2}^{4m-3} + A_{4(r-1)+3}^{4m-3} - A_{4(r-1)+4}^{4m-3} - A_{4(r-1)+5}^{4m-3}\big). \qquad (1)\end{aligned}$$

Retornamos novamente na Equação (4.3) e fazemos (4.3) $\circ\, y_{4m-4}$, aplicamos então $\frac{1}{4m-5}\phi$, para a partir da segunda parte do Lema 4.11 obtermos

$$\begin{aligned}(m-2)! \sum_{r=1}^{m-1} (m-r)\big(A_{4(r-1)+1}^{4m-3} - A_{4(r-1)+2}^{4m-3} - A_{4(r-1)+3}^{4m-3} + A_{4(r-1)+4}^{4m-3}\big) \\ + r\big(A_{4(r-1)+2}^{4m-3} - A_{4(r-1)+3}^{4m-3} - A_{4(r-1)+4}^{4m-3} + A_{4(r-1)+5}^{4m-3}\big). \qquad (2)\end{aligned}$$

Por fim de $(2) - (1)$ temos,

$$\begin{aligned}&2(m-2)! \sum_{r=1}^{m-1} (m-r)\big(A_{4(r-1)+1}^{4m-3} - A_{4(r-1)+3}^{4m-3}\big) + r\big(A_{4(r-1)+5}^{4m-3} - A_{4(r-1)+3}^{4m-3}\big) \\ &= 2(m-2)! \sum_{r=1}^{m-1} \Big[(m-r)\ A_{4(r-1)+1}^{4m-3} - m\ A_{4(r-1)+3}^{4m-3} + r\ A_{4(r-1)+5}^{4m-3}\Big] \\ &= 2(m-2)!\big((m-1)A_1^{4m-3} - mA_3^{4m-3} + A_5^{4m-3} + (m-2)A_5^{4m-3} - mA_7^{4m-3} + 2A_9^{4m-3} \\ &\qquad + (m-3)A_9^{4m-3} - mA_{11}^{4m-3} + \cdots + A_{4m-7}^{4m-3} - mA_{4m-5}^{4m-3} + (m-1)A_{4m-3}^{4m-3}\big) \\ &= 2(m-2)!\big((m-1)A_1^{4m-3} - mA_3^{4m-3} + (m-1)A_5^{4m-3} - mA_7^{4m-3} \\ &\qquad + (m-1)A_9^{4m-3} - mA_{11}^{4m-3} + \cdots - mA_{4m-5}^{4m-3} + (m-1)A_{4m-3}^{4m-3}\big)\end{aligned}$$

$$= 2(m-2)![\sum_{i=1}^{m}(m-1)A_{4i-3}^{4m-3} - m\sum_{i=1}^{m-1}A_{4i-1}^{4m-3}]$$

que é um múltiplo escalar do polinômio $q_m(y_1,\ldots,y_{4m-4};\mathbf{y})$.

Agora realizando na parte de traço, da $*$-identidade (4.1), o mesmo processo realizado na parte livre de traço, obtém-se $(1)'$ e $(2)'$. Observe que fazendo-se isso o polinômio $(2)-(1)+(2)'-(1)'$ será consequência da $*$-identidade (4.1) e portanto também será uma $*$-identidade para $(M_{2m}(\mathbb{F}), s)$. Então, como vimos que $(2)-(1)$ é um múltiplo escalar de $q_m(y_1,\ldots,y_{4m-4};\mathbf{y})$ no que se segue o nosso objetivo será mostrar que $(2)'-(1)'$ é nulo.

Desse modo, consideremos a parte de traço de (4.1). Expandindo e ignorando os coeficientes, temos que um termo arbitrário de (4.1) é da forma

$$T(f_1(y_1,\ldots,y_m))T(f_2(y_1,\ldots,y_m))\ldots T(f_j(y_1,\ldots,y_m))g(y_1,\ldots,y_m)),$$

onde $j$ é um inteiro positivo e os $f_j's$, e $g$ são $*$-polinômios multilineares.

Agora, substituímos $Y_1$ por $\{\mathbf{y}, y_2, y_3\} = \mathbf{y}y_2y_3 + y_3y_2\mathbf{y}, Y_2$ por $y_1$ e $Y_i$ $(i>2)$ por $Q_i$ e aplicamos $\phi$. Pelo Lema 4.9, todos os termos nos quais $\{\mathbf{y}, y_2, y_3\}$ aparece dentro do traço se anulam, além disso, pelo Lema 4.10 os traços onde aparecem apenas $Q_j's$ também se anulam. Então os únicos termos que não se anulam são aqueles em que aparece exatamente um traço; $y_1$ aparece dentro desse traço e $\{\mathbf{y}, y_2, y_3\}$ aparece fora dele.

Isso mostra que os termos restantes são da forma

$$T(St_{4t+1})A_r^{4m-4-(4t+1)} = T(St_{4t+1})A_r^{4(m-t)-5},$$

onde $t$ é um inteiro positivo e $r$ é ímpar, pois $y_1$ está dentro do traço e cada $Q_j$ tem um número par de variáveis.

Agora, aplicamos a esses termos as duas transformações que aplicamos à 4.3, com as quais obtivemos (1) e (2). Pelo Lema 4.12 isso nos resultará em duas equações, $(1)'$ e $(2)'$, iguais. Portanto, $(2)'-(1)'=0$, o que mostra que $(2)-(1)$ é uma $*$-identidade em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$. Dessa forma, concluímos que $q_m(y_1,\ldots,y_{4m-4};\mathbf{y})$ é uma $*$-identidade polinomial em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$.

■

Afim de ilustrar essa demonstração, vamos mostrar no exemplo a seguir que o polinômio $q_3(y_1, y_2,\ldots,y_8,\mathbf{y})$ é uma $*$-identidade em variáveis simétricas para $(M_6(\mathbb{F}), s)$.

**Exemplo 4.14.** *Nesse exemplo mostraremos que*

$$q_3(y_1,y_2,\ldots,y_8,\boldsymbol{y}) = 2\sum_{i=1}^{3}A_{4i-3}^{9} - 3\sum_{i=1}^{2}A_{4i-1}^{9} = 2A_1^9 - 3A_3^9 + 2A_5^9 - 3A_7^9 + 2A_9^9$$

*é uma $*$-identidade polinomial em variáveis simétricas para $(M_6(\mathbb{F}), s)$.*

*Começamos considerando o $*$-polinômio genérico mínimo para $(M_6(\mathbb{F}), s)$,*

$$Y^3 + \sum_{k=1}^{3} (-1)^k \mu_k Y^{3-k},$$

*onde $\mu_k$ é obtido indutivamente por*

$$\mu_0 = 1 \qquad \mu_k = \frac{1}{k} \sum_{i=1}^{k} (-1)^{i-1} \mu_{k-i} T(Y^i).$$

