Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Programa de Pós-Graduação em Matemática

Gabriel Pereira de Figueiredo †

Aplicações Comutantes Sobre Subconjuntos de Matrizes

Campina Grande - PB
2024

†Este trabalho contou com apoio financeiro da CAPES e do CNPq, sob o Processo nº 404851/2021-5.

Gabriel Pereira de Figueiredo

Aplicações Comutantes Sobre Subconjuntos de Matrizes

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática da Universidade Federal de Campina Grande, pertencente à linha de pesquisa Álgebra e área de concentração Matemática como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Claudemir Fideles Bezerra Júnior

Campina Grande - PB
2024

F475a Figueiredo, Gabriel Pereira de.

Aplicações comutantes sobre subconjuntos de matrizes / Gabriel Pereira de Figueiredo. – Campina Grande, 2024.

87 f. : il. color.

Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2024.

"Orientação: Prof. Dr. Claudemir Fideles Bezerra Júnior".

Referências.

1. Matrizes Invertíveis. 2. Matrizes Singulares. 3. Aplicações Comutantes – Subconjuntos de Matrizes. 4. Álgebra. I. Bezerra Júnior, Claudemir Fideles. II. Título.

CDU 519.142(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Aplicações Comutantes Sobre Subconjuntos de Matrizes

por

Gabriel Pereira de Figueiredo

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada em: 16/08/2024

Prof. Dr. Antônio Pereira Brandão Jr. - UFCG

Prof. Dr. Pedro Souza Fagundes - UFSCAR

Prof. Dr. Willian Versolati França - UFJF

Prof. Dr. Claudemir Fideles Bezerra Júnior - UNICAMP
Orientador

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Agosto - 2024

Agradecimentos

Agradeço, em primeiro lugar, ao meu Senhor e meu Deus, porque, em meu caminho até aqui, me possibilitou viver tudo que se fez necessário para conseguir passar por todos os desafios e obstáculos. Nos momentos em que não acreditei que pudesse chegar aqui, Ele não me deixou desistir e se fez presente, pondo em meu caminho pessoas que muito me ensinaram, ensinam, e que me deram forças para seguir. Bendito seja Deus!

Aos meus pais, Josivaldo e Aldací (Alda), que me deram o seu apoio sempre que precisei, até mesmo quando não o pedi, por efeito do seu amor incondicional. Vocês são para mim inspirações. Sou grato a Deus por tê-los em minha vida; São a parte especial do que tenho e considero como mais valioso neste mundo, a minha família. Amo-os muito!

Oportunamente, agradeço a toda a minha família paterna e materna, em nome de minhas avós, Dulcineia (Dulce-avó materna) e Maria do Socorro (avó paterna). Certamente não conseguirei retribuir sozinho o tamanho do amor que me demonstram e o bem que me fizeram até aqui. Por isso, peço que Deus os guarde e conduza para a felicidade eterna. Faço aqui um agradecimento especial a Scarlet Marques, que, (como ela costuma dizer) por efeito da providência Divina, nossos caminhos se cruzaram e por capricho dos traços e linhas escritas pelas mãos do Senhor, nos puseram a partilhar os dias de nossas vidas. Você me fez ressignificar e compreender o caminho que o Senhor pensou para mim. Agradeço por teu amor, carinho, cumplicidade, apoio e aprendizados. Quero partilhar contigo o que Deus me conceder e viver ao teu lado até quando Ele nos permitir.

Também, aos amigos que fiz neste percurso, seja na universidade ou fora dela. Sou muito grato por ter conhecido cada um de vocês. Saibam que, me ajudaram muito em suas preces, orações e conversas. Especialmente, agradeço aos companheiros de turma no mestrado, Matheus Nascimento e Diego Jonathan.

Agradeço a cada um dos professores do departamento de Matemática, especialmente aos professores Daniel Cordeiro, Antônio Brandão, Diogo Diniz, Angelo Roncalli, Kennerson Nascimento, os demais professores e funcionários do PPGMAT/UFCG e da Unidade Acadêmica de Matemática, por todos os momentos de aprendizado. As boas conversas, os conselhos, a dedicação e ajuda de vocês nos possibilitam trilhar caminhos para realizar o que sonhamos. Agradeço, especialmente ao professor Claudemir Fideles, pela dedicação e orientação neste trabalho, pelas boas conversas e pela paciência. Também, a cada um dos membros da banca desta dissertação, pela disponibilidade de participarem, pelo tempo empregado na leitura do texto e por todas as sugestões, ponderações e correções feitas para o enriquecimento da versão final desta dissertação de mestrado.

Encerro agradecendo a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) por todo o suporte financeiro ao longo desses dois anos e ao auxílio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ).

Dedicatória

A minha família, em especial ao meu avô, José Inácio Pereira (in Memoriam).

Resumo

A Teoria das Identidades Funcionais (FI), introduzida na tese de doutorado de Matej Brešar, é relativamente nova. Desde então, essa teoria tem sido desenvolvida através de uma série de artigos que estudaram algumas identidades funcionais básicas, em particular aquelas relacionadas às chamadas aplicações comutantes. Nesta dissertação, dividida em quatro capítulos, estudamos aplicações aditivas $G\colon M_n(\mathbb{K}) \to M_n(\mathbb{K})$ que satisfazem a propriedade comutante sobre algum subconjunto A de $M_n(\mathbb{K})$, isto é, $G(x)x = xG(x)$, para todo $x \in A$. Tais aplicações serão chamadas de "Aplicações Comutantes" sobre A. Nosso trabalho é baseado em resultados de França em [8, 9] e de Xu e Zhu em [23]. Primeiramente, apresentamos uma descrição de aplicações comutantes sobre matrizes invertíveis ou singulares. Como uma generalização, obtemos a descrição de aplicações m-aditivas $G\colon M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ cujo traço $T(x) = G(x,\ldots,x)$ é comutante sobre os mesmos conjuntos citados anteriormente. Por fim, exibimos um resultado interessante que diz quando uma aplicação multiaditiva que possui traço nulo em matrizes invertíveis é nula em $M_n(\mathbb{K})$ e, como aplicação deste resultado, fornecemos uma variação da demonstração dada para traços comutantes de multiaditivas no subconjunto de matrizes invertíveis.

