Relatório Final de Iniciação Científica

Álgebras com Identidades Polinomiais *

Douglas Mendes — Bolsista
Prof. Dr. Plamen Emilov Kochloukov — Orientador

Instituto de Matemática, Estatística e Computação Científica
Universidade Estadual de Campinas

"A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original."
Albert Einstein

Resumo de atividades

Um dos objetivos principais desta iniciação científica foi o de complementar minha formação acadêmica em matemática, apresentando-me a uma teoria algébrica bastante recente e que vem oferecendo resultados e questões intrigantes aos pesquisadores desde sua origem. A sugestão por este tema foi dada pelo meu próprio orientador, que viu nela não somente um dos seus objetos de pesquisa, mas também uma maneira de aproveitar todo o conhecimento que obtive em álgebra durante meus anos de graduação e outras duas iniciações científicas que oportunamente realizei.

Apesar de sua contemporaneidade, devo dizer que a teoria em questão é relativamente fácil de ser estudada, ao menos do ponto de vista combinatório com a qual a abordamos e até a profundidade que eu cheguei durante os estudos da presente iniciação científica. Para tanto, empregamos os capítulos 1 ao 7 do livro [1], o artigo [2] e, ainda, trechos de [3], [4] e [5], que nos "entreteram" durante o período de agosto de 2008 à janeiro de

*Pesquisa apoiada pelo CNPq sob processo #113065/2008-6.

2009. Como é de praxe em iniciações científicas em matemática e física, cada um destes capítulos foi cuidadosamente analisado e, buscando-se uma maior fixação dos conceitos envolvidos, a maior quantidade possível de seus exercícios foi resolvida. A presente pesquisa deverá, todavia, ser interrompida a partir de fevereiro próximo, devido a conclusão de um dos meus cursos de graduação, ao meu ingresso no mestrado da matemática e a possibilidade de obter uma bolsa de estudos própria a esta categoria. Justifica-se, portanto, o formato final deste texto, escrito como um relatório final.

Não obstante seu término, os trinta meses em que fui estudante de iniciação científica do CNPq foram decisivos para minha vida profissional, tendo expandido minhas perspectivas ao academicismo e corroborado com a decisão de continuar meus estudos em matemática (em álgebra, particularmente). Sendo assim, agradeço ao CNPq por incentivar tais atividades e aos professores envolvidos, pelo apoio incondicional e dedicação em sua concretização.

Introdução

A teoria das álgebras que satisfazem a identidades polinomiais, ou, simplesmente, PI-álgebras, teve início na década de 20 a partir de uma questão geométrica e já no final dos anos 40 atingiu sua independência como tema de estudo. Originalmente ela buscava classificar *todas* as álgebras, mas tamanha generalidade não pôde, evidentemente, ser satisfatoriamente respondida, o que ocasionou algumas restrições ao problema original. Hoje em dia procura-se estudá-la através de outras frentes, seja tentando demonstrar quais identidades polinomiais uma certa classe de álgebras satisfaz, ou, o que seria o problema contrário, quais álgebras satisfazem a uma dada coleção de identidades. Algumas de suas aplicações podem ser encontradas nas áreas da teoria de invariantes, geometria não-comutativa, teoria de Lie e, mais geralmente, em álgebras não-associativas. Nesta última, inclusive, as identidades aparecem de uma maneira natural. Por exemplo: a classe de todas as álgebras associativas pode ser definida, dentro de todas as álgebras (não necessariamente associativas), por meio da identidade $(xy)z - x(yz) = 0$. Outros exemplos seriam a classe das álgebras de Lie, que é definida através da anti-comutatividade e da identidade de Jacobi, as classes das álgebras alternativas, de Jordan, etc. Ressaltamos que existe, ainda, uma teoria análoga e bem desenvolvida para grupos.

1 Algumas definições e exemplos

Precisamos fazer algumas definições antes de descrevermos a teoria propriamente dita. Exemplos são fornecidos com o intuito de ilustrá-las.

Definição 1. Um espaço vetorial A sobre um corpo $\mathbb{K}$ é uma **álgebra** se, em A, estiver definida uma operação binária $*$, denominada **multiplicação**, para a qual valha as leis distributivas pela esquerda e direita,

$$a * (b + c) = a * b + a * c \qquad \text{e} \qquad (a + b) * c = a * c + b * c,$$

e que ainda satisfaça

$$\alpha(a * b) = (\alpha a) * b = a * (\alpha b)$$

para todo a, b, $c \in A$ e $\alpha \in \mathbb{K}$. Um subespaço $B \subset A$ que seja fechado com respeito a esta multiplicação é uma **subálgebra** de A.

Exemplo 1. O espaço $M(n, \mathbb{K})$ das matrizes quadradas de ordem n é uma álgebra com a multiplicação usual de matrizes e seu subespaço $U(n, \mathbb{K})$ constituído por todas as matrizes triangulares superiores, uma subálgebra.

Definição 2. Um **ideal** de uma álgebra A é um subespaço $I \subset A$ no qual

$$a * i \in I \qquad \text{e} \qquad i * a \in I$$

para todo $a \in A$ e $i \in I$.

De agora em diante, sempre que nos referirmos a um espaço vetorial, omitiremos o corpo sobre o qual ele está definido. Portanto, a menos que especificado, estaremos trabalhando sobre um corpo $\mathbb{K}$ qualquer. Também deixaremos de indicar a multiplicação entre dois elementos a e b, representando-a apenas por ab, ao invés de $a * b$.

Definição 3. Uma álgebra A é **associativa**, se $(ab)c = a(bc)$, **comutativa**, se $ab = ba$, e **unitária**, se existir $e \in A$ tal que $ea = ae = a$, para quaisquer a, b, $c \in A$. Como de costume, denotaremos o elemento e por 1.

Por convenção, toda subálgebra de uma álgebra unitária também é unitária, isto é, o elemento 1 pertence às subálgebras da nossa álgebra.

Exemplo 2. O espaço dos polinômios $\mathbb{K}[X]$ nas variáveis comutantes de um conjunto X é uma álgebra associativa, comutativa e unitária com as operações usuais.

Existem, é claro, álgebras que não apresentam todas estas características.

Exemplo 3. As álgebras $M(n, \mathbb{K})$ e $U(n, \mathbb{K})$ são associativas e unitárias, embora não sejam comutativas para $n > 1$.

Definição 4. Se $\circ$ é uma operação bilinear definida em um espaço vetorial J que satisfaz

$$x \circ y = y \circ x, \qquad x^2 \circ (y \circ x) = (x^2 \circ y) \circ x,$$

então dizemos que J é uma **álgebra de Jordan**.

Exemplo 4. A partir de uma álgebra associativa, a multiplicação

$$x \circ y = (1/2)(xy + yx)$$

define, sobre um corpo de característica diferente de 2, uma álgebra de Jordan cujos elementos comutam entre si, mas para a qual a associatividade não se verifica.

Definição 5. Uma **álgebra de Lie** é um espaço vetorial L equipado com uma operação bilinear $[\ ,\ ] : L \times L \to L$, denominada **colchete de Lie**, que satisfaz, respectivamente, a **lei anti-comutativa** e a **identidade de Jacobi**,

$$[a, a] = 0 \qquad \text{e} \qquad [a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0,$$

para quaisquer a, b, c em L.

Exemplo 5. Toda álgebra associativa A é uma álgebra de Lie com respeito ao colchete $[a, b] = ab - ba$, a, $b \in A$.

Definição 6. O produto descrito no exemplo anterior denomina-se **comutador**.

Exemplo 6. O conjunto $sl(n, \mathbb{K})$ de todas as matrizes $n \times n$ de traço nulo é uma álgebra de Lie com o comutador.