*No nosso exemplo temos,*

$$\mu_0 = 1 \qquad \mu_1 = T(Y)$$
$$\mu_2 = \frac{1}{2}((T(Y))^2 - T(Y^2)) \quad \mu_3 = \frac{1}{3}(\frac{1}{2}((T(Y))^3 - T(Y^2)T(Y)) - T(Y)T(Y^2) + T(Y^3).)$$

*Portanto o $*$-polinômio genérico mínimo para $(M_6(\mathbb{F}), s)$ é dado explicitamente por:*

$$Y^3 - T(Y)Y^2 + \frac{1}{2}((T(Y))^2 - T(Y^2))Y - \frac{1}{6}T(Y)^3 + \frac{1}{2}T(Y^2)T(Y) - \frac{1}{3}T(Y^3)$$

*Multilinearizando em $Y$ a $*$-identidade polinomial de traço acima, obtemos pelo Teorema 2.16 uma $*$-identidade polinomial de traço multilinear para $(M_6(\mathbb{F}), s)$. Escrevendo essa identidade multilinear na forma,*

$$\sum_{\sigma \in S_3} Y_{\sigma(1)} Y_{\sigma(2)} Y_{\sigma(3)} + (\textit{parte de traço})$$

*e então substituindo $Y_1$ por $\{\boldsymbol{y}, y_2, y_3\} = \boldsymbol{y}y_2y_3 + y_3y_2\boldsymbol{y}, Y_2$ por $y_1$ e $Y_3$ por $Q_3$, onde $Q_3 = \frac{1}{2}(y_4y_5y_6y_7 + y_7y_6y_5y_4)$ obtêm-se a seguinte $*$-identidade polinomial de traço para $(M_6(\mathbb{F}), s)$:*

$$\{\boldsymbol{y}, y_2, y_3\} y_1 Q_3 + \ldots Q_3 y_1 \{\boldsymbol{y}, y_2, y_3\} + \textit{parte de traço} \tag{4.4}$$

*Nosso objetivo será usar a parte livre de traço, da identidade acima, para "gerar" o polinômio $q_3(y_1, \ldots, y_8; \boldsymbol{y})$ e provar que (após as transformações realizadas para obter $q_3$) a parte de traço será nula.*

*Dessa forma, consideremos a parte livre de traço da Equação 4.4*

$$\begin{aligned} &\{\boldsymbol{y}, y_2, y_3\} y_1 Q_3 + \{\boldsymbol{y}, y_2, y_3\} Q_3 y_1 + y_1 \{\boldsymbol{y}, y_2, y_3\} Q_3 \\ &+ y_1 Q_3 \{\boldsymbol{y}, y_2, y_3\} + Q_3 \{\boldsymbol{y}, y_2, y_3\} y_1 + Q_3 y_1 \{\boldsymbol{y}, y_2, y_3\} \end{aligned} \tag{4.5}$$

*e apliquemos à ela o endomorfismo $\phi$ definido na Definição 4.6. Obtemos, pela notação estabelecida na Definição 4.7,*

$$2\big(A_1^8 - A_3^8\big) + \big(A_2^8 - A_4^8\big) + \big(A_5^8 - A_7^8\big) + 2\big(A_6^8 - A_8^8\big) \tag{4.6}$$

*Para ver isso considere por exemplo o coeficiente do termo* $\big(A_6^8 - A_8^8\big)$ *e perceba que consideramos em 4.6 apenas aquelas permutações de* $\{\boldsymbol{y}, y_2, y_3\}, y_1$ *e* $Q_3$ *que tem* $\{\boldsymbol{y}, y_2, y_3\}$ *na terceira posição e* $y_1$ *à esquerda de* $\{\boldsymbol{y}, y_2, y_3\}$*, ou seja, o quarto termo e o sexto termo de 4.5. Aplicando-se* $\phi$ *à esses termos, temos que* $1!$ *aparecerá no coeficiente devido à permutação de* $Q_3$ *e o número* $2$ *devido ao número de posições possíveis, à esquerda de* $\{\boldsymbol{y}, y_2, y_3\}$*, para* $y_1$*. Finalmente, note que as permutações de* $Q_3$ *e* $y_1$ *correspondem as permutações pares de* $\{1, 4, 5, 6, 7\}$*, portanto o único sinal negativo em* $\big(A_6^8 - A_8^8\big)$ *se deve ao sinal da permutação de* $\{2, 3\}$*, advindo do fator* $\{\boldsymbol{y}, y_2, y_3\}$*, e portanto aparece na frente de* $A_8^8$*.*

*Agora, iremos transformar a Equação 4.6 de duas maneiras:*

*Primeiro substituímos* $\boldsymbol{y}$ *por* $\boldsymbol{y} \circ y_8$ *(em 4.3) e aplicamos* $\frac{1}{7!}\phi$*. Então, usando a primeira parte do Lema 4.11 obtemos*

$$\begin{aligned} &2\big( - A_1^9 - A_2^9 + A_3^9 + A_4^9\big) + \big(A_2^9 + A_3^9 - A_4^9 - A_5^9\big) \\ &\quad + \big( - A_5^9 - A_6^9 + A_7^9 + A_8^9\big) + 2\big(A_6^9 + A_7^9 - A_8^9 - A_9^9\big) \end{aligned} \tag{1}$$

*Retornamos novamente na Equação 4.6 e fazemos* $(4.6) \circ y_8$*, aplicamos* $\frac{1}{7!}\phi$ *para, a partir da segunda parte do Lema 4.11, obtermos*

$$\begin{aligned} &2\big(A_1^9 - A_2^9 - A_3^9 + A_4^9\big) + \big(A_2^9 - A_3^9 - A_4^9 + A_5^9\big) \\ &\quad + \big(A_5^9 - A_6^9 - A_7^9 + A_8^9\big) + 2\big(A_6^9 - A_7^9 - A_8^9 + A_9^9\big). \end{aligned} \tag{2}$$

*Por fim de (2)-(1) temos,*

$$2\big(2A_1^9 - 2A_3^9\big)\big( - 2A_3^9 + 2A_5^9\big) + \big(2A_5^9 - 2A_7^9\big) + \big( - 2A_7^9 + 2A_9^9\big)$$

*que se torna,*

$$2(2A_1^9 - 3A_3^9 + 2A_5^9 - 3A_7^9 + 2A_9^9)$$

*que é um múltiplo escalar do* $*$*-polinômio* $q_3(y_1, \ldots, y_8; \boldsymbol{y})$*.*

*Agora, realizando na parte de traço, da* $*$*-identidade 4.4, o mesmo processo realizado na parte livre de traço, obtêm-se* $(1)'$ *e* $(2)'$*. Observe que fazendo-se isso o polinômio* $(2) - (1) + (2)' - (1)'$ *será consequência da* $*$*-identidade 4.4 e portanto também será uma* *identidade para* $(M_6(\mathbb{F}), s)$*. Então, como vimos que* $(2) - (1)$ *é um múltiplo escalar de* $q_3(y_1, \ldots, y_8; \boldsymbol{y})$*, no que se segue o nosso objetivo será mostrar que* $(2)' - (1)'$ *é nulo.*