Palavras chaves: Aplicações Comutantes; Matrizes Invertíveis; Matrizes Singulares.

Abstract

The theory of Functional Identities (FI), introduced in Matej Brešar's Ph.D. thesis, is relatively new. Since then, this theory has been developed through a series of papers in which he studied some basic FIs, particularly those concerning the so-called commuting maps. This work is divided into four chapters, where we study additive maps $G\colon M_n(\mathbb{K}) \to M_n(\mathbb{K})$ that satisfy the commuting property over some subset A of $M_n(\mathbb{K})$, i.e., $G(x)x = xG(x)$ for all $x \in A$. Such mappings will be called "commuting mappings over A". Our master's thesis is based on results from França in [8, 9] and from Xu and Zhu in [23]. Firstly, we present a description of commuting maps over invertible or singular matrices. As a generalization, we obtain the description of m-additive maps $G\colon M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ whose trace $T(x) = G(x,\dots,x)$ is commuting over the same sets mentioned earlier. Finally, we exhibit an interesting result that states that if $T(x) = 0$ for all invertible matrices x, then $T(M_n(\mathbb{K})) = 0$ if one of the following holds: (1) char $\mathbb{K} = 0$; (2) char $\mathbb{K} > m$; (3) char $\mathbb{K} = m$ and $|\mathbb{K}| \neq m$; (4) $|\mathbb{K}| \geq 2m$. As a consequence of this last result, We provide an alternative proof for commuting traces of multiadditives on the subset of invertible matrices.

Key Words: Commuting Maps; Invertible Matrices; Singular Matrices.

Sumário

Introdução

A Teoria das Identidades Funcionais, ou FI-teoria (do inglês *Functional Identities*), é uma parte importante da Teoria de Anéis. A FI-teoria é relativamente nova e foi introduzida na tese de doutorado de M. Brešar em 1990. Desde então, essa teoria tem sido desenvolvida através de uma série de artigos que estudaram algumas identidades funcionais básicas, em particular aquelas que são chamadas de "Aplicações Comutantes".

Segundo Brešar et al. [5], uma identidade funcional, de maneira informal, é uma relação de identidade envolvendo elementos arbitrários em um anel e funções, na qual aparecem somas de produtos entre elementos do anel por valores de funções desconhecidas. A FI-teoria tem como objetivo determinar a forma dessas funções ou, quando isso não for possível, determinar a estrutura do anel que admite a FI em questão. Além disso, entre os conceitos clássicos estudados na grande área de Álgebra, o de Álgebras com Identidades Polinomiais (PI-álgebras), de forma superficial, é o que mais se aproxima do conceito de FI-teoria. Pode-se imaginar uma identidade polinomial como sendo um exemplo especial de FI, em que as funções são polinômios. Entretanto, o estudo de Identidades Polinomiais tem objetivos diferentes da FI-teoria. Brešar et al. [5] afirmam que, especialmente do ponto de vista das aplicações, as duas teorias tornam-se complementares entre si. Sob algumas condições, a teoria de PI-álgebras trabalha com anéis mais próximos a álgebras de dimensões finitas, enquanto que a FI-teoria consegue obter respostas mais aguçadas em álgebras de dimensões suficientemente grandes ou infinitas.

É conhecido que existem conexões entre a FI-teoria e a área de pesquisa conhecida como "Problemas de Preservadores (ou preservantes) Lineares" (do inglês *Linear Preserver Problems*). Entende-se preservadores lineares como sendo aplicações lineares entre álgebras que, a grosso modo, preservam certas propriedades de alguns elementos da álgebra. O objetivo é descrever a forma dessas aplicações lineares que preservam certas propriedades. A maioria dos resultados em preservação linear preocupam-se com álgebras de matrizes. Por outro lado, vários problemas de preservação linear também foram considerados em álgebras de operadores lineares limitados, bem como em algumas outras álgebras que aparecem na Análise Funcional. Usando FIs, podemos obter generalizações na teoria dos anéis de alguns desses resultados.

A lista de publicações sobre preservadores lineares é volumosa, e por isso nos referimos apenas a alguns artigos de pesquisa relevantes [3, 5, 19, 20, 21], bem como suas referências. Os artigos citados tratam de diversos aspectos dos preservadores lineares e são fundamentais para a compreensão e o desenvolvimento contínuo da teoria dos preservadores lineares, estabelecendo uma base sólida para futuras pesquisas e aplicações.

Nesta dissertação, estamos interessados em um dos problemas de preservadores lineares mais conhecidos: os preservadores de comutatividade. Tal problema se concentra em encontrar a forma de uma aplicação linear α de uma álgebra B para uma álgebra A com a propriedade de que os elementos $\alpha(x)$ e $\alpha(y)$ em A comutam sempre que x e y em B comutam. É claro que todo homomorfismo de Lie satisfaz esta condição e, de fato, a mesma ideia que funciona para os homomorfismos de Lie é aplicável neste problema mais geral. Pode-se ainda considerar este problema de uma forma mais geral, assumindo, por exemplo, que apenas a comutatividade de elementos simétricos em álgebras com involução é preservada.

Desta forma, a FI-teoria oferece uma ferramenta robusta e flexível para abordar e resolver problemas complexos de preservação linear em diversas estruturas algébricas. Assim, estamos particularmente interessados em aplicações aditivas e multiaditivas que possuem a propriedade *Commuting*, a qual traduziremos livremente por Comutante. Tal propriedade é estabelecida no seguinte sentido: sendo X um subconjunto não vazio de um anel A, diremos que uma aplicação $f : X \to A$ é uma aplicação comutante em X se satisfaz $f(x)x = xf(x)$ para todo $x \in X$. Essa ideia é estendida para aplicações multiaditivas por meio da aplicação traço (vide a Definição 3.7).