Muitos conceitos de espaços vetoriais e os principais resultados relacionados a eles podem ser naturalmente estendidos as álgebras. Para citar apenas alguns:

Definição 7. Um **homomorfismo de álgebras** $\phi : A_1 \to A_2$ é uma transformação linear definida entre álgebras, que preserva a multiplicação, isto é, ϕ é tal que

$$\phi(a_1 * a_2) = \phi(a_1) * \phi(a_2).$$

Em particular, ϕ é um **isomorfismo de álgebras**, quando também for uma bijeção.

Definição 8. Na notação da definição anterior, os conjuntos

$$\ker \phi = \{a \in A_1 \mid \phi(a) = 0\} \qquad \text{e} \qquad \operatorname{Im} \phi = \{\phi(a) \mid a \in A_1\}$$

são, respectivamente, o **núcleo** e a **imagem** de ϕ.

Lema 1. *$\ker \phi$ e $\operatorname{Im} \phi$ são, respectivamente, ideal de A_1 e subálgebra de A_2.*

Proposição 1. *Se I é um ideal de uma álgebra A, então o conjunto A/I, cujos elementos são da forma $a + I = \{a + i \mid i \in I\}$, $a \in A$, é uma álgebra com as operações*

$$(a+I)+(b+I)=(a+b)+I, \quad \lambda(a+I)=(\lambda a)+I, \quad (a+I)(b+I)=(ab)+I,$$

definidas para todo a, $b \in A$ e $\lambda \in \mathbb{K}$.

Definição 9. A álgebra acima é conhecida como a **álgebra quociente** de A por I.

Teorema 1 (do isomorfismo). *A álgebra quociente $A_1/\ker \phi$ é isomorfa a $\phi(A_1)$.*

A noção abaixo é útil de muitos modos.

Definição 10. Seja $\mathfrak{V}$ uma classe de álgebras e $F \in \mathfrak{V}$ uma álgebra gerada por um conjunto X. F é dita **livre** em $\mathfrak{V}$ e **livremente gerada** por X se, para toda álgebra A em $\mathfrak{V}$, toda função de X em A puder ser estendida a um homomorfismo de F em A.

Definição 11. Dado um conjunto não-vazio X, uma **palavra** é uma expresão da forma

$$w = x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}, \quad x_i \in X, \quad m_i \in \mathbb{Z},\, m_i \geq 0, \quad i = 1, \ldots, k.$$

A **concatenação** de duas palavras w_1 e w_2 é dada por $w_1 w_2$.

Exemplo 7. A álgebra $\mathbb{K}\langle X\rangle$ que tem como base todas as palavras

$$x_{i_1} \ldots x_{i_n}, \quad x_{i_j} \in X, \quad n = 0, 1, 2, \ldots$$

e multiplicação definida por concatenação é livre na classe de todas as álgebras associativas e unitárias. As palavras acima são do mesmo tipo da Definição pois admitimos repetições entre os índices i_1, ..., i_n.

A própria notação indica $\mathbb{K}\langle X\rangle$ tratar-se de uma generalização de $\mathbb{K}[X]$, podendo a primeira ser interpretada como a álgebra dos polinômios em variáveis não-comutantes.

Vamos introduzir agora uma das mais importantes álgebras para a PI-teoria. Para isso, considere um espaço vetorial V com base ordenada $\{e_i \mid i \in I\}$.

Definição 12. A **álgebra de Grassmann** $E(V)$ de V é a álgebra associativa e unitária gerada pela base $\{e_i \mid i \in I\}$ e pelas relações

$$e_i e_j + e_j e_i = 0,$$

se $\operatorname{char} \mathbb{K} = 0$, ou $e_i^2 = 0$, no caso de $\operatorname{char} \mathbb{K} = 2$. Esta álgebra também é conhecida como **álgebra exterior** de V.

Pode ser demonstrado que $E(V)$ é isomorfa a álgebra quociente $\mathbb{K}\langle X\rangle/J$, onde X é o conjunto $\{x_i \mid i \in I\}$ e J é o ideal gerado por $x_i x_j + x_j x_i$, i, $j \in I$. Pode ser demonstrado que o conjunto

$$e_{i_1} \cdots e_{i_n}, \quad i_1 < \ldots < i_n, \quad i_k \in I, \quad n = 0, 1, 2, \ldots$$

é uma base para ela.

Uma última observação antes de encerrarmos a seção:

Proposição 2. *Se A e B são álgebras, então, $A \otimes B$ com multiplicação*

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb'), \quad a,\, a' \in A \text{ e } b,\, b' \in B,$$

também é uma álgebra.

2 Álgebras com identidades polinomiais

Muitos resultados clássicos admitem uma reformulação na linguagem de identidades. Por isto e outras razões que ficarão claras mais adiante, precisemos este conceito.

Definição 13. Dizemos que um polinômio não-nulo $f = f(x_1, \ldots, x_n) \in \mathbb{K}\langle X\rangle$ é uma **identidade polinomial** para uma álgebra associativa A se

$$f(a_1, \ldots, a_n) = 0 \quad \text{para todo } a_1, \ldots, a_n \in A.$$

Quando uma tal identidade existir diremos que A é uma **PI-álgebra**.

Exemplo 8. Trivialmente,

$$f(x_1, x_2) = [x_1, x_2] = x_1 x_2 - x_2 x_1$$

é uma identidade polinomial para as álgebras comutativas.

A classe das PI-álgebras é bem ampla, muito embora a existência de uma identidade polinomial não-nula para uma álgebra seja uma exigência bastante forte. Existem, é claro, álgebras que não possuem nem ao menos uma delas.

Exemplo 9. A álgebra $\mathbb{K}\langle X\rangle$ não satisfaz a nenhuma identidade polinomial não-nula. De fato, sabemos que todos os polinômios desta álgebra são combinações lineares de monômios. Se um destes polinômios pudesse ser uma identidade polinomial para $\mathbb{K}\langle X\rangle$, então, ele deveria, em particular, se anular nestes monômios. Melhor ainda: ele se anularia em suas próprias variáveis (vistas como vetores de $\mathbb{K}\langle X\rangle$) e, assim, seria o polinômio nulo, dada a independência linear de tais variáveis.

Exemplo 10. A álgebra dos operadores lineares em um espaço vetorial de dimensão infinita também não satisfaz a nenhuma identidade polinomial, uma vez que ela possui subálgebras isomorfas a $M(n, \mathbb{K})$ para todo n e cada uma delas não apresenta identidade polinomial de grau menor ou igual a $2n-1$. Observe que utilizamos aqui o resultado descrito no lema 3, a ser demonstrado nas próximas páginas.

Seja S_n o grupo simétrico em n letras. O seguinte polinômio, presente em alguns resultados importantes, utiliza-o em sua expressão.

Definição 14. O polinômio de $\mathbb{K}\langle X\rangle$

$$s_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) x_{\sigma(1)} \cdots x_{\sigma(n)},$$

onde $\operatorname{sgn} \sigma$ é o sinal da permutação σ, é denominado **polinômio *standard*** de grau n.