*Desse modo, consideremos a parte de traço de 4.4. Expandindo e ignorando os coeficientes, temos que um termo arbitrário de 4.4 é da forma*

$$T(f_1(Y_1, Y_2, Y_3))T(f_2(Y_1, Y_2, Y_3))T(f_j(Y_1, Y_2, Y_3))g(Y_1, Y_2, Y_3)),$$

*onde* $j = 1, 2$ *ou* $3$ *e os* $f_j$*'s, e* $g$ *são polinômios multilineares.*

*Agora, substituímos* $Y_1$ *por* $\{\boldsymbol{y}, y_2, y_3\} = \boldsymbol{y}y_2y_3 + y_3y_2\boldsymbol{y}, Y_2$ *por* $y_1$ *e* $Y_3$ *por* $Q_3$ *e então aplicamos* $\phi$*. Pelo Lema 4.9, todos os termos nos quais* $\{\boldsymbol{y}, y_2, y_3\}$ *aparece dentro do traço se anulam, além disso, pelo Lema 4.10 os traços onde aparecem apenas* $Q_3$ *também se anulam. Desse modo, os únicos termos que não se anulam são aqueles em que aparece exatamente um traço, além disso,* $x_1$ *aparece dentro desse traço e* $\{y, x_2, x_3\}$ *aparece fora dele. Isso mostra que os termos restantes são da forma*

$$T(St_5)\big(A_1^3 - A_3^3\big) \quad e \quad T(St_1)\big(A_1^7 - A_3^7 + A_5^7 - A_7^7\big).$$

*Por fim, aplicamos a esses termos as duas transformações que aplicamos em 4.6 (com as quais obtivemos* $(1)$ *e* $(2)$*). Pelo Lema 4.12, isso nos resultará em duas equações,* $(1)'$ *e* $(2)'$*, iguais. Portanto* $(2)' - (1)' = 0$*, o que mostra que* $(2) - (1)$ *é uma* $*$*-identidade polinomial para* $(M_6(\mathbb{F}), s)$*.*

Dessa forma, concluímos que $q_3(y_1, \ldots, y_8; \mathbf{y})$ é uma $*$-identidade polinomial em variáveis simétricas para
$(M_6(\mathbb{F}), s)$.

A partir do resultado de J.D. Hill obtemos uma nova cota superior para o grau de uma $*$-identidade polinomial em variáveis simétricas $f$ de $(M_{2m}(\mathbb{F}), s)$, isto é, o grau de uma identidade polinomial em variáveis simétricas $f$ de $(M_{2m}(\mathbb{F}), s)$ é tal que $4m - 3 \geq \mathrm{gr}(f) \geq 2m + 2$, quando $m > 2$.

## 4.3 Construção de uma base para $(M_{2^m}(\mathbb{F}), s)$

No Capítulo 2 vimos que se a característica de $\mathbb{F}$ é zero o estudo das identidades de uma $\mathbb{F}$-álgebra pode ser reduzido ao estudo de identidades multilineares. No mesmo capítulo foi visto que para determinar se um polinômio multilinear é uma identidade polinomial para uma $\mathbb{F}$-álgebra de dimensão finita, basta avaliarmos esse polinômio nos elementos de uma base da álgebra. Além disso, no Capítulo 3 foi observado que todos esses resultados são válidos no contexto de $*$-identidades polinomiais.

Desse modo, a fim de se encontrar $*$-identidades polinomiais para $(M_n(\mathbb{F}), s)$, se torna interessante procurar bases para $(M_n(\mathbb{F}), s)$ com boas características. Nesse sentido, iremos expor nessa seção a construção de uma base, feita em [14], para $(M_{2^m}(\mathbb{C}), s)$ que tem a surpreendente propriedade de que todos os seus elementos são invertiveís e são simétricos ou antissimétricos com relação a involução simplética. Mais ainda, os elementos da base que são simétricos formam uma base para $(M_{2^m}(\mathbb{C}), s)^+$ e os elementos que são antissimétricos formam uma base para $(M_{2^m}(\mathbb{C}), s)^-$.

No Exemplo 1.47 vimos que a decomposição da álgebra do 2-grupo extra-especial $E_m$ é dada por

$$\mathbb{C}E_m \cong \overset{2^m}{\oplus}\, \mathbb{C} \oplus M_{2^m}(\mathbb{C}).$$

Por outro lado na Proposição 5.8 vimos que existe uma bijeção entre as representações de um dado grupo $G$ e os seus $\mathbb{C}$G-módulos. Desse modo, pela decomposição acima, temos que existem representações de grau $2^m$ (diferentes da trivial) para o grupo $E_m$.

A seguir, iremos apresentar para cada $m \geq 1$, uma representação de grau $2^m$ do grupo extra-especial $E_m$. Ao longo de todo essa seção iremos denotar por $I_m$ a matriz identidade $2^m \times 2^m$.

Começamos dando uma representação de grau 2 para $E_1 = D^1 \cong D_4$. Sabemos que o grupo $E_1$ tem dois geradores, esses geradores serão denotados por $a_1^{(1)}$ e $b_1^{(1)}$. Usando a representação definida em 5.3 para $D_4$, temos a seguinte representação para o grupo extra-especial $E_1$:

$$a_1^{(1)} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad b_1^{(1)} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Agora, para $m = 2$, o grupo extra-especial $E_2 = D^1D^2$ tem quatro geradores que serão denotados por $a_1^{(2)}$, $b_1^{(2)}$, $a_2^{(2)}$ e $b_2^{(2)}$. Utilizando a representação anterior e a representação trivial de grau 2 de $E_1$ obtemos através dos produtos tensoriais dessas representações, uma representação de grau 4 de $E_2$ dada por

$$a_1^{(2)} = \begin{pmatrix} 0 & -I_1 \\ I_1 & 0 \end{pmatrix} \qquad b_1^{(2)} = \begin{pmatrix} -I_1 & 0 \\ 0 & I_1 \end{pmatrix}$$

$$a_2^{(2)} = \begin{pmatrix} a_1^{(1)} & 0 \\ 0 & a_1^{(1)} \end{pmatrix} \qquad b_2^{(2)} = \begin{pmatrix} b_1^{(1)} & 0 \\ 0 & b_1^{(1)} \end{pmatrix}.$$