Em resumo, esta dissertação se concentra em entender e caracterizar aplicações aditivas e multiaditivas com a propriedade comutante sobre subconjuntos da álgebra de matrizes. Através do uso de identidades funcionais, buscamos descrever tais aplicações e explorar suas implicações em problemas de preservação linear. O primeiro resultado importante sobre aplicações comutantes é o Teorema de Posner [22] de 1957. Este teorema afirma que a existência de uma derivação comutante diferente de zero em um anel primo A implica que o anel é comutativo. Tal teorema tem sido extremamente influente e, pelo menos indiretamente, deu início a muitas questões discutidas neste artigo.

Em nossa pesquisa, focamos em aplicações aditivas e multiaditivas que satisfazem a propriedade comutante em subconjuntos específicos da álgebra de matrizes. Com base nos resultados pioneiros de Brešar e no impacto do Teorema de Posner, buscamos aprofundar o entendimento dessas aplicações, explorando suas propriedades e implicações teóricas.

O objetivo principal no desenvolvimento desta dissertação é o estudo das técnicas desenvolvidas por França em [8, 9] e por Xu e Zhu em [23]. Estes três artigos formaram a base desse trabalho de dissertação. No estudo, a ideia geral é trabalhar com aplicações aditivas e multiaditivas que enviam matrizes quadradas (ou m-uplas de matrizes) em matrizes quadradas, sob a hipótese de preservarem uma determinada propriedade em subconjuntos de matrizes. A meta é obter uma descrição completa dessas aplicações em tais subconjuntos. Conforme mencionado anteriormente, este é um típico problema dentro do estudo de Problemas de Preservadores Lineares.

A dissertação consiste em quatro capítulos e a seguir descreveremos como ela está organizada.

Prezando por oferecer suporte ao texto que vamos apresentar, decidimos dedicar o Capítulo 1 à apresentação de alguns conceitos básicos que julgamos importantes recordar. Advertimos ao leitor que muitos conceitos básicos de Álgebra Abstrata, os quais utilizaremos no texto, serão apenas citados sem os pormenores. Dedicaremos as duas primeiras seções para abordar, de forma resumida, a Teoria de Anéis e Álgebras, pois, em boa parte do que trabalhamos, consideramos nossos resultados sobre tais estruturas algébricas. Também faremos, neste capítulo, uma descrição sobre o Anel de Frações de Martindale, do qual obtemos conceitos que são base para importantes resultados que utilizamos em nosso trabalho. Adiantamos ao leitor que desejar consultar sobre os objetos matemáticos trabalhados de Álgebra Linear, Teoria de Anéis, Álgebras e Módulos, que estes podem ser encontrados nas referências [5, 11, 13, 14, 17].

Conforme França [8], os resultados de Identidades Funcionais, até onde se tem conhecimento, foram obtidos para subconjuntos que são fechados sob a adição. França destaca ainda em [8], que muitos resultados importantes na área de Problemas de Preservadores Lineares valem para subconjuntos de matrizes que não são fechados sob a adição. No Capítulo 2, veremos uma forma de estender alguns resultados de FI para subconjuntos de matrizes que não são fechados sob a adição. O objetivo deste capítulo é descrever a forma de uma aplicação aditiva e comutante no subconjunto das matrizes singulares ou invertíveis. Neste segundo, o procedimento é similar ao anterior, no entanto, há uma maior dificuldade nas argumentações, sendo necessário provar que G aplicada a elementos do centro é um elemento central. Esta hipótese é fundamental para prosseguir com as argumentações, além de ser necessário que o corpo base tenha pelo menos três elementos. Veremos que, nos passos da demonstração, conseguimos obter uma FI e descrevê-la, o que apresenta uma forma de estender resultados de FI para subconjuntos que não são fechados sob a adição.

No Capítulo 3 apresentamos uma generalização da noção estudada no capítulo anterior. A ideia de descrever a forma de uma aplicação aditiva comutante em subconjuntos de matrizes é agora ampliada para aplicações multiaditivas, com o auxílio da aplicação traço. Este capítulo contém dois resultados principais. No primeiro, o Teorema 3.14, obtemos a descrição da forma de uma aplicação multiaditiva G, cuja respectiva aplicação traço satisfaz a propriedade comutante no subconjunto das matrizes invertíveis. Neste resultado, assumimos que char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$ e que $|\mathbb{K}| \geq m^2+2m+3$, onde K denota o corpo base. A ideia da demonstração se assemelha um pouco com a utilizada nos resultados do Capítulo 2, mas com suas dificuldades naturais. Aqui, também realizamos uma extensão da propriedade comutante no subconjunto das matrizes invertíveis para todo o espaço das matrizes. No segundo, o Teorema

3.15, obtemos a descrição da forma de uma aplicação multiaditiva, cuja respectiva aplicação traço satisfaz a propriedade comutante no subconjunto das matrizes singulares. Neste resultado, não há necessidade de supor uma quantidade mínima de elementos no corpo, como é feito no primeiro resultado. A ideia é, novamente, estender tal propriedade para todo o espaço das matrizes. Com o auxílio do Teorema 3.10[1], provamos que a aplicação G, nos dois resultados, satisfaz a expressão:

$$G(x,\ldots,x) = \mu_0 x^m + \mu_1(x)x^{m-1} + \cdots + \mu_{m-1}(x)x + \mu_m(x),\ \forall x \in M_n(\mathbb{K}),$$

onde $\mu_0 \in \mathcal{Z}$ e $\mu_i : M_n(\mathbb{K}) \to \mathcal{Z}$, em que $\mathcal{Z}$ denota o centro de $M_n(\mathbb{K})$, é o traço de uma aplicação i-aditiva para $i \in \{1,\ldots,m\}$. Assim, com esses dois resultados em mãos, juntamente com a noção da aplicação traço comutante, conseguimos descrever a forma das aplicações multiaditivas que são comutantes em matrizes invertíveis ou em matrizes singulares, proporcionando mais uma forma de estender resultados de Identidades Funcionais para conjuntos que não são fechados sob a adição.