Por ora, mostremos com o auxílio dele que

Proposição 3. *Toda álgebra associativa de dimensão finita é uma PI-álgebra.*

Demonstração: Seja A tal álgebra, com $\dim A = m$ e $m < n$. Fixemos uma permutação τ de S_n. Então,

$$\begin{aligned} s_n(x_{\tau(1)}, \ldots, x_{\tau(n)}) &= \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) x_{\sigma\tau(1)} \cdots x_{\sigma\tau(n)} \\ &= \sum_{\mu \in S_n} (\operatorname{sgn} \mu\tau) x_{\mu(1)} \cdots x_{\mu(n)} \\ &= (\operatorname{sgn} \tau) \sum_{\mu \in S_n} (\operatorname{sgn} \mu) x_{\mu(1)} \cdots x_{\mu(n)} \\ &= (\operatorname{sgn} \tau) s_n(x_1, \ldots, x_n). \end{aligned}$$

Logo, s_n é anti-simétrica e, daí, $s_n(a_1, \ldots, a_n) = 0$ para todo $a_1, \ldots, a_n \in A$. De fato, seja $\{e_1, \ldots, e_m\}$ uma base de A, então $a_i = \sum_{j=1}^{m} a_{ij} e_j \in A$. Mas o polinômio $s_n(x_1, \ldots, x_n)$ é linear em cada uma das suas variáveis, portanto $s_n(a_1, \ldots, a_n)$ é uma combinação linear de expressões do tipo $s_n(e_{i_1}, \ldots, e_{i_n})$, onde $1 \leq i_j \leq m$. Observe que então existem $p \neq q$ tais que $i_p = i_q$. Usando-se o fato estabelecido no início da demonstração, que s_n é anti-simétrico, obtemos que $s_n(e_{i_1}, \ldots, e_{i_n}) = 0$. $\square$

Definição 15. Dizemos que uma identidade polinomial g **decorre (segue)** de uma identidade f se g é identidade em qualquer álgebra onde f é identidade.

Pode ser demonstrado que g segue de f se g está no ideal gerado por todos $f(p_1, \ldots, p_n)$, onde p_i são polinômios.

Proposição 4. *O polinômio standard de grau $n+1$ decorre daquele de grau n.*

Demonstração: De fato, mostraremos que

$$s_{n+1}(x_1,\ldots,x_{n+1}) = \textstyle\sum_{i=1}^{n+1}(-1)^{i-1}x_i s_n(x_1,\ldots,\widehat{x}_i,\ldots,x_{n+1}),$$

onde $\widehat{x}_i$ significa que a variável x_i não participa da respectiva expressão. Para isso, observamos que todas as permutações de um conjunto $\{x_1,\ldots,x_{n+1}\}$ podem ser obtidas fixando-se cada um dos seus elementos e considerando-se todas as permutações possíveis dos demais. Isto é verdade, porque, a cada letra fixada, obtemos $n!$ permutações e temos $n+1$ letras para fixar, ou seja, conseguimos $(n+1)!$ permutações distintas de um conjunto com $n+1$ elementos. Sendo assim,

$$\begin{aligned} s_{n+1}(x_1,\ldots,x_{n+1}) &= \textstyle\sum_{\sigma \text{ fixa } 1}(\mathrm{sgn}\,\sigma)x_1x_{\sigma(2)}\ldots x_{\sigma(n+1)} \\ &+ \textstyle\sum_{\sigma \text{ fixa } 2}(\mathrm{sgn}\,\sigma)x_{\sigma(1)}x_2\ldots x_{\sigma(n+1)} \\ &+ \cdots + \\ &+ \textstyle\sum_{\sigma \text{ fixa } n+1}(\mathrm{sgn}\,\sigma)x_{\sigma(1)}x_{\sigma(2)}\ldots x_{n+1}. \end{aligned}$$

Definindo, daí, τ_{ij}^{σ} como sendo a transposição $(i\;\sigma(i-j))$ podemos reescrever cada permutação σ do grupo S_{n+1} como

$$\sigma = \tau_{i,i-1}\tau_{i,i-2}\cdots\tau_{i,2}\tau_{i,1}\cdot\tau_{i,1}\tau_{i,2}\cdots\tau_{i,i-2}\tau_{i,i-1}\cdot\sigma = \tau_{i,i-1}\tau_{i,i-2}\cdots\tau_{i,2}\tau_{i,1}\cdot\mu,$$

onde o índice σ de τ_{ij}^{σ} fica subentendido. Ganhamos, assim, uma permutação μ que se comporta essencialmente como a própria σ, simplesmente deslocando a variável fixa x_i de cada monômio $x_{\sigma(1)}\cdots x_i\cdots x_{\sigma(n+1)}$ para a esquerda de todas as demais. Logo,

$$\begin{aligned} s_{n+1}(x_1,\ldots,x_{n+1}) &= \textstyle\sum_{\mu \text{ fixa } 1}(\mathrm{sgn}\,\mu)x_1x_{\mu(2)}\ldots x_{\mu(n+1)} \\ &+ \textstyle\sum_{\mu \text{ fixa } 2}(\mathrm{sgn}\,\tau_{2,1}\cdot\mu)x_2x_{\mu(1)}\ldots x_{\mu(n+1)} \\ &+ \cdots + \\ &+ \textstyle\sum_{\mu \text{ fixa } n+1}(\mathrm{sgn}\,\tau_{n+1,n}\tau_{n+1,n-1}\cdots\tau_{n+1,1}\cdot\mu)x_{n+1}x_{\mu(1)}\ldots x_{\mu(n)}. \end{aligned}$$

Acontece, contudo, que a função sgn é um homomorfismo de grupos e, por isso,

$$\mathrm{sgn}\,(\tau_1\tau_2\cdots\tau_j\cdot\mu) = \mathrm{sgn}\,\tau_1\cdot\mathrm{sgn}\,\tau_2\cdots\mathrm{sgn}\,\tau_j\cdot\mathrm{sgn}\,\mu = (-1)^j\mathrm{sgn}\,\mu.$$

Isto é suficiente para concluirmos esta proposição. □

Algumas definições são necessárias para que prossigamos.

Definição 16. Sejam $f = f_i(x_1,\ldots,x_{n_i})$, $i\in I$, alguns polinômios de $\mathbb{K}\langle X\rangle$. A classe $\mathfrak{V}$ de todas as álgebras associativas que têm os polinômios anteriores como identidades polinomiais é a **variedade** determinada pelo sistema $\{f_i \mid i \in I\}$. O conjunto $T(\mathfrak{V})$ de todas as identidades polinomiais satisfeitas pela variedade $\mathfrak{V}$ é o **T-ideal** de $\mathfrak{V}$.

Na notação acima costuma-se dizer que $T(\mathfrak{V})$ é gerado por $\{f_i \mid i \in I\}$ ou, ainda, que $\{f_i \mid i \in I\}$ é uma base para o T-ideal, embora $T(\mathfrak{V})$ não contenha apenas combinações lineares dos elementos deste conjunto. É convenção denotar, também, o T-ideal de todas as identidades polinomiais satisfeitas por uma álgebra A por $T(A)$.

Com relação a variedades e T-ideais sabemos que

Teorema 2. *Existe uma bijeção entre variedades de álgebras associativas e T-ideais dada por $\mathfrak{V} \mapsto T(\mathfrak{V})$. Esta bijeção inverte as inclusões.*

Teorema 3 (Birkhoff). *Uma condição necessária e suficiente para que uma classe de álgebras seja uma variedade é que ela seja fechada com relação a somas diretas (inclusive infinitas), subálgebras e álgebras quocientes.*

O teorema acima tem muitas aplicações, sendo também conhecido como **teorema HSP**, onde H, S e P referem-se, respectivamente, as operações fechadas de tomar homomorfismos, subálgebras e produtos.

Definição 17. Denotemos por $\deg_{x_i} f$ o grau de $f = f(x_1, \ldots, x_n) \in \mathbb{K}\langle X \rangle$ com relação a variável x_i. A n-upla $(\deg_{x_1} f, \ldots, \mathrm{def}_{x_n} f)$ é o **multigrau** de f.

Definição 18. Um polinômio é dito **multilinear** se seu multigrau é $(1, \ldots, 1)$ e, **multihomogêneo** se todos os seus monômios têm o mesmo multigrau.