De maneira análoga, para $m = 3$, o grupo $E_3 = D^1D^2D^3$ tem seis geradores, os quais iremos denotar por $a_1^{(3)}$, $b_1^{(3)}$, $a_2^{(3)}$, $b_2^{(3)}$, $a_3^{(3)}$e $b_3^{(3)}$. Então, utilizamos a representação anterior de grau 4 de $E_2$ e a representação trivial de grau 2 de $E_1$ para obter através dos produtos tensoriais dessas representações, uma representação de grau 8 de $E_3$ dada por

$$a_1^{(3)} = \begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix} \qquad b_1^{(3)} = \begin{pmatrix} -I_2 & 0 \\ 0 & I_2 \end{pmatrix}$$

$$a_2^{(3)} = \begin{pmatrix} a_1^{(2)} & 0 \\ 0 & a_1^{(2)} \end{pmatrix} \qquad b_2^{(3)} = \begin{pmatrix} b_1^{(2)} & 0 \\ 0 & b_1^{(2)} \end{pmatrix}$$

$$a_3^{(3)} = \begin{pmatrix} a_2^{(2)} & 0 \\ 0 & a_2^{(2)} \end{pmatrix} \qquad b_3^{(3)} = \begin{pmatrix} b_2^{(2)} & 0 \\ 0 & b_2^{(2)} \end{pmatrix}.$$

Em geral, para cada $m \in \mathbb{N}$, temos que o grupo extra-especial $E_m = D^1D^2 \dots D^m$ tem $2m$ geradores, os quais serão denotados por $a_j^{(m)}$ e $b_j^m$, com $1 \leq j \leq m$. Por fim, usaremos a representação de grau $2^m$ de $E_m$, obtida de forma recursiva usando o processo, e a representação trivial de grau 2 do grupo $E_1$, para obter através dos produtos tensoriais dessas representações (ver Apêndice), uma representação de grau $2^{m+1}$ para o grupo $E_{m+1}$ dada por

$$a_1^{(m+1)} = \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} \qquad b_1^{(m+1)} = \begin{pmatrix} -I_m & 0 \\ 0 & I_m \end{pmatrix}$$

$$a_j^{(m+1)} = \begin{pmatrix} a_{j-1}^{(m)} & 0 \\ 0 & a_{j-1}^{(m)} \end{pmatrix} \qquad b_j^{(m+1)} = \begin{pmatrix} b_{j-1}^{(m)} & 0 \\ 0 & b_{j-1}^{(m)} \end{pmatrix}.$$

**Exemplo 4.15.** *Vamos usar esse processo para construir uma representação de grau 8 para $E_3$.*

*Começamos com a representação de $E_1$ de grau 2 :*

$$a_1^{(1)} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad b_1^{(1)} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

*Agora, através dos produtos tensoriais dessa representação com a representação trivial de grau 2 de $E_1$, obtemos uma representação de grau 4 para $E_2$ dada por*

$$a_1^{(2)} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad b_1^{(2)} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$a_2^{(2)} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad b_2^{(2)} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

*E por último, tomamos os produtos tensoriais da representação anterior de grau* $4$ *para* $E_2$ *com a representação trivial de* $E_1$*, para obter a representação de grau* $2^3$ *para* $E_3$*:*

$$a_1^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad b_1^{(3)} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$a_2^{(3)} = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad b_2^{(3)} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$a_3^{(3)} = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad b_3^{(3)} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A fim de simplificar a notação, quando não houver possibilidade de confusão em relação ao grupo $E_m$ com o qual estivermos trabalhando, iremos omitir o $m$ na notação estabelecida para os geradores de $E_m$, ou seja, os mesmos serão denotados apenas por $a_j$ e $b_j$, com $1 \leq j \leq m$. Além disso, denotaremos por $s$ o comutador de $a_j$ e $b_j$ (observe que, por $E_m$ ser um grupo 2-extra-especial os comutadores de $a_j$ e $b_j$ são iguais, para todo $1 \leq j \leq m$). Então, com essas notações estabelecidas, temos que $a_j^4 = b_j^2 = 1$ e $s^2 = 1$.

Seja $W$ o produto dos transversais $W_j = \{1, a_j, b_j, a_jb_j\}$ de $D^{j'}$ em $D^j$, com $1 \leq j \leq m$. A seguir iremos mostrar que através dos elementos de $W$ (via a representação dada acima) obtemos uma base para $M_{2^m}(\mathbb{C})$.

**Lema 4.16.** *O conjunto $W$ é um conjunto transversal de $E_m' = \langle s \rangle$.*

**Demonstração.** Seja $E_m = D^1D^2 \ldots D^m$, $E_m' = \{1, s\} = Z(E_m)$ e $\{1, a_i, b_i, a_ib_i\}$ um conjunto transversal para $D^{i'}$ em $D^i$, com $1 \leq i \leq m$. Consideremos $x$ um elemento qualquer de $E_m$, temos que $x = a_1^{j_1}b_1^{i_1}a_2^{j_2}b_2^{i_2} \ldots a_m^{j_m}b_m^{i_m}$, com $0 \leq j_k \leq 3$ e $0 \leq i_k \leq 1$.

Agora, pela definição de produto central de grupos, temos $[D_k, D_l] = 1$, para quaisquer $1 \leq k < l \leq m$ e $Z(E_m) = Z(D_j) = \langle a_j^2 \rangle$, para todo $1 \leq j \leq m$. Então,

$$a_k^{j_k}b_k^{i_k}a_l^{j_l}b_l^{i_l} = a_l^{j_l}b_l^{i_l}a_k^{j_k}b_k^{i_k}, \quad \text{para quaisquer } 1 \leq k < l \leq m$$

e $a_j^2 = s$, para todo $1 \leq j \leq m$. Através dessas observações podemos concluir que

$$x = a_1^{\beta_1}b_1^{\alpha_1}a_2^{\beta_2}b_2^{\alpha_2} \ldots a_m^{\beta_m}b_m^{\alpha_m} \quad \text{ou} \quad x = sa_1^{\beta_1}b_1^{\alpha_1}a_2^{\beta_2}b_2^{\alpha_2} \ldots a_m^{\beta_m}b_m^{\alpha_m}, \qquad \text{com } \alpha_k, \beta_k \in \{1, 0\}.$$

Desse modo, o produto dos transversais $W_j = \{1, a_j, b_j, a_jb_j\}$, com $1 \leq j \leq m$, é de fato um conjunto transversal de $E_m'$ em $E_m$. ∎

Como consequência imediata do Lema anterior temos a seguinte proposição:

**Proposição 4.17.** *O transversal $W$ de $E_m'$ em $E_m$ é uma base para o ideal $\mathbb{C}E_m\left(\frac{1-s}{2}\right)$.*

No Exemplo 1.47 vimos que $\mathbb{C}E_m\left(\frac{1-s}{2}\right)$ é uma componente simples de $\mathbb{C}E_m$ e por ter dimensão $2^{2m}$, temos que $\mathbb{C}E_m\left(\frac{1-s}{2}\right) \cong M_{2^m}(\mathbb{C})$, então pela proposição anterior e via a representação apresentada, podemos concluir que temos uma base para $M_{2^m}(\mathbb{C})$, ou seja, que via a representação construída acima para $E_m$ as matrizes que representam os elementos de $W$ constituem uma base para a álgebra de matrizes $2^m \times 2^m$.