Por fim, como resultado de nossa busca por desenvolver o tema proposto, encontramos um resultado interessante dado por Xu e Zhu [23]. Este resultado oferece uma nova perspectiva para abordar o problema de descrever uma aplicação multiaditiva comutante sobre matrizes invertíveis. Assim, o último capítulo é dedicado a demonstrar que se o traço de uma aplicação multiaditiva se anula no subconjunto das matrizes quadradas invertíveis $GL_n(\mathbb{K})$, então essa aplicação deve ser nula em $M_n(\mathbb{K})$, sob algumas condições específicas: 1) char $\mathbb{K} = 0$; 2) char $\mathbb{K} > m$; 3) char $\mathbb{K} = m$ e $|\mathbb{K}| \neq m$; 4) $|\mathbb{K}| \neq 2^m$. Este resultado pode ser adaptado para fornecer uma aplicação de como obter a forma completa de uma aplicação multiaditiva cuja aplicação traço satisfaz a propriedade comutante no subconjunto das matrizes invertíveis. Como consequência direta deste resultado, obtemos uma demonstração alternativa da prova apresentada no Teorema 3.14, que já tinha sido provado no capítulo anterior.

Além dos capítulos, o trabalho conta com um apêndice. Reservamos ao apêndice algumas contas básicas, obtidas de forma indutiva, de algumas identidades que aparecem nos resultados do Capítulo 3, cuja disposição no texto julgamos não ser a melhor forma de torná-lo claro. Também apresentaremos, como extra, um breve estudo sobre o determinante de uma matriz quadrada e introduziremos conceitos e resultados de forma sucinta sobre o tema. Realizaremos algumas demonstrações que consideramos interessantes, enquanto para os resultados não demonstrados, indicaremos onde o leitor pode encontrá-los.

Por último, esperamos que a estrutura do texto possa auxiliar o leitor, especialmente alunos de mestrado, a compreender o estudo de Problemas de Preservadores Lineares aplicado à álgebra de matrizes $M_n(\mathbb{K})$, proporcionando um caminho claro para desenvolver a compreensão dos conceitos e resultados apresentados na dissertação. Além disso, esperamos estimular o interesse pelo estudo nesta área.

[1] A demonstração encontra-se em [18, Theorem 3.1].

CAPÍTULO 1

Preliminares

Neste capítulo, abordaremos conceitos importantes para o desenvolvimento do estudo que apresentaremos neste trabalho. Nas duas primeiras seções nos dedicaremos a fazer uma descrição, sem muitos detalhes, sobre anéis e álgebras. Na Seção 1.3 traremos as definições de aplicações aditivas e comutantes em anéis, que servirão de base para o que será retratado nos Capítulos 2, 3 e 4. A Seção 1.4 é destinada a definir derivações e biderivações e trazer alguns resultados e suas demonstrações sobre tais conceitos matemáticos, que são de suma importância e serão utilizados como suporte nas demonstrações dos resultados principais presentes no Capítulo 2.

Na Seção 1.5, traremos resumidamente uma descrição de conceitos importantes sobre PI-álgebras que são utilizados em nosso texto, e sentimos que serão importantes para o conhecimento do leitor. A saber, falaremos sobre a definição de PI-álgebra, sobre as *identidades Standard*, sobre o Teorema de Amitsur-Levitzki, que nos diz sobre a *Identidade Standard* de matrizes, e complementaremos com uma apresentação sobre o processo de linearização.

Por último, na Seção 1.6, objetivamos apresentar a construção do *Martindale Rings of Quotients*, que traduzimos por Anéis de Frações de Martindale, juntamente com algumas noções básicas e resultados sobre a teoria, sem muita preocupação em trazer demonstrações vinculadas a essa construção.

Para um leitor interessado em um estudo mais detalhado desses conceitos e resultados, indicamos as referências [4, 5, 7, 12, 16, 17].

Lembramos ao leitor que em nosso texto $\mathbb{K}$ sempre denotará um corpo. Quando necessário, especificaremos sob quais condições devemos considerar o corpo $\mathbb{K}$. Ademais, no decorrer deste capítulo almejamos, além da apresentação dos conceitos e resultados que utilizaremos, abordar sobre o conjunto de matrizes sobre um corpo $\mathbb{K}$ no contexto de anéis e de álgebras. Especialmente, nesta seção fixaremos algumas notações a respeito de matrizes quadradas de ordem n, as quais utilizaremos ao longo de toda a redação.

1.1 Anéis

Em nosso trabalho, os conhecimentos básicos acerca de anéis serão influentes na linguagem básica e por esta razão resolvemos trazer um pouco sobre tais estruturas algébricas aqui nesta seção. O que será tratado aqui será proveitoso para a breve apresentação sobre álgebras na próxima seção.