Existe um método, conhecido como **processo de linearização**, que reduz um polinômio multihomogêneo f de multigrau $(k_1, \ldots, k_n)$ a um polinômio multilinear. Ele emprega o seguinte operador, onde $\widehat{y_j}$ indica a parcela ausente da respectiva soma:

$$\begin{aligned} L_i^k(f) = {} & f(x_1, \ldots, x_{i-1}, y_1 + \cdots + y_k, x_{i+1}, \ldots, x_n) \\ & - \textstyle\sum_{j=1}^k f(x_1, \ldots, x_{i-1}, y_1 + \cdots + \widehat{y_j} + \cdots + y_k, x_{i+1}, \ldots, x_n) \\ & + \textstyle\sum_{1 \le j_1 < j_2 \le k} f(x_1, \ldots, x_{i-1}, y_1 + \cdots + \widehat{y}_{j_1} + \cdots + \widehat{y}_{j_2} + \cdots + y_k, x_{i+1}, \ldots, x_n) \\ & - \cdots + (-1)^{k-1} \textstyle\sum_{j=1}^k f(x_1, \ldots, x_{i-1}, y_j, x_{i+1}, \ldots, x_n). \end{aligned}$$

A **forma linearizada** de f é dada por $L_1^{k_1} \cdots L_n^{k_n}(f)$.

Exemplo 11. A forma linearizada de $f(x_1, x_2) = x_1^2 x_2 x_1$ é

$$y_1 y_2 x_2 y_3 + y_1 y_3 x_2 y_2 + y_2 y_3 x_2 y_1 + y_2 y_1 x_2 y_3 + y_3 y_1 x_2 y_2 + y_3 y_2 x_2 y_1.$$

De fato, observando inicialmente que $L_1^3L_2^1(f) = L_1^3(f)$, pois o polinômio f já é linear na variável x_2, temos

$$\begin{aligned}
L_1^3(f) &= (y_1+y_2+y_3)^2x_2(y_1+y_2+y_3) \\
&\quad - (y_2+y_3)^2x_2(y_2+y_3) - (y_1+y_3)^2x_2(y_1+y_3) - (y_1+y_2)^2x_2(y_1+y_2) \\
&\quad + y_3^2x_2y_3 + y_2^2x_2y_2 + y_1^2x_2y_1 \\
&= ((y_1+y_2)^2 + (y_1+y_2)y_3 + y_3(y_1+y_2) + y_3^2)x_2(y_1+y_2+y_3) \\
&\quad - (y_2^2 + y_2y_3 + y_3y_2 + y_3^2)x_2(y_2+y_3) \\
&\quad - (y_1^2 + y_1y_3 + y_3y_1 + y_3^2)x_2(y_1+y_3) \\
&\quad - (y_1+y_2)^2x_2(y_1+y_2) \\
&\quad + y_3^2x_2y_3 + y_2^2x_2y_2 + y_1^2x_2y_1 \\
&= (y_1+y_2)^2x_2(y_1+y_2) + (y_1+y_2)^2x_2y_3 \\
&\quad + (y_1+y_2)y_3x_2(y_1+y_3) + (y_1+y_2)y_3x_2y_2 \\
&\quad + y_3(y_1+y_2)x_2(y_1+y_3) + y_3(y_1+y_2)x_2y_2 \\
&\quad + y_3^2x_2y_1 + y_3^2x_2y_2 + y_3^2x_2y_3 \\
&\quad - (y_2^2 + y_2y_3 + y_3y_2 + y_3^2)x_2(y_2+y_3) \\
&\quad - (y_1^2 + y_1y_3 + y_3y_1 + y_3^2)x_2(y_1+y_3) \\
&\quad - (y_1+y_2)^2x_2(y_1+y_2) \\
&\quad + y_3^2x_2y_3 + y_2^2x_2y_2 + y_1^2x_2y_1 \\
&= (y_1^2 + y_1y_2 + y_2y_1 + y_2^2)x_2y_3 \\
&\quad + y_2y_3x_2y_1 + y_2y_3x_2y_3 + y_1y_3x_2y_2 + y_2y_3x_2y_2 \\
&\quad + y_3y_2x_2y_1 + y_3y_2x_2y_3 + y_3y_1x_2y_2 + y_3y_2x_2y_2 \\
&\quad - y_2^2x_2(y_2+y_3) - y_2y_3x_2(y_2+y_3) - y_3y_2x_2(y_2+y_3) - y_1^2x_2(y_1+y_3) \\
&\quad + y_2^2x_2y_2 + y_1^2x_2y_1 \\
&= y_1y_2x_2y_3 + y_1y_3x_2y_2 + y_2y_3x_2y_1 + y_2y_1x_2y_3 + y_3y_1x_2y_2 + y_3y_2x_2y_1,
\end{aligned}$$

como gostaríamos.

T-ideais sobre certos corpos têm uma característica interessante que permite que muitos resultados da PI-teoria sejam enunciados a partir de identidades multilineares.

Proposição 5. *Sobre um corpo de característica nula, todo T-ideal é gerado por suas identidades polinomiais multilineares.*

Vamos aproveitar a proposição acima e levantar uma questão interessante. Podemos concluir, pela proposição 3, que a álgebra matricial $M(n, \mathbb{K})$ é uma PI-álgebra, satisfazendo, por exemplo, s_{n^2+1}, pois $\dim M(n, \mathbb{K}) = n^2$. Curiosamente, entretanto,

Proposição 6. *$M(n, \mathbb{K})$, sobre um corpo de característica nula, não satisfaz a nenhuma identidade polinomial de grau inferior a $2n$.*
Demonstração: Em vista da proposição 5 basta mostrarmos que a álgebra $M(n, \mathbb{K})$ não possui nenhuma identidade polinomial multilinear. Pois bem, um polinômio multilinear qualquer em m variáveis, $m < 2n$, é da forma

$$f(x_1, \ldots, x_m) = \textstyle\sum_{\sigma \in S_m} a_\sigma x_{\sigma(1)} \cdots x_{\sigma(m)}.$$

Como estamos interessados em identidades polinomiais não-triviais, sabemos que existe ao menos um a_σ não-nulo (a menos de "renomear" as variáveis) o qual, por simplicidade, tomaremos como sendo a_1. Isto sempre é possível, pois

$$f(x_1, \ldots, x_m) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(m)}),$$

já que o polinômio f é determinado considerando-se todas as possíveis combinações dos índices 1, ..., m. Seja, daí, $\{e_{ij} \mid 1 \leq i \leq j \leq n\}$ a base canônica da álgebra matricial em questão, cujos elementos sabemos satisfazer a relação $e_{ij}e_{rs} = \delta_{jr}e_{is}$ (aqui δ_{jr} representa a função delta de Kronecker). Se, então, $m = 2r$ temos trivialmente que

$$f(e_{11}, e_{12}, e_{22}, e_{23}, \ldots, e_{r,r+1}) = a_1 e_{1,r+1} \neq 0$$

e, se $m = 2r - 1$,

$$f(e_{11}, e_{12}, e_{22}, e_{23}, \ldots, e_{rr}) = a_1 e_{1r} \neq 0.$$

Logo, nenhum polinômio multilinear de grau $< 2n$ é identidade para $M(n, \mathbb{K})$. $\square$

Dada a importância da álgebra de matrizes é natural se perguntar pela identidade polinomial de menor grau satisfeita por $M(n, \mathbb{K})$. A resposta a esta questão somente foi dada em 1950 pelos matemáticos Amitsur e Levitski, com uma prova bastante complexa. Outras demonstrações surgiram mais tarde, sendo, talvez, a mais simples delas fornecida por Rosset em [2]. Devido a sua extensão, será necessário, entretanto, dedicar toda uma seção deste documento para discutí-la. Por enquanto, contentemo-nos então em mostrar apenas mais algumas identidades polinomiais para álgebras matriciais específicas, cuja importância, sentimos dizer, somente ficará evidente daqui a pouco, quando discorrermos sobre o problema de Specht.