Consideremos agora a álgebra $M_{2^m}(\mathbb{C})$ com involução simplética $*$ definida no capítulo 3 (estamos denotando aqui a involução simplética por $*$ para evitar confusões com a notação $s$ dada para o gerador de $E_m'$). Pela representação de $E_m$ dada acima e induzindo a involução simplética no grupo $E_m$ podemos observar que

$$a_1^* = sa_1 \quad b_1^* = sb_1 \qquad \text{e} \qquad a_j^* = sa_j \quad b_j^* = b_j \quad \text{para todo } 2 \leq j \leq m.$$

Assim, observando que em $\mathbb{C}E_m\left(\frac{1-s}{2}\right)$ podemos identificar o elemento s com -1 e denotando por $S$ o conjunto dos elementos de $W$ que são simétricos e $A$ os que são antissimétricos com relação a involução simplética, podemos ver que (por $s \in Z(E_m)$) $W = S \cup A$. No que se segue iremos provar que $S$ é uma base para $(M_{2^m}(\mathbb{C}), *)^+$ e que $A$ é uma base para $(M_{2^m}(\mathbb{C}), *)^-$.

Consideremos a tabela abaixo

| Transversais | $W_1$ | $W_2$ | $W_3$ | $\dots$ | $W_m$ |
|---|---|---|---|---|---|
| $n^{\text{o}}$ elementos simétricos | 1 | 3 | 3 | $\dots$ | 3 |
| $n^{\text{o}}$ elementos antissimétricos | 3 | 1 | 1 | $\dots$ | 1 |

A fim de produzir um elemento simétrico em $W$ nós primeiro consideramos o número de elementos simétricos $S^+$ em $W_2W_3\dots W_m$. Lembrando que elementos em grupos $D^j$'s diferentes comutam, esse número é dado quando escolhemos no produto um número par de elementos antissimétricos. Logo,

$$S^+ = \binom{m-1}{0}3^{m-1} + \binom{m-1}{2}3^{m-1-2} + \dots = \sum_{k \geq 0} \binom{m-1}{2k}3^{m-1-2k}.$$

Agora, consideramos o número de elementos antissimétricos $S^-$ em $W_2W_3\dots W_m$. Esse número é dado quando escolhemos no produto um número ímpar de elementos antissimétricos. Logo,

$$S^- = \binom{m-1}{1}3^{m-1-1} + \binom{m-1}{3}3^{m-1-3} + \cdots = \sum_{k\geq 0}\binom{m-1}{2k+1}3^{m-1-(2k+1)}.$$

Então, observamos que,

$$S^+ + S^- = \sum_{j\geq 0}\binom{m-1}{j}3^{m-1-j} = \sum_{j=0}^{m-1}\binom{m-1}{j}3^{m-1-j}1^j = (3+1)^{m-1} = 4^{m-1} = 2^{2m-2}$$

que é igual ao número de elementos em $W_2W_3\ldots W_m$.

Por outro lado,

$$\begin{aligned} S^+ - S^- &= \binom{m-1}{0}3^{m-1-0}1^0 - \binom{m-1}{1}3^{m-1-1}1^1 + \binom{m-1}{2}3^{m-1-2}1^2 - \ldots \\ &= \sum_{j\geq 0}\binom{m-1}{j}3^{m-1-j}(-1)^j \\ &= (3-1)^{m-1} = 2^{m-1}. \end{aligned}$$

Desse modo,

$$S^+ = \frac{(S^+ + S^-) + (S^+ - S^-)}{2} = \frac{2^{2m-2} + 2^{m-1}}{2} = 2^{2m-3} + 2^{m-2} \quad \text{e}$$

$$S^- = \frac{(S^+ + S^-) - (S^+ - S^-)}{2} = 2^{2m-3} - 2^{m-2}.$$

Agora, observe que os elementos simétricos de $W$ são produzidos considerando-se o produto de elementos simétricos em $W_1$ (pela tabela temos apenas 1 elemento) com elementos simétricos em $W_2W_3\ldots W_m$ ou considerando-se o produto de elementos antissimétricos em $W_1$ (pela tabela temos 3 elementos)com elementos antissimétricos em $W_2W_3\ldots W_m$. Assim, o total de elementos simétricos em $W$ é dado por,

$$S^+ + 3S^- = 2^{2m-3} + 2^{m-2} + 3(2^{2m-3} - 2^{m-2}) = 2^{m-1}(2^m - 1).$$

Como, pelo Exemplo 3.8, temos que a dimensão do subespaço $(M_{2^m}(\mathbb{C}), *)^+$ é igual a $2^{m-1}(2^m-1)$. Concluímos que elementos simétricos $S$ em $W$ formam uma base para $(M_{2^m}(\mathbb{C}), *)^+$.

Por sua vez, temos que os elementos antissimétricos de $W$ são produzidos considerando-se o produto de elementos simétricos em $W_1$ (pela tabela temos apenas 1 elemento) com elementos antissimétricos em $W_2W_3\ldots W_m$ ou considerando-se o produto de elementos antissimétricos em $W_1$ (pela tabela temos 3 elementos) com elementos simétricos em $W_2W_3\ldots W_m$. Assim, o total de elementos antissimétricos em $W$ é dado por,

$$3S^+ + S^- = 3(2^{2m-3} + 2^{m-2}) - 2^{2m-3} + 2^{m-2} = 2^{m-1}(2^m + 1).$$

Novamente, pelo Exemplo 3.8, temos que a dimensão do subespaço $(M_{2^m}(\mathbb{C}), *)^-$ é igual a $2^{m-1}(2^m+1)$. Então, concluímos que os elementos antissimétricos $A$ em $W$ formam uma base para $(M_{2^m}(\mathbb{C}), *)^-$.

Dessa forma, $W$ é uma base para $(M_{2^m}(\mathbb{C}), *)$ cujos elementos são invertíveis e são simétricos ou antissimétricos com relação a involução simplética. Além disso, seus elementos simétricos formam uma base para $(M_{2^m}(\mathbb{C}), *)^+$ e seus elementos antissimétricos formam uma base para $(M_{2^m}(\mathbb{C}), *)^-$.

## 4.4 Implementação da base em GAP

Nessa seção iremos apresentar os algoritmos implementados no GAP, que é um software livre próprio para a linguagem algébrica [23]. O objetivo desses algoritmos é se obter computacionalmente as bases de $(M_{2^m}(\mathbb{C}), s)^+$ e $(M_{2^m}(\mathbb{C}), s)^-$ construídas na seção anterior. Veremos que cada função foi desenvolvida seguindo os passos da construção feita acima.