Definição 1.1. *Seja A um conjunto não vazio e "$+$" e "$\cdot$" operações em A. Diremos que a terna $(A,+,\cdot)$ é um anel se valem as seguintes condições:*

(a) $(a+b)+c = a+(b+c)$*, para quaisquer* $a,b,c \in A$*;*

(b) $a+b = b+a$*, para quaisquer* $a,b \in A$*;*

(c) existe $0 \in A$ *tal que* $0+a = a$*, para todo* $a \in A$*;*

(d) para cada $a \in A$ *existe* $-a \in A$ *tal que* $a+(-a) = 0$*;*

(e) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$*, para quaisquer* $a,b,c \in A$*;*

(f) $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ *e* $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$*, para quaisquer* $a,b,c \in A$ *(distributividade de "$\cdot$" em relação a "$+$").*

Chamaremos a operação "$+$" de *adição* e a operação "$\cdot$" de *multiplicação*. Por simplicidade, denotaremos o anel $(A,+,\cdot)$ por A, e, para quaisquer $a,b \in A$, o resultado dado por $a\cdot b$ é o produto entre a e b, nesta ordem. Novamente, com a finalidade de deixar a notação o mais simples possível, caso não haja dúvida sobre a multiplicação utilizada, podemos omitir o símbolo "$\cdot$", e dessa forma $a\cdot b$ será substituído por ab.

Dizemos que A é comutativo se $ab = ba$, para quaisquer $a,b \in A$. Além disso, dizemos que A possui unidade se existe $1 \in A$ tal que $1a = a = a1$, para todo $a \in A$. O elemento neutro aditivo de um anel A é chamado de zero e denotado por 0_A (ou, simplesmente por 0). Dizemos que um anel A é não nulo se existe $a \in A$ tal que $a \neq 0$. Se A tem unidade, então $1 \neq 0$ e, então A é não nulo. Quando necessário, utilizaremos a notação $|A|$ (pronunciaremos "ordem de A") para nos referirmos ao número de elementos do anel A. Se A tem uma quantidade infinita de elementos, diremos que $|A|$ é infinita; se for finita, diremos que $|A|$ é finita.

Exemplo 1.2. *As estruturas algébricas* $(\mathbb{Z},+,\cdot)$*,* $(\mathbb{Q},+,\cdot)$*,* $(\mathbb{R},+,\cdot)$*,* $(\mathbb{C},+,\cdot)$*, em que "$+$" e "$\cdot$" são as operações de adição e multiplicação usuais, são exemplos de anéis.*

Exemplo 1.3. *Sejam A um anel e $n \in \mathbb{N}$. Denotamos por $M_n(A)$ o conjunto das matrizes quadradas de ordem $n \times n$ com entradas em A. Para $X \in M_n(A)$ denotamos*

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix},$$

ou ainda, $X = (x_{ij})_{n \times n}$, com $x_{ij} \in A$, para $i, j \in \{1, 2, \ldots, n\}$. Dadas as matrizes $X = (x_{ij})_{n \times n}$, $Y = (y_{ij})_{n \times n} \in M_n(A)$, definimos as operações de adição e multiplicação, respectivamente, por

$$X + Y = (c_{ij})_{n \times n} \quad e \quad X \cdot Y = (d_{ij})_{n \times n},$$

em que $c_{ij} = x_{ij} + y_{ij} \in A$ e $d_{ij} = \sum_{k=1}^{n} x_{ik} y_{kj} \in A$. Munido destas operações, $M_n(A)$ é um anel, chamado de anel das matrizes de ordem $n \times n$ sobre A ou, simplesmente, anel das matrizes quadradas de ordem n sobre A. A matriz nula, isto é, a matriz $(a_{ij})_{n \times n}$ em que $a_{ij} = 0_A$, é o zero do anel $M_n(A)$, o qual denotaremos por 0_n. Além do mais, dadas $A = (a_{ij})_{n \times n}$ e $B = (b_{ij})_{n \times n}$ diremos que $A = B$ quando $a_{ij} = b_{ij}$, para todo $i, j \in \{1, \ldots, n\}$.

Continuando a desenvolver o exemplo anterior, não é difícil ver que, se A possui unidade, então a matriz $(a_{ij})_{n \times n}$, com $a_{ii} = 1_A$ e, para $j \neq i$, $a_{ij} = 0_A$, com $i, j \in \{1, 2, \ldots, n\}$, é a unidade de $M_n(A)$. Denotaremos tal unidade de $M_n(A)$ por I_n ou, quando conveniente, simplesmente por I e denominaremos de *matriz identidade*. Ademais, sob a hipótese de A ter unidade, fixados $i, j \in \{1, \ldots, n\}$, a matriz quadrada de ordem n com 1_A na entrada (i, j) e zero nas demais é chamada de matriz elementar e é denotada por $e_{ij}(1_A)$ ou, simplesmente, e_{ij}. Em símbolos:

$$e_{ij} = \begin{array}{cc} \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 1_A & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} & \begin{array}{c} \\ \\ \leftarrow i \\ \\ \\ \\ \\ \end{array} \\ \begin{array}{ccccccc} & & & & \uparrow & & \\ & & & & j & & \end{array} & \end{array}.$$

De forma similar define-se a matriz elementar $e_{ij}(a)$, que tem $a \in A$ na entrada da linha i e coluna j e zero nas demais. Para uma melhor utilidade nas contas, definiremos $e_{ij}(a) = ae_{ij}$, para todo $a \in A$. Não é difícil ver que, se $j = l$, então $e_{ij}(a)e_{lk}(b) = e_{ik}(ab)$ e se $j \neq l$, então $e_{ij}(a)e_{lk}(b) = 0_n$. Em outras palavras, temos $(ae_{ij})(be_{lk}) = (ab)e_{ik}$, se $j = l$, e $(ae_{ij})(be_{lk}) = 0_n$, se $j \neq l$. Mais à frente, utilizaremos essa identificação.

Observação 1.4. *Sendo A um anel com unidade, não é difícil ver que $M_n(A)$ é comutativo se, e* *somente se, A é comutativo e $n = 1$.*

Definição 1.5. *Seja A um anel com unidade e considere $a \in A$. Diremos que:*

(a) a é inversível à direita em A se existe $b \in A$ tal que $ab = 1$. Diz-se que b é um inverso à direita de a em A.

(b) a é inversível à esquerda em A se existe $c \in A$ tal que $ca = 1$. Diz-se que c é um inverso à esquerda de a em A.