Proposição 7. *$M(2, \mathbb{K})$ satisfaz s_4 e $[[x_1, x_2]^2, x_3]$.*
Demonstração: Provaremos, inicialmente, que o polinômio s_4 é uma identidade polino-

mial para a álgebra de matrizes 2×2. Façamos isto observando que a expressão

$$x_1x_2x_3x_4 - x_2x_1x_3x_4 - x_1x_2x_4x_3 + x_2x_1x_4x_3 = [x_1, x_2][x_3, x_4]$$

certamente participa de s_4 e que a ela podemos corresponder naturalmente o conjunto

$$V_4 = \{\mathrm{id}, (12), (34), (12)(34)\}$$

de permutações do grupo S_4, o qual é isomorfo ao grupo de Klein-4 e, por isso, normal em S_4. Consideremos, daí, o quociente S_4/V_4, que sabemos ser um grupo finito. Aplicando o teorema de Lagrange, descobrimos que S_4/V_4 possui seis classes laterais, cada uma das quais relacionada a uma única expressão como a anterior. Evidentemente, nenhuma destas expressões compartilham termos, pois classes laterais são disjuntas. Logo, todas elas são distintas e estas, em conjunto, envolvem vinte e quatro monômios em quatro variáveis. Portanto,

$$s_4(x_1, x_2, x_3, x_4) = 2([x_1, x_2] \circ [x_3, x_4] + [x_1, x_3] \circ [x_4, x_2] + [x_1, x_4] \circ [x_2, x_3]).$$

Tomemos, então, uma base de $M(2, \mathbb{K})$, digamos $\{1 = e_{11} + e_{22}, e_{12}, e_{21}, e_{22}\}$, onde e_{ij} são como no lema 2. Temos, assim, que $s_4(1, e_{12}, e_{21}, e_{22}) = 0$, pois a matriz identidade comuta com qualquer outra matriz e ela aparece em exatamente um dos comutadores de cada parcela da soma acima. Logo,

$$s_4(a_1, a_2, a_3, a_4) = 0 \quad \text{para todo } a_1,\ a_2,\ a_3,\ a_4 \in M(n, \mathbb{K}),$$

pois o polinômio *standard* é multilinear.

Resta, agora, averiguar somente a segunda identidade. Pois bem, sabemos que o polinômio característico de uma matriz a quadrada de ordem 2 é

$$t^2 - (\mathrm{tr}\, a)t + \det a.$$

Tomemos, então, esta matriz como sendo o comutador de duas outras, isto é, façamos $a = [a_1, a_2]$. Agindo desta forma, obtemos que $\mathrm{tr}\, a = 0$, uma vez que o traço de uma matriz é um funcional linear com a propriedade de que $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ para todo a, $b \in M(2, \mathbb{K})$. Logo, $t^2 = -\det a$, ou ainda, $a^2 = -(\det a)1$, já que toda matriz se anula em seu polinômio característico. Portanto, a^2 é uma matriz múltipla da identidade e, assim, deve comutar com qualquer outra matriz. Então, $[a^2, a_3] = 0$, ou seja,

$$[[a_1, a_2]^2, a_3] = 0$$

para quaisquer a_1, a_2, $a_3 \in M(2, \mathbb{K})$. □

Definição 19. O polinômio $[[x_1, x_2]^2, x_3]$ é a **identidade de Hall** para $M(2, \mathbb{K})$.

Proposição 8. *$U(n, \mathbb{K})$ satisfaz o polinômio $[x_1, x_2] \cdots [x_{2n-1}, x_{2n}]$.*

Demonstração: Sejam u_1 e u_2 matrizes triangulares superiores de ordem n. Sabemos que u_1u_2 e u_2u_1 também são matrizes triangulares superiores, pois $U(n, \mathbb{K})$ é uma álgebra. Além disso, as entradas diagonais do comutador de u_1 e u_2 são

$$\begin{aligned}([u_1, u_2])_{ii} &= (u_1u_2)_{ii} - (u_2u_1)_{ii} \\ &= \textstyle\sum_{j=1}^{n}(u_{1,ij}u_{2,ji} - u_{2,ij}u_{1,ji}) \\ &= \textstyle\sum_{j=1}^{i}(u_{1,ij}u_{2,ji} - u_{2,ij}u_{1,ji}) \\ &= u_{1,ii}u_{2,ii} - u_{2,ii}u_{1,ii} = 0,\end{aligned}$$

uma vez que $u_{1,ji}$, $u_{2,ji}$ são zeros para $j > i$ e $u_{1,ij}$, $u_{2,ij}$, zeros para $j < i$. Portanto, $[u_1, u_2]$ é uma matriz triangular estritamente superior. Afirmamos que um produto de n destas matrizes resulta na matriz nula. De fato, poderíamos mostrar, como acabamos de fazer, que o produto de duas matrizes triangulares estritamente superiores é uma matriz triangular estritamente superior com zeros também na diagonal imediatamente acima da diagonal principal. Suponha, por isso, que um produto de $n-1$ destas matrizes seja uma matriz triangular estritamente superior com as $n-2$ primeiras diagonais acima da diagonal principal nulas. Considerando, daí, n matrizes triangulares estritamente superiores, v_1, ..., v_n, e notando que o produto usual de matrizes é associativo, teríamos

$$v_1v_2\cdots v_n = (v_1\cdots v_{n-1})v_n$$

e, assim, a única possível entrada não-nula neste produto seria $(v_1v_2\cdots v_n)_{1n}$. Contudo,

$$\begin{aligned}(v_1v_2\cdots v_n)_{1n} &= ((v_1v_2\cdots v_{n-1})v_n)_{1n} \\ &= \textstyle\sum_{j=1}^{n}(v_1v_2\cdots v_{n-1})_{1j}(v_n)_{jn} \\ &= (v_1v_2\cdots v_{n-1})_{1n}(v_n)_{nn} \\ &= 0,\end{aligned}$$

pois $(v_n)_{nn} = 0$. Logo, $[u_1, u_2][u_3, u_4]\cdots[u_{2n-1}, u_{2n}] = 0$ para todo $u_i \in U(n, \mathbb{K})$. □

O próximo resultado sugere uma resposta para o problema da identidade polinomial de menor grau satisfeita por $M(n, \mathbb{K})$.