As funções abaixo são destinadas a computação das matrizes obtidas via a representação (definida na seção anterior) dos geradores do grupo $E_m$. Seus parâmetros de entrada estão associadas a notação estabelecida na representação, por exemplo a fim de se obter a representação de $a_n^m$ iremos usar como parâmetro os valores $n$ (denota um dos geradores de $D^n$) e $m$ (advém da ordem de $|E_m| = 2^{2m+1}$).

```
A:= function(n,m)
local b, c;
b := [[0, −1], [1, 0]];
if n = 1 and m = 1 then
return b;
elif n = 1 and m > 1 then
c:= KroneckerProduct( A(1, m − 1), IdentityMat(2));
b:= c;
elif n > 1 and m > 1 then
c:= KroneckerProduct(IdentityMat(2),A(n − 1, m − 1));
b:= c;
else
return "Esse elemento não existe";
```

```
fi;
return b;
end; ;

B:= function(n, m)
local a,  c;
a:= [[−1, 0], [0, 1]];
if n = 1 and m = 1 then
return a;
elif n = 1 and m > 1 then
c:= KroneckerProduct( B(1, m − 1), IdentityMat(2));
a:= c;
elif n > 1 and m > 1 then
c:= KroneckerProduct(IdentityMat(2),B(n − 1, m − 1));
a:= c;
else
return "Esse elemento não existe";
fi;
return a;
end; ;
```

A função abaixo obtêm a representação dos elementos dos conjuntos transversais $W_n = \{1, a_n, b_n, a_nb_n\}$, seus parâmetros de entrada também seguirão a notação estabelecida e portanto serão: $n$ (denota o transversal de $D^{n'}$, $W_n$) e $m$, assim como foi denotado acima, advém da ordem de $E_m$. Essa função será necessária para a funcionalidade da ¨função base¨ que obtém a partir do cálculo de todos os $W_j'$s as representações dos elementos do transversal $W$ de $E_m'$ em $E_m$ que mostramos ser uma base para $M_{2^m}(\mathbb{C})$.

```
Trans:= function(n, m)
local c, i, j, k;
c:= [IdentityMat(2^m), A(n, m), B(n, m), A(n, m)*B(n, m)];
return c;
end; ;
```

A função abaixo retorna o conjunto de matrizes que constituem uma base para $M_{2^m}(\mathbb{C})$, seu parâmetro de entrada é o valor $m$ que está associada a dimensão $2^{2m}$ da álgebra de matrizes $M_{2^m}(\mathbb{C})$.

```
base := function(m)
local d,  j,  k,  p,  l;
l:=1;
j:=1;
k:=1;
d:= List(Trans(1,m));
p:=2;
while p <= m do
while j <= 4^l do
while k < 5 do
Add(d,d[j]*Trans(p,m)[k]);
k:=k+1;
od;
k:=1;
j:= j+1;
od;
j:=1;
l:=l+1;
p:=p+1;
d:= Set(d);
od;
return d;
end; ;
```

A função Sympl tem como parâmetro de entrada uma matriz e retorna a matriz obtida via a aplicação da involução simplética na matriz de entrada.

```
Sympl:= function(n)
local m, j, l;
l:=[[0,1],[-1,0]];
j:= KroneckerProduct(l,IdentityMat(DimensionsMat(n)[1]/2));
m:= j*TransposedMat(n)*TransposedMat(j);
return m;
end; ;
```

A função basesim retorna uma base para o subespaço $(M_{2^m}(\mathbb{C}), s)^+$ das matrizes simétricas com relação a involução simplética. Seu parâmetro de entrada é m que novamente está associada de maneira óbvia à dimensão de $M_{2^m}(\mathbb{C})$.

```
basesim:= function(m)
local d,i,c;
i:=1;
c:=[];
d:= base(m);
while i <= Length(base(m)) do
if base(m)[i]=Sympl(base(m)[i]) then
Add(c, base(m)[i]);
fi;
i:=i+1;
od;
return c;
end; ;
```

Por sua vez a função baseanti retorna a base para o subespaço $(M_{2^m}(\mathbb{C}), s)^-$ das matrizes antissimétricas com relação a involução simplética. Seu parâmetro de entrada é m que está associada novamente de maneira óbvia à dimensão de $M_{2^m}(\mathbb{C})$.

```
baseanti:= function(m)
local d,i,c;
i:=1;
c:=[];
d:= base(m);
while i <= Length(base(m)) do
if -1*base(m)[i] = Sympl(base(m)[i]) then
Add(c, base(m)[i]);
fi;
i := i + 1;
od;
return c;
end; ;
```

# Capítulo 5

# Considerações finais

Na Seção 4.2, vimos que o grau de uma identidade polinomial $f$ em variáveis simétricas para $(M_{2m}(\mathbb{F}), s)$ é tal que $4m - 3 \geq \mathrm{gr}(f) \geq 2m + 2$ e apresentamos uma identidade polinomial multilinear de grau $4m-3$ para $(M_{2m}(\mathbb{F}), s)^+$. Entretanto nesse contexto uma pergunta interessante a ser feita é: qual o menor valor de $k$ para que $St_k$ (em variáveis simétricas ou antissimétricas) seja uma identidade de $(M_{2m}(\mathbb{F}), s)$?.

Vimos que Rowen demonstrou em [19] que $St_{4m-2}$ é uma identidade polinomial para $(M_{2m}(\mathbb{F}), s)^+$. Conscientes do resultado de J.D. Hill é natural nos perguntarmos se $St_{4m-3}$ é uma identidade polinomial para $(M_{2m}(\mathbb{F}), s)^+$, porém já foi demonstrado por Rowen que $St_5$ não é uma identidade polinomial para $(M_4(\mathbb{C}), s)^+$. Além disso J.Adamsson demonstrou em [1], que que $St_9$ e $St_{13}$ não são identidades polinomiais para $(M_6(\mathbb{C}), s)^+$ e $(M_8(\mathbb{C}), s)^+$, respectivamente. Desse modo, $4m-2$ parece ser o grau mínimo para uma identidade polinomial de $(M_{2m}(\mathbb{F}), s)^+$, porém isto ainda não foi provado em geral. Assim, o nosso tópico de estudo para trabalhos futuros será utilizar a base que foi apresentada na Seção 4.3 para tentar resolver esta questão para $(M_{2^m}(\mathbb{C}), s)^+$.

# Apêndice

Nesse apêndice iremos fazer uma breve exposição da teoria de representações de grupos, que consiste em relacionar grupos com espaços vetoriais. Nosso objetivo principal será definir e estudar o produto tensorial entre duas representações.