(c) a é inversível em A se existe $b \in A$ tal que $ab = ba = 1$. Diz-se que b é um inverso de a em A.

Sob a hipótese de associatividade segue que se $a \in A$ possui inverso multiplicativo bilateral, então este deve ser único. Ademais, se A possui unidade, observe que o conjunto

$$U(A) = \{a \in A \mid a \text{ é inversível em } A\}$$

é não vazio e multiplicativamente fechado. Munido da multiplicação de A tem-se que $U(A)$ é um grupo, chamado de *grupo multiplicativo de A*.

Observação 1.6. *Denotaremos o grupo multiplicativo do anel $M_n(A)$ por $GL_n(A)$, o qual é conhecido como grupo geral linear de grau n sobre A.*

Definição 1.7. *Dizemos que um anel A não nulo e com unidade é um anel com divisão se $U(A) = A \setminus \{0_A\}$. Além disso, o anel A é um corpo se é um anel com divisão comutativo.*

Exemplo 1.8. *Os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, cujas operações são a adição e multiplicação usuais são exemplos de corpos. Já o anel $\mathbb{Z}$, com as operações usuais, não é um corpo.*

Exemplo 1.9. *Considere $\mathbb{K} = \mathbb{R}$ e os símbolos $1, i, j$ e k tais que $-1 = i^2 = j^2 = k^2$, $ij = -ji = k$, $ik = -ki = j$ e $jk = -kj = i$ e $1x = x1 = x$, onde $x \in \{i, j, k\}$. Temos que:*

$$\mathbb{H}_{\mathbb{R}} = \{\alpha = \alpha_0 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}\},$$

munido da adição termo a termo e da multiplicação estendida por linearidade para $1, i, j, k$, é um anel com divisão não comutativo, logo não é um corpo. Este anel é chamado de anel dos quatérnios reais.

Considere A um anel com unidade e $e_{11}, e_{12} \in M_2(A)$. É fácil verificar que $e_{11}^2 = e_{11}$ e que $e_{12}^2 = 0_2$. De maneira geral, para $e_{ii}, e_{ij} \in M_n(A)$ vale que $e_{ii}^2 = e_{ii}$ e $e_{ij}^2 = 0$, com $i \neq j$ e $i, j \in \{1, \ldots, n\}$. Isto nos motiva a fazer a seguinte definição.

Definição 1.10. *Sejam A um anel e $a \in A$. Dizemos que:*

(a) a é idempotente, se $a^2 = a$.

(b) a é nilpotente, se existe $n \in \mathbb{N}$ tal que $a^n = 0$.

(c) a é um divisor de zero, se $a \neq 0$ e existe $b \in A \setminus \{0\}$ tal que $ab = 0$ ou $ba = 0$.

Sendo $a \in A$ nilpotente, dizemos que o menor $n \in \mathbb{N}$ tal que $a^n = 0$ é chamado de *índice* de nilpotência de a. Neste caso, dizemos que a é nilpotente de índice n.

Observação 1.11. *Todo elemento nilpotente não nulo é um divisor de zero.*

Exemplo 1.12. *Seja A um anel não nulo e $n \geq 2$. O anel das matrizes $M_n(A)$ possui divisores de zero. De fato, tomando $a, b \in A \setminus \{0_A\}$ tem-se $e_{ij}(a), e_{lk}(b) \in M_n(A)$ matrizes não nulas. Daí, tomando $j \neq l$, segue que $e_{ij}(a)$ e $e_{lk}(b)$ são ambas não nulas e $e_{ij}(a) \cdot e_{lk}(b) = 0_n$. Além disso, se A possui unidade, vemos que e_{ii} é idempotente e e_{ij}, sempre que $i \neq j$, é nilpotente de índice 2.*

Definição 1.13. *Seja A um anel não nulo com unidade. Dizemos que A é um domínio se não tem divisores de zero. Dizemos que A é um domínio de integridade se A é um domínio comutativo.*

Exemplo 1.14. *Veja que se $x \in U(A)$, então x não é um divisor de zero. Daí, todo anel com divisão é um domínio, particularmente todo corpo $\mathbb{K}$ é um domínio de integridade. Agora, observe que nem todo domínio de integridade é um corpo. Para exemplificar essa última afirmação, temos que $\mathbb{Z}$ é um domínio de integridade que não é um corpo.*

Seja A um anel. Para $x, y \in A$, arbitrários, denominaremos de *comutador de x por y*, denotado por $[x, y]$, o elemento $xy - yx$ em A. Ao longo do texto utilizaremos essa notação sempre que necessário. Ademais, $[x, y] = 0$ se, e somente se, $xy = yx$. É fácil ver que $[x, y] = -[y, x]$.

Agora, definimos *o centralizador de $a \in A$ em A* como sendo o conjunto

$$C_A(a) = \{x \in A \mid [x, a] = 0\}.$$

Note que podemos estender a definição anterior para um conjunto $S \subset A$, não vazio, da seguinte forma: *o centralizador de S em A* é o conjunto

$$C_A(S) = \{x \in A \mid [x, s] = 0, \forall s \in S\}.$$

Por fim, *o centro de um anel A* é definido como sendo o conjunto

$$Z(A) = \{x \in A \mid [x, a] = 0, \forall a \in A\}.$$

Observa-se que $Z(A) = C_A(A)$. Note, ainda, que nenhum dos conjuntos é vazio, pois o zero de A cumpre as condições dadas nas definições dos conjuntos acima. Na verdade, é possível ver que eles são subanéis de A conforme a Definição 1.17.

É importante salientar que trabalharemos com o anel de matrizes sobre um corpo $\mathbb{K}$ nos capítulos subsequentes. Por isso, para acostumarmos o leitor com essa informação, vamos trabalhar a partir de agora com observações e fatos que podem ser vistos para $M_n(\mathbb{K})$.