Proposição 9. *O polinômio s_{2n} também é uma identidade polinomial para $U(n, \mathbb{K})$.*
Demonstração: Considere o polinômio

$$f(x_1, \ldots, x_{2n}) = [x_1, x_2][x_3, x_4]\cdots[x_{2n-1}, x_{2n}]$$

que acabamos de mostrar ser uma identidade polinomial para a álgebra de matrizes triangulares superiores. Esta é, obviamente, uma maneira bastante compacta de escrever seus 2^n monômios, dos quais, $x_1x_2x_3x_4\cdots x_{2n-1}x_{2n}$, é o primeiro deles. Considere, por isso, todas as expressões da forma

$$(\text{sgn } \sigma)[x_{\sigma(1)}, x_{\sigma(2)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}], \quad \sigma \in S_{2n}. \tag{1}$$

Afirmamos que $x_1x_2x_3x_4 \cdots x_{2n-1}x_{2n}$ aparece exatamente 2^n vezes no conjunto de todas estas expressões (em realidade, isto vale para qualquer termo presente em uma delas). De fato, existem duas maneiras de se conseguir x_1x_2 logo no primeiro comutador de (1): empregando-se as permutações $\sigma = \text{id}$ e $\sigma = (12)$ (quando $\sigma = (12)$ consegue-se, contudo, $-x_1x_2$, mas isto não importa, visto que o sinal negativo é cancelado com (sgn (12))). Existem duas maneiras, também, de se obter x_3x_4 no segundo comutador de (1): tomando-se $\sigma = (34)$ e $\sigma = (12)(34)$ (a primeira delas dá $-x_3x_4$, mas como sgn $(34) = -1$, não há problemas). Não é difícil de perceber, então, que se continuássemos com este procedimento acabaríamos com duas possibilidades de escrever $x_{2n-1}x_{2n}$ no n-ésimo comutador, o que, por sua vez, resulta em um total de 2^n aparições do monômio $x_1x_2x_3x_4 \cdots x_{2n-1}x_{2n}$. Evidentemente, todas as permutações de $x_1x_2x_3x_4 \cdots x_{2n-1}x_{2n}$ aparecem, pois permitimos que σ percorresse todo o grupo S_{2n}. Logo, contamos $(2n)!$ monômios diferentes, cada um aparecendo 2^n vezes. Além disso, estes são todos os monômios que aparecem nestas expressões. Portanto, para $a_1, \ldots, a_{2n} \in U(n, \mathbb{K})$ temos:

$$\begin{aligned} 0 &= \textstyle\sum_{\sigma \in S_{2n}} (\text{sgn } \sigma)[a_{\sigma(1)}, a_{\sigma(2)}] \cdots [a_{\sigma(2n-1)}, a_{\sigma(2n)}] \\ &= 2^n \textstyle\sum_{\sigma \in S_{2n}} (\text{sgn } \sigma) a_{\sigma(1)} \cdots a_{\sigma(2n)} = 2^n s_{2n}(a_1, \ldots, a_{2n}). \end{aligned}$$

Por isso, $s_{2n}(a_1, \ldots, a_{2n}) = 0$, quaisquer que sejam $a_1, \ldots, a_{2n} \in U(n, \mathbb{K})$. Assim, s_{2n} é uma identidade polinomial para a álgebra das matrizes triangulares superiores. $\square$

Até agora discutimos extensivamente a álgebra matricial e algumas de suas subálgebras, nos esquecendo, contudo, de tratar propriamente de uma outra álgebra muito importante para a PI-teoria: a álgebra de Grassmann. Mostremos, por isso, que

Proposição 10. *A álgebra de Grassmann satisfaz o polinômio* $[[x_1, x_2], x_3]$.

Demonstração: Dado um espaço vetorial V, tomemos quaisquer três vetores de uma base da álgebra de Grassmann associada a ele:

$$a_1 = e_{i_1} \ldots e_{i_r}, \quad a_2 = e_{j_1} \ldots e_{j_s} \quad \text{e} \quad a_3 = e_{k_1} \ldots e_{k_t}.$$

Sabemos que $e_ue_v = -e_ve_u$ nesta álgebra e, por isso,

$$[a_1, a_2] = e_{i_1} \cdots e_{i_r} e_{j_1} \cdots e_{j_s} - e_{j_1} \cdots e_{j_s} e_{i_1} \cdots e_{i_r} = (1 - (-1)^{rs}) e_{i_1} \cdots e_{i_r} e_{j_1} \cdots e_{j_s},$$

onde a potência rs indica o número mínimo de transposições necessárias para ordenar a_2a_1 em função crescente de seus índices. Não é difícil de ver, então, que a expressão anterior se anula para r ou s pares. Suponha, por isso, que a_1 e a_2 sejam ambos números ímpares. Desta forma, $[a_1, a_2]$ será uma combinação não-nula de dois monômios de comprimento par. Portanto, $[[a_1, a_2], a_3] = 0$, qualquer que seja o comprimento de a_3. Logo, o polinômio $[[x_1, x_2], x_3]$ é uma identidade polinomial para a álgebra de Grassmann, pois é multilinear e acabamos de ver que ele se anula em uma base desta. $\square$

Para finalizar esta seção, mencionemos que

Teorema 4 (Regev). *O produto tensorial de duas PI-álgebras é uma PI-álgebra.*

3 O problema de Specht

Uma das razões que nos motivou a introduzir a noção de variedades de álgebras foi a de podermos, com ela, classificar as álgebras através de suas identidades polinomiais. Seria bastante conveniente, contudo, se pudéssemos realizar esta tarefa de classificação com meios finitos. Para deixar claro o que estamos dizendo, considere que

Definição 20. Uma variedade de álgebras associativas $\mathfrak{V}$ tem uma **base finita**, se ela puder ser determinada por um sistema finito de identidades polinomiais. Caso contrário, ela tem uma **base infinita**. Se todas as subvariedades de $\mathfrak{V}$, inclusive a própria $\mathfrak{V}$, tiverem base finita, então diz-se que $\mathfrak{V}$ tem a **propriedade de Specht**.

Perguntamos, agora, pelo que ficou conhecido como **Problema de Specht**:

Toda variedade de álgebras associativas sobre um corpo de característica 0, tem base finita?

Podemos fazer uma pergunta análoga para o caso de álgebras de Lie e/ou para álgebras sobre qualquer corpo, não necessariamente de característica 0.

A resposta é não! O primeiro contra-exemplo, por exemplo, foi dado por Vaughan-Lee, em 1970, para álgebras de Lie sobre corpos de característica 2. Em 1999, Belov, Shschigolev, e Grishin, de maneira independente, construiram exemplos para álgebras associativas sobre corpos infinitos de característica positiva.

O seguinte teorema foi provado, em 1987, e é muito forte:

Teorema 5 (Kemer). *Toda variedade de álgebras associativas sobre um corpo de característica nula tem uma base finita para suas identidades polinomiais.*

A demonsração do Teorema de Kemer é muito complexa. Mais tarde o teorema foi adaptado para o caso de álgebras de Lie de dimensão finita, e para uma ampla classe de álgebras de Jordan (tudo em característica 0).

O problema de Specht tem sido um dos principais problemas na teoria de variedades de álgebras nas últimas décadas, sendo o objeto de estudos de muitos matemáticos. Ainda assim, ele continua em aberto para álgebras associativas sobre corpos de característica positiva e para álgebras de Lie sobre um corpo de característica nula.

Fornecemos abaixo alguns resultados bastante concretos a respeito de álgebras com base finita para o T-ideal de suas identidades polinomiais. Todos os resultados envolvidos são de álgebras e identidades polinomiais apresentadas na seção 2 deste texto.

Teorema 6 (Krakowski, Regev). *O T-ideal de uma álgebra de Grassmann é gerado por* $[[x_1, x_2], x_3]$.

Teorema 7 (Razmyslov, Drensky). *As identidades polinomiais de* $M(2, \mathbb{K})$ *seguem do polinômio standard* s_4 *e da identidade de Hall, quando* $\operatorname{char} \mathbb{K} = 0$*. Ainda mais: estes polinômios são independentes como identidades, isto é, um não pode ser obtido a partir do outro.*

Teorema 8. *O polinômio*

$$f(x_1, \ldots, x_{2n}) = [x_1, x_2] \cdots [x_{2k-1}, x_{2k}]$$

gera o T-ideal de $U(n, \mathbb{K})$.

4 O teorema de Amitsur e Levitski

Nesta seção demonstraremos o teorema de Amitsur e Levitski que identifica a identidade polinomial de menor grau satisfeita pela álgebra matricial. A prova que seguimos aqui é, em linhas gerais, àquela publicada por Rosset em [2]. Antes de começarmos, entretanto, vamos precisar de algumas poucas definições e um resultado auxiliar.