## 5.1 Representações de grupos

**Definição 5.1.** *Sejam $G$ um grupo finito e $V$ um espaço vetorial de dimensão finita sobre $\mathbb{F}$. Uma representação de $G$ sobre $V$ é um homomorfismo*

$$\begin{aligned} \rho : & G \longrightarrow GL(V) \\ & g \longmapsto \rho_g. \end{aligned}$$

*O grau de uma representação de $G$ sobre $V$ será definido como sendo a dimensão de $V$.*

**Exemplo 5.2.** *Seja $G = S_n$ e $V = \mathbb{C}$. Então*

$$\begin{aligned} \rho : & G \longrightarrow GL(\mathbb{C}) \cong \mathbb{C}^* \\ & \sigma \longmapsto \begin{cases} 1, & se \quad \sigma \quad par, \\ -1, & se \quad \sigma \quad ímpar. \end{cases} \end{aligned}$$

*é uma representação de $S_n$ com grau igual a 1.*

**Exemplo 5.3.** *Seja $G$ o grupo diedral de ordem 8,*

$$D_4 =< a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1} >$$

*e consideremos as matrizes*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad e \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

*Como* $A^4 = B^2 = I$, $B^{-1}AB = A^{-1}$, *temos que a aplicação*

$$\rho : D_4 \longrightarrow GL(2, \mathbb{C})$$

$$a \longrightarrow A$$

$$b \longrightarrow B$$

*é uma representação de* $D_4$ *de grau* 2 *sobre* $\mathbb{C}$.

**Definição 5.4.** *Duas representações* $\rho_1 : G \longrightarrow GL(V)$ *e* $\rho_2 : G \longrightarrow GL(W)$ *de um grupo* $G$ *são ditas equivalentes se existe uma transformação linear invertível* $T : V \longrightarrow W$ *tal que,*

$$T \circ \rho_1(g) = \rho_2(g) \circ T \quad \forall\ g \in G.$$

**Definição 5.5.** *Sejam* $V$ *um espaço vetorial sobre* $\mathbb{F}$ *e* $G$ *um grupo finito.*

*Uma* $G$*-ação invariante em* $V$ *é uma função,*

$$G \times V \longrightarrow V$$

$$(g, v) \longmapsto g.v$$

*que satisfaz,*

*1)* $1.v = v$

*2)* $(gh).v = g.(h.v)$

*3)* $g(u + v) = g.u + g.v$

*4)* $g.(\lambda v) = \lambda(g.v)$.

Observe que a um espaço vetorial $V$ sobre $\mathbb{C}$ com uma $G$-ação invariante definida em $V$ pode ser dada uma estrutura de $\mathbb{C}G$-módulo.

**Definição 5.6.** *O espaço vetorial* $\mathbb{C}G$ *com a* $G$*-ação definida como sendo a multiplicação natural* $g.v$, *com* $g \in G$ *e* $v \in \mathbb{C}G$. *É denominado o* $\mathbb{C}G$*-módulo regular.*

**Definição 5.7.** *Seja* $G$ *um subgrupo do grupo simétrico* $S_n$.

*O* $\mathbb{C}G$ *- módulo* $V$, *com base* $\beta = \{v_1, v_2, \ldots, v_n\}$, *definido pela* $G$*-ação,*

$$g.v_i = v_{g(i)} \quad \forall\ 1 \leq i \leq n \ \text{e}\ g \in G$$

*é chamado o* $\mathbb{C}G$*-módulo de permutação.*

**Proposição 5.8.** *Existe uma correspondência biunívoca entre as representações de $G$ sobre $\mathbb{F}$ e os $\mathbb{F}G$-módulos de dimensão finita.*

Uma vez entendidos esses conceitos de representações. Vamos a seguir aprender a obter uma representação $S$ de $G \times H$ de grau $r.s$ a partir de representações, $T$ do grupo $G$ com grau $r$ e $U$ do grupo $H$ com grau $s$.

Inicialmente iremos considerar $M$ e $N$ espaços vetoriais sobre $\mathbb{C}$ com base $\{m_i\}_{i=1}^{r}$ e $\{n_i\}_{i=1}^{s}$, respectivamente.

Dadas $T : M \longrightarrow M$ e $U : N \longrightarrow N$ transformações lineares. Obtemos uma nova transformação linear $T \otimes U$, definindo a aplicação

$$T \otimes U : M \otimes N \longrightarrow M \otimes N$$
$$m_i \otimes n_j \longrightarrow T(m_i) \otimes U(n_j)$$

na base de $M \otimes N$ e então a estendendo linearmente.

Fixando a base $\delta = \{m_i \otimes n_j \mid 1 \leq i \leq r \text{ e } 1 \leq j \leq s\}$ podemos computar a matriz da aplicação $T \otimes U$ com respeito a $\delta$. Observando que para quaisquer $1 \leq i \leq r$ e $1 \leq j \leq s$, temos

$$T(m_i) = \sum_{l=1}^{r} \alpha_{li}\ m_l \qquad \text{e} \qquad U(n_j) = \sum_{k=1}^{s} \beta_{kj}\ n_k,$$

então

$$\begin{aligned} T \otimes U(m_i \otimes n_j) &= T(m_i) \otimes U(n_j) \\ &= \sum_{l=1}^{r} \alpha_{li} m_l \otimes \sum_{k=1}^{s} \beta_{kj} n_k \\ &= \sum_{l=1}^{r} \sum_{k=1}^{s} \alpha_{li} \beta_{kj} m_l \otimes n_k. \end{aligned}$$

Se organizarmos a base $\delta$, em $s$ blocos com $r$ vetores, da forma:

$$m_1 \otimes n_j, m_2 \otimes n_j, \ldots, m_r \otimes n_j \qquad 1 \leq j \leq s$$

a matriz de $T \otimes U$ com relação a base $\delta$ terá $s^2$ blocos de submatrizes $r \times r$, onde o bloco $r \times r$ que aparece na $k$-ésima linha de blocos e na $j$-ésima coluna é a matriz dada por $\beta_{kj}(\alpha_{pq})$ ( em que $(\alpha_{pq})$ denota a matriz da aplicação $T$ com relação a base $\{m_i\}_{i=1}^{r}$), ou seja, podemos pensar que obtemos a matriz de $T \otimes U$ com relação a base $\delta$, considerando-se a matriz $(\beta_{kj})$ de $U$ e substituindo cada entrada $\beta_{kj}$ pela matriz $\beta_{kj}(\alpha_{pq})$.

Para exemplificar esse processo daremos um exemplo usando a mesma notação utilizada acima para o caso em que $r = 3$ e $s = 2$.