Exemplo 1.15. *Não é difícil ver que*

$$Z(M_n(\mathbb{K})) = \{\alpha \cdot I \mid \alpha \in \mathbb{K}\}.$$

Observação 1.16. *Em todo o texto, por simplicidade denotaremos o centro $Z(M_n(\mathbb{K}))$ de $M_n(\mathbb{K})$ por $\mathcal{Z}$. Por tal motivo, para uma maior facilidade nas demonstrações, denotaremos $\alpha \cdot I \in \mathcal{Z}$, com $\alpha \in \mathbb{K}$, apenas por α.*

Definição 1.17. *Sejam A um anel e B um subconjunto não vazio de A. Dizemos que B é um subanel de A se valem:*

(a) $x - y \in B$, para quaisquer $x, y \in B$;

(b) $xy \in B$, para quaisquer $x, y \in B$.

Definição 1.18. *Sejam A um anel e I um subgrupo aditivo de A. Dizemos que I é:*

(a) um ideal à direita se $xa \in I$ para quaisquer $x \in I$ e $a \in A$;

(b) um ideal à esquerda se $ax \in I$ para quaisquer $x \in I$ e $a \in A$;

(c) um ideal se $xa, ax \in I$ para quaisquer $x \in I$ e $a \in A$.

Exemplo 1.19. *Fixado $n \in \mathbb{Z}$, tem-se que $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ é um ideal do anel $\mathbb{Z}$. Não é difícil provar que todos os ideais de $\mathbb{Z}$ são dessa forma.*

Agora, dado A um anel e I e J ideais de A definimos

$$IJ = \langle \{xy \mid x \in I, y \in J\} \rangle.$$

De maneira similar, temos que A^2 denota o ideal gerado por $\{ab \mid a, b \in A\}$.

Definição 1.20. *Um anel A é dito* ***simples*** *se $A^2 \neq \{0_A\}$ e A e $\{0_A\}$ são seus únicos ideais.*

Exemplo 1.21. *Todo corpo $\mathbb{K}$ é um anel simples. Por este motivo, os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são simples. Também o anel dos quatérnios reais $\mathbb{H}_{\mathbb{R}}$ é um anel simples.*

Exemplo 1.22. *O anel $M_n(\mathbb{K})$ é um anel simples. Na verdade, $M_n(D)$ é um anel simples, em que D é um anel com divisão. De fato, tome I um ideal não nulo de $M_n(D)$. Escolha $X = (a_{ij})_{n \times n} \in I$ diferente da matriz nula. Selecione j e k de modo que $a_{jk} \neq 0$. Notavelmente,*

$$e_{ij} X e_{kl} = a_{jk} e_{il},$$

para todo $1 \leq i, j, k, l \leq n$. Dessa forma, vemos que $a_{jk} e_{il} \in I$, para todo $i, l \in \{1, \ldots, n\}$, e portanto também

$$((d a_{jk}^{-1}) e_{ii}) \cdot (a_{jk} e_{il}) = d e_{il} \in I, \text{ para todo } d \in D.$$

Consequentemente, $I = M_n(D)$ e, portanto, $M_n(D)$ é um anel simples. Com a abordagem utilizada na demonstração, é possível chegar a uma correspondência biunívoca entre ideais de um anel com unidade A e ideais de $M_n(A)$. Entretanto, é necessário aprofundar-se na teoria de anéis e ideais, o que está fora do escopo imediato.

Definição 1.23. *Um ideal próprio I de A é dito ser um ideal primo se para J_1 e J_2 ideais de A tais que $J_1J_2 \subset I$ tem-se $J_1 \subset I$ ou $J_2 \subset I$.*

Quando o anel tem unidade e é comutativo diremos que I é um ideal primo de A se para quaisquer $a,b \in A$ tais que $ab \in I$ tem-se $a \in I$ ou $b \in I$.

Definição 1.24. *Um ideal próprio I de A é dito ser um ideal maximal se não existe nenhum ideal próprio J de A tal que $I \subsetneq J \subsetneq A$, ou seja, se $I \subsetneq J \subseteq A$ implica em $J = A$.*

Observação 1.25. *Todo anel A com unidade possui pelo menos um ideal maximal.*

Exemplo 1.26. *Veja que os ideais $p\mathbb{Z}$, em que $p \in \mathbb{Z}$ é um número primo, são ideais primos de $\mathbb{Z}$. Na verdade, prova-se que são também ideais maximais de $\mathbb{Z}$.*

Sejam A um anel e I um ideal de A. Considere a relação de *congruência módulo I em A*, denotada por "$(mod\ I)$", dada por

$$a \equiv b(mod\ I) \text{ se } a - b \in I$$

para $a,b \in A$. Não é difícil ver que esta relação é uma relação de equivalência. Denotaremos a classe de equivalência de $a \in A$ por $a + I = \{a + x \mid x \in I\}$ ou, simplesmente, $\overline{a}$. Denotaremos o conjunto das classes por A/I. Temos

$$A/I = \{\overline{a} \mid a \in A\}.$$

Considerando as operações de adição "$\oplus$" e multiplicação "$\odot$" definidas por

$$\begin{array}{rccc} \oplus: & A/I \times A/I & \to & A/I \\ & (\overline{a},\overline{b}) & \mapsto & \overline{a} \oplus \overline{b} = \overline{a+b} \end{array} \quad \text{e} \quad \begin{array}{rccc} \odot: & A/I \times A/I & \to & A/I \\ & (\overline{a},\overline{b}) & \mapsto & \overline{a} \odot \overline{b} = \overline{ab} \end{array}$$

temos que estas operações estão bem definidas e que $(A/I, \oplus, \odot)$ é um anel, chamado de anel quociente de A por I. Veja que se A tem unidade, então $\overline{1_A}$ é a unidade do anel A/I e, além disso, $\overline{0_A}$ é o elemento neutro aditivo de A/I. Temos que $\overline{a} = \overline{b}$ se, e somente se, $a - b \in I$. Daí, $\overline{a} = \overline{0_A}$ se, e somente se, $a \in I$.