Definição 21. O polinômio abaixo

$$p_k(x_1, \ldots, x_n) = x_1^k + \cdots x_n^k \in \mathbb{K}\langle x_1, \ldots, x_n \rangle$$

é conhecido como a **soma de potências** de grau k em n variáveis. Por sua vez,

$$e_k(x_1, \ldots, x_n) = \textstyle\sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k} \in \mathbb{K}\langle x_1, \ldots, x_n \rangle, \quad k \le n,$$

é chamado de **polinômio elementar** de grau k em n variáveis.

Estas duas classes de polinômios aparecem com freqüência em álgebra e, entre outras coisas, constituem bases para o espaço de polinômios simétricos (no caso das somas de potências, somente para corpos de característica nula). A seguinte proposição relaciona uma com a outra.

Proposição 11. *Os polinômios e_k e p_k em n variáveis são tais que*

$$p_k - p_{k-1}e_1 + p_{k-2}e_2 - \cdots + (-1)^{k-1}p_1e_{k-1} + (-1)^k ke_k = 0,$$

se $k \leq n$, e

$$p_k - p_{k-1}e_1 + p_{k-2}e_2 - \cdots + (-1)^{n-1}p_{k-n+1}e_{n-1} + (-1)^n p_{k-n}e_n = 0,$$

para $k > n$.

Definição 22. As expressões acima são conhecidas como **identidades de Newton**.

Enfim,

Teorema 9 (Amitsur-Levitski). *O polinômio standard s_{2n} é uma identidade polinomial para a álgebra $M(n, \mathbb{K})$ das matrizes $n \times n$ definidas sobre um corpo $\mathbb{K}$ qualquer.*
Demonstração: Seja V um espaço vetorial e $\{e_1, \ldots, e_{2n}\}$ uma base ordenada para ele. Podemos assumir, sem perda de generalidade, que o corpo $\mathbb{K}$ sobre o qual V está definido é de característica nula. Isto é possível porque desejamos mostrar que

$$s_{2n}(a_1, \ldots, a_{2n}) = 0$$

para todo a_1, …, $a_{2n} \in M(n, \mathbb{K})$ e o lado esquerdo desta igualdade é uma matriz cujas entradas são polinômios de coeficientes inteiros, 1, -1 e 0, nas entradas das matrizes a_i. Pode ser demonstrado que, se todos estes polinômios se anulassem em qualquer corpo infinito, então eles seriam, necessariamente, identicamente nulos. Se, por outro lado, o nosso corpo é finito, esses coeficientes irão pertencer ao subcorpo primo $\mathbb{Z}_p$, para algum primo p. Mas $\mathbb{Z} \subset \mathbb{Q}$ e $\mathbb{Z}_p$ é uma imagem homomorfa de $\mathbb{Z}$. Assim, basta demonstrar o teorema somente no caso quando a característica do corpo é 0.

Consideremos, daí, a álgebra de Grassmann E de V e uma de suas subálgebras, F, que tomamos como sendo gerada por $1 \in \mathbb{K}$ e pelo conjunto $\{e_ie_j \mid i < j\}$ (observe que F é uma álgebra comutativa sobre $\mathbb{K}$, já que seus vetores satisfazem trivialmente a identidade $[x_1, x_2] = 0$, segundo o argumento que apresentamos na proposição 9). Identifiquemos, então, $M(n, \mathbb{K}) \otimes E$ com $M(n, E)$, isto é, olhemos para o produto tensorial da álgebra matricial pela álgebra de Grassmann como sendo a álgebra de matrizes definidas sobre E. Tomemos, por fim,

$$a = a_1e_1 + a_2e_2 + \cdots + a_{2n}e_{2n} \in M(n, E).$$

Afirmamos, daí, que

$$a^k = \sum_{1\leq i_1<\cdots<i_k\leq 2n} s_k(a_{i_1},\ldots,a_{i_k})e_{i_1}\cdots e_{i_k} \tag{2}$$

para todo $k \geq 1$. De fato, não há nada para provar se $k = 1$. Suponha, por isso, que

$$a^m = \sum_{1\leq i_1<\ldots<i_m\leq 2n} s_m(a_{i_1},\ldots,a_{i_m})e_{i_1}\cdots e_{i_m},$$

onde $m > 1$. Assim,

$$\begin{aligned}
a^{m+1} = aa^m &= \sum_{i_{m+1}=1}^{2n} a_{i_{m+1}}e_{i_{m+1}} \cdot \sum_{1\leq i_1<\cdots<i_m\leq 2n} s_m(a_{i_1},\ldots,a_{i_m})e_{i_1}\cdots e_{i_m}\\
&= \sum_{1\leq i_1<\cdots<i_m\leq 2n} \sum_{i_{m+1}=1}^{2n} a_{i_{m+1}} s_m(a_{i_1},\ldots,a_{i_m})e_{i_{m+1}}e_{i_1}\cdots e_{i_m} \qquad (3)\\
&= \sum_{1\leq i_1<\cdots<i_m<i_{m+1}\leq 2n}\Big(\sum_{j=1}^{m+1}(-1)^{j-1}a_{i_j}s_m(a_{i_1},\ldots,\widehat{a}_{i_j},\ldots,a_{i_{m+1}})\Big)e_{i_1}\cdots e_{i_m}e_{i_{m+1}}\\
&= \sum_{1\leq i_1<\cdots<i_{m+1}\leq 2n} s_{m+1}(a_{i_1},\ldots,a_{i_{m+1}})e_{i_1}\cdots e_{m+1},
\end{aligned}$$

onde a quarta igualdade exige alguma justificativa. Seja ela: dado um subconjunto qualquer de $\{1, 2, \ldots, 2n\}$ com $m+1$ números, digamos $\{j_1, \ldots, j_{m+1}\}$, podemos ordenar seus elementos (pois tratam-se de números naturais) e obter

$$j_{l_1} < j_{l_2} < \cdots < j_{l_{m+1}}.$$

Suponhamos, por isso, que eles já foram ordenadamente escolhidos, isto é, são tais que $j_1 < \cdots < j_{m+1}$. Fazendo, então, $i_l = j_l$, para $l = 1, \ldots, m+1$, notamos que a esta escolha corresponde o termo

$$a_{j_{m+1}}s_m(a_{j_1},\ldots,a_{j_m},\widehat{a}_{j_{m+1}})e_{j_{m+1}}e_{j_1}\cdots e_{j_m}$$

de (3). Por sua vez, se $i_l = j_l$ para $l = 1, \ldots, m-1$, $i_m = j_{m+1}$ e $i_{m+1} = j_m$, temos

$$a_{j_m}s_m(a_{j_1},\ldots,\widehat{a}_{j_m},a_{j_{m+1}})e_{j_m}e_{j_1}\cdots e_{j_{m+1}}.$$