**Exemplo 5.9.** *Começamos organizando a base da forma:*

$$\delta = \{m_1 \otimes n_1, m_2 \otimes n_1, m_3 \otimes n_1, m_1 \otimes n_2, m_2 \otimes n_2, m_3 \otimes n_2\}.$$

*Sendo* $T \otimes U(m_i \otimes n_j) = \sum_{l=1}^{3}\sum_{k=1}^{2} \alpha_{li}\beta_{kj} m_l \otimes n_k$*, temos que a matriz de* $T \otimes U$ *com relação a base* $\delta$ *é dada por:*

$$\begin{bmatrix} \alpha_{11}\beta_{11} & \alpha_{12}\beta_{11} & \alpha_{13}\beta_{11} & \alpha_{11}\beta_{12} & \alpha_{12}\beta_{12} & \alpha_{13}\beta_{12} \\ \alpha_{21}\beta_{11} & \alpha_{22}\beta_{11} & \alpha_{23}\beta_{11} & \alpha_{21}\beta_{12} & \alpha_{22}\beta_{12} & \alpha_{23}\beta_{12} \\ \alpha_{31}\beta_{11} & \alpha_{32}\beta_{11} & \alpha_{33}\beta_{11} & \alpha_{31}\beta_{12} & \alpha_{32}\beta_{12} & \alpha_{33}\beta_{12} \\ \alpha_{11}\beta_{21} & \alpha_{12}\beta_{21} & \alpha_{13}\beta_{21} & \alpha_{11}\beta_{22} & \alpha_{12}\beta_{22} & \alpha_{13}\beta_{22} \\ \alpha_{21}\beta_{21} & \alpha_{22}\beta_{21} & \alpha_{23}\beta_{21} & \alpha_{21}\beta_{22} & \alpha_{22}\beta_{22} & \alpha_{23}\beta_{22} \\ \alpha_{31}\beta_{21} & \alpha_{32}\beta_{21} & \alpha_{33}\beta_{21} & \alpha_{31}\beta_{22} & \alpha_{32}\beta_{22} & \alpha_{33}\beta_{22} \end{bmatrix} = \begin{bmatrix} \beta_{11}T & \beta_{12}T \\ \beta_{21}T & \beta_{22}T \end{bmatrix}.$$

Agora, consideremos as representações

$$\begin{aligned} T : G &\longrightarrow GL(M) & \quad \text{e} \quad U : H &\longrightarrow GL(N) \\ g &\longmapsto T_g & h &\longmapsto U_h \end{aligned}$$

de um grupo finito $G$.

O produto tensorial dessas representações é definido por

$$\begin{aligned} T \otimes U :\ G \times H &\longrightarrow GL(M \otimes N) \\ (g,h) &\longmapsto T_g \otimes U_h \end{aligned}$$

e é uma representação de $G \times H$. Além disso, supondo que $T$ é uma representação de grau $r$ e $U$ é uma representação de grau $s$, temos que $T \otimes U$ é uma representação de grau $rs$.

**Exemplo 5.10.** *Consideremos a representação, do grupo diedral de ordem* 8 *dada no Exemplo 5.3,*

$$\begin{aligned} T : D_4 &\longrightarrow GL(2, \mathbb{C}) \\ a &\longrightarrow A \\ b &\longrightarrow B, \end{aligned}$$

*onde* $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *e* $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *e consideremos a representação trivial de* *grau* 2 *de* $D_4$ *dada por*

$$\begin{aligned} U : D_4 &\longrightarrow GL(2,\mathbb{C}) \\ a &\longrightarrow I_2 \\ b &\longrightarrow I_2, \end{aligned}$$

*onde* $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Então* $T \otimes U$ *é uma representação de grau* 4 *de* $D_4$ *(basta olhar para a imersão diagonal de* $D_4$ *em* $D_4 \times D_4$*) dada por,*

$$T \otimes U(a) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad T \otimes U(b) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

*e* $U \otimes T$ *é a representação de grau* 4 *de* $D_4$ *dada por*

$$U \otimes T(a) = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad U \otimes T(b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

# Referências Bibliográficas


[1] J.M.H. Adamsson, *The standard polynomial as an identity on symplectic matrices,* M.Sc thesis, University of Ottawa 1992.

[2] A.S. Amitsur, *Identities in rings with involutions,* Israel J.Math, 7, 63-68, 1969.

[3] A.S. Amitsur and J. Levitzki, *Minimal identities for algebras,* Proc. Amer. Math. Soc, 1 (1950) 449-463.

[4] M.Atiyah and I. Macdonald, *Introduction to commutative algebra,* Addison-Wesley publishing company, London, 1969.

[5] M. Dehn, *Uber die grundlagen der projektiven geometrie und allgemeine zahlsysteme,* Math. Ann. 85, 184-194, 1922.

[6] A. D'Amour and M.L Racine, *$*$-polynomial identities of matrices with symplectic involution: The low degrees* Comm. Algebra 32 (2004) 895-918.

[7] V. Drensky, *A minimal basis for the identities of a second-order matrix algebra over a fiel of characteristic 0* , Algebra and Logic, 20 (1981) 188-194.

[8] V. Drensky and A. Giambruno, *On $*$-polynomial identities of minimal degree for matrices with involution* , Boll. Unione Mat. Ital. 7 (1995) 471-482.

[9] A. Giambruno and M. Zaicev, *Polynomial identities and asymptotic methods,* Mathematical Society, 2005.

[10] G D. James, M.W. Liebeck, *Representations and characteres of groups,* Vol.1 Cambridge University Press 1993.

[11] H.D. Jordan, *Polynomial identities for matrices symmetric with respect to the symplectic involution,* Journal of Algebra, 349 (2012) 8-21.

[12] A.R. Kemer, *Ideals of Identities of Associative Algebras,* AMS Translations of Math. Monographs, Vol 87, 1988.

[13] B. Konstant, *A theorem of Frobenius, a theorem of Amitsur-Levitski and cohomology theory,* J. Math. Mech. 7 (1958) 237-264.

[14] G. Leal and A. Vieira, *A basis for* $M_{2^m}(\mathbb{C})$ *with involution formed by symmetric and skew elements* preprint.

[15] T.S. Nascimento, *Sobre as Subvariedades das Variedades de Crescimento Quase Polinomial*, dissertação de mestrado, UFMG, 2013.

[16] C. Polcino and S. K. Sehgal, *An Introduction to Group Rings,* Kluwer Academic Publishers, Netherlands, 2002.

[17] M.L. Racine, *Minimal identities for Jordan algebras of degree 2,* Comm. Algebra 13 (1985) 2493-2506.

[18] T.G. Rashkova, *$*$-polynomial identities of minimal degree in matrix algebra of low order,* Period. Math. Hungar. 34 (1998) 229-233.

[19] L.H. Rowen, *A simple proof of Konstant's theorem and a analogue for the sympletic involution,* Contemp. Math. Amer. Math. Soc, Providence, RI, (1982) 207-215.

[20] L.H. Rowen and A.K. Belov, *Computational Aspects of Polynomial Identities,* Contemp. Math. Amer. Math. Soc, Providence, RI, (1982) 207-215.

[21] L. H. Rowen, *Polynomial identities in ring theory,* Academic press, INC. London, 1980.

[22] A.R.F. Teixeira, *O Problema do Isomorfismo para Álgebras de Grupos Racionais de p-Grupos Extra-Especiais*, dissertação de mestrado, UFMG, 2006.

[23] The GAP group, *Algorithms and Programming*, versão 4.8.6 disponível em: http://www.gap-system.org, 2016.

[24] A.C. Vasconcelos, *Crescimento polinomial das codimensões e $*$-codimensões*, dissertação de mestrado, UFMG, 2013.

[25] W. Wagner, *Uber die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme* , Math. Ann. 113, 528-567, 1937.