Não é difícil de perceber, portanto, que a cada uma das combinações abaixo

$$\begin{array}{lllllll}
i_1 = j_1 & i_2 = j_2 & i_3 = j_3 & \cdots & i_{m-1} = j_{m-1} & i_m = j_m & i_{m+1} = j_{m+1},\\
i_1 = j_1 & i_2 = j_2 & i_3 = j_3 & \cdots & i_{m-1} = j_{m-1} & i_m = j_{m+1} & i_{m+1} = j_m,\\
i_1 = j_1 & i_2 = j_2 & i_3 = j_3 & \cdots & i_{m-1} = j_{m+1} & i_m = j_{m-1} & i_{m+1} = j_m,\\
\ldots\ldots & & & & & & \\
i_1 = j_1 & i_2 = j_2 & i_3 = j_{m+1} & \cdots & i_{m-1} = j_{m-2} & i_m = j_{m-1} & i_{m+1} = j_m,\\
i_1 = j_1 & i_2 = j_{m+1} & i_3 = j_2 & \cdots & i_{m-1} = j_{m-2} & i_m = j_{m-1} & i_{m+1} = j_m,\\
i_1 = j_{m+1} & i_2 = j_1 & i_3 = j_2 & \cdots & i_{m-1} = j_{m-2} & i_m = j_{m-1} & i_{m+1} = j_m
\end{array}$$

corresponde um único termo em (3) e que estas são todas as combinações possíveis. De fato, $i_1, \ldots, i_m$ devem satisfazer a restrição $i_1 < i_2 < \cdots < i_m$ e não estamos interessados que i_{m+1} coincida com nenhum dos índices anteriores, isto é, que haja repetição de índices, pois $e_i^2 = 0$ em uma álgebra de Grassmann. Assim, ao conjunto ordenado $\{j_1, \ldots, j_{m+1}\}$ correspondem $m+1$ termos de (3),

$$(-1)^{k-1} a_{j_k} s_m(a_{j_1}, \ldots, \widehat{a}_{j_k}, \ldots, a_{j_{m+1}}) e_{j_1} \cdots e_{j_m} e_{j_{m+1}}, \quad k = 1, \ldots, m+1,$$

que somados resultam em

$$\textstyle\sum_{k=1}^{m+1} (-1)^{k-1} a_{j_k} s_m(a_{j_1}, \ldots, \widehat{a}_{j_k}, \ldots, a_{j_{m+1}}) \cdot e_{j_1} \cdots e_{j_m} e_{j_{m+1}}.$$

Contudo, como o conjunto $\{j_1, \ldots, j_{m+1}\}$ foi escolhido arbitrariamente dentre todas as possibilidades possíveis, devemos somar sobre

$$1 \leq i_1 < \cdots < i_{m+1} \leq 2n$$

para assegurar a quarta igualdade.

Como um resultado particular de (2) temos que

$$a^{2n} = s_{2n}(a_1, \ldots, a_{2n}) e_1 \cdots e_{2n}.$$

Portanto, mostrar que $M(n, \mathbb{K})$ satisfaz o polinômio *standard* de grau $2n$ é equivalente a concluir que $a^{2n} = 0$. Mas $a^{2n} = (a^2)^n = b^n$ e

$$b = a^2 = \textstyle\sum_{i_1 < i_2} s_2(a_{i_1}, a_{i_2}) e_{i_1} e_{i_2} = \sum_{i_1 < i_2} (a_{i_1} a_{i_2} - a_{i_2} a_{i_1}) e_{i_1} e_{i_2},$$

ou seja, a^{2n} é a n-ésima potência de uma matriz b de elementos b_{ij} da subálgebra comutativa F de E. Afirmamos que, nesta situação, $a^{2n} = 0$ se $\mathrm{tr}\,(a^2)^k = 0$ para todo $k \geq 1$. De fato, consideremos a álgebra comutativa $\mathbb{K}[b_{ij} \mid i, j = 1, \ldots, n]$. Ela é a imagem homomorfa da álgebra $\mathbb{K}[x_1, \ldots, x_{n^2}]$, que, por sua vez, é um subanel do corpo das funções racionais $\mathbb{K}(x_1, \ldots, x_{n^2}) = \mathbb{F}$. Evidentemente, verificar que nossa afirmação é válida para matrizes com entradas em $\mathbb{F}$ é suficiente para concluí-la sobre a subálgebra F de E. Por isso, consideraremos este primeiro caso. Para tanto, denotemos por $\lambda_1, \ldots, \lambda_n$ as raízes características de b no fecho algébrico de $\mathbb{F}$ e observemos que, sobre ele, o polinômio característico desta matriz é

$$p_b(t) = \det\,(t1 - a) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^{n-1} e_{n-1} t + (-1)^n e_n,$$

com cada e_i avaliado em $\lambda_1, \ldots, \lambda_n$. Notemos, também, que as raízes características de b^k são $\lambda_1^k, \ldots, \lambda_n^k$, pois as raízes características de uma matriz e de sua forma de Jordan coincidem, bem como seus traços. Portanto, o traço de b^k, que é zero por hipótese, é $p_k(\lambda_1, \ldots, \lambda_n)$ e, assim, $p_k(\lambda_1, \ldots, \lambda_n) = 0$. Isto, as identidades de Newton e o fato de $\mathbb{K}$ ser um corpo de característica nula implicam, então, que $e_k(\lambda_1, \ldots, \lambda_n) = 0$ para todo $k \geq 1$. Logo, $p_b(t) = t^n$ e, daí, $b^n = 0$ pelo teorema de Cayley-Hamilton.

Se mostrarmos, então, que $\mathrm{tr}\,(a^2)^k = 0$ para todo $k \geq 1$, teremos concluído este teorema. Mas isto é trivial, pois $a^{2k} = 0$ para $k > n$ e, se $k \leq n$,

$$\mathrm{tr}\,(a^2)^k = \mathrm{tr}\,a^{2k} = \textstyle\sum_{1\le i_1<\cdots<i_{2k}\le 2n} \mathrm{tr}\,s_{2k}(a_{i_1},\ldots,a_{i_{2k}})e_{i_1}\cdots e_{i_{2k}},$$

com

$$\mathrm{tr}\,(s_{2k}(a_{i_1},\ldots,a_{2k})) = \textstyle\sum_{\sigma\in S_{2k}}(\mathrm{sgn}\,\sigma)\mathrm{tr}\,(a_{\sigma(i_1)}\cdots a_{\sigma(i_{2k-1})}a_{\sigma(i_{2k})})e_{i_1}\cdots e_{i_{2k}},$$

de onde vemos que $\mathrm{tr}\,(a_{i_1}\cdots a_{i_{2k-1}}a_{i_{2k}})$ cancela-se com $\mathrm{tr}\,(a_{i_{2k}}\cdots a_{i_{2k}}a_{i_1})$. □

Uma extensão para este teorema ainda é possível:

Proposição 12. *Se $f(x_1,\ldots,x_{2n})$ é uma identidade polinomial multilinear de grau $2n$ para a álgebra $M(n,\mathbb{K})$, então,*

$$f(x_1,\ldots,x_{2k}) = \alpha s_{2n}(x_1,\ldots,x_{2n}), \quad \alpha\in\mathbb{K},$$

isto é, f e s_{2n} coincidem a menos de uma constante.

Esta última proposição ainda é válida em situação bem mais geral: falha somente para a álgebra das matrizes quadradas de ordem 2 definidas sobre o corpo $\mathbb{Z}_2$.

Bem, isto é tudo que gostaríamos de tratar aqui. Esperamos, sinceramente, ter sido bem sucedidos em nossa apresentação.

Referências

[1] Drensky, V., *Free Algebras and PI-Algebras*, Springer, 1999.

[2] Rosset, S., *A New Proof of the Amitsur-Levitzki Identity*, Israel J. Math., **23** (1976), 187–188.

[3] Galvão, A. T., *PI-Álgebras*, dissertação de mestrado, Universidade Estadual de Campinas, 2003.

[4] Kochloukov, P. E., *Algebras with Polynomial Identities*, anotações de um minicurso de mesmo título proferido, em 1998, na 15ª Escola de Álgebra.

[5] Freitas, J. A. O. de, *Identidades Polinomiais para a Álgebra das Matrizes de Ordem Dois sobre Corpos de Característica Zero*, dissertação de mestrado, Universidade Estadual de Campinas, 2006.