Um resultado bem interessante da teoria de anéis quocientes clássica é o seguinte:

Teorema 1.27. *Sejam A um anel comutativo com unidade e I um ideal próprio de A. Então:*

i. I é um ideal primo de A se, e somente se, A/I é um domínio de integridade.

ii. I é um ideal maximal de A se, e somente se, A/I é um corpo.

Diante deste resultado, quando p é um número primo, temos que o anel quociente $\mathbb{Z}/p\mathbb{Z}$ é um corpo e denotamos por $\mathbb{Z}_p$. Neste caso, $|\mathbb{Z}_p| = p$, isto é, $\mathbb{Z}_p$ é um corpo de p elementos.

Pela construção de anéis quocientes, temos que $\overline{m} = \overline{0}$ se, e somente se, $m \in p\mathbb{Z}$. Se $m \in \mathbb{Z}$, então $\overline{m} = \{m + pn \mid n \in \mathbb{Z}\}$. Pelo Algoritmo da Divisão, $m = pq + r$, com $0 \leq r \leq p-1$ e $q \in \mathbb{Z}$. Daí, $\overline{m} = \overline{r}$ e segue que

$$\mathbb{Z}_p = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\right\}.$$

Exemplo 1.28. *Sendo p um número primo, temos que $\mathbb{Z}_p$ é um anel simples, pois é corpo.*

Definição 1.29. *Um anel A é dito ser um **anel primo** se para quaisquer I e J ideais de A tais que $IJ = \{0_A\}$ tem-se $I = \{0_A\}$ ou $J = \{0_A\}$.*

Equivalentemente, tem-se que A é um anel primo quando para $I \neq \{0_A\}$ e $J \neq \{0_A\}$ ideais de A tem-se $IJ \neq \{0_A\}$.

Exemplo 1.30. *Todo anel simples é um anel primo. Em particular, o anel $M_n(\mathbb{K})$ é um anel primo.*

Exemplo 1.31. *O anel $\mathbb{Z}$ é um anel primo, porém não é simples. Basta ver que $2\mathbb{Z}$ é um ideal bilateral não nulo de $\mathbb{Z}$ e, obviamente, é um ideal próprio.*

Agora, vamos falar de homomorfismos de anéis.

Definição 1.32. *Sejam A e B anéis. Dizemos que uma aplicação $\varphi : A \to B$ é um homomorfismo de anéis se $\varphi(x+y) = \varphi(x) + \varphi(y)$ e $\varphi(xy) = \varphi(x)\varphi(y)$ para quaisquer $x, y \in A$. Ademais, dizemos que o homomorfismo φ é um isomorfismo de anéis se é bijetivo.*

Neste último caso, dizemos que A e B são *anéis isomorfos* ou que A é *isomorfo* a B, e denotamos por $A \simeq B$.

Observe que o Exemplo 1.15 implica que $Z(M_n(\mathbb{K})) \simeq \mathbb{K}$. Além disso, a definição do centro obtida nesse exemplo é válida para $M_n(A)$, no sentido de que $Z(M_n(A)) \simeq Z(A)$, onde A é um anel com unidade.

Definição 1.33. *Dizemos que uma aplicação $\varphi : A \to B$ é um anti-isomorfismo de anéis, se é bijetora, $\varphi(x+y) = \varphi(x) + \varphi(y)$ e $\varphi(xy) = \varphi(y)\varphi(x)$.*

1.2 Álgebras

Boa parte dos conceitos trabalhados na seção destinada para anéis podem ser estendidos para álgebras.

Definição 1.34. *Uma $\mathbb{K}$-álgebra é um par $(A, *)$, onde A é um $\mathbb{K}$-espaço vetorial e "$*$" é uma operação em A que é bilinear, ou seja, $* : A \times A \to A$ satisfaz:*

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

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

(c) $(\lambda a)*b = a*(\lambda b) = \lambda(a*b)$

para quaisquer $a,b,c \in A$ e $\lambda \in \mathbb{K}$.

Por simplicidade de notação, uma $\mathbb{K}$-álgebra $(A,*)$ será denotada por A. Denominaremos "$*$" como *multiplicação* da $\mathbb{K}$-álgebra A. Diremos que A é uma álgebra associativa, comutativa ou que possui elemento neutro, quando "$*$" for uma operação associativa, comutativa ou tiver elemento neutro em A, respectivamente. Também, por simplicidade $a*b$ será denotado por ab.

Observação 1.35. *Notemos que uma $\mathbb{K}$-álgebra associativa é um anel. Em nosso trabalho, salvo menção em contrário, estaremos considerando álgebras associativas.*

Exemplo 1.36. *Considere o $\mathbb{K}$-espaço $M_n(\mathbb{K})$, das matrizes quadradas de ordem n. Com a multiplicação usual de matrizes, temos que $M_n(\mathbb{K})$ é uma $\mathbb{K}$-álgebra associativa e com unidade, porém é não comutativa se $n \geq 2$. Além disso, se A é uma $\mathbb{K}$-álgebra, podemos tomar $M_n(A)$ de forma análoga ao que fizemos para anéis. Neste caso, $M_n(A)$ possui estrutura de $\mathbb{K}$-espaço vetorial, a qual, munida do produto usual, é uma $\mathbb{K}$-álgebra.*

Exemplo 1.37. *Se L é uma extensão de um corpo $\mathbb{K}$, então L tem uma estrutura natural de $\mathbb{K}$-espaço vetorial. Ainda mais, L é um anel associativo, comutativo e com unidade. Dito isso, L é uma $\mathbb{K}$-álgebra associativa, comutativa e com unidade cuja a multiplicação é a mesma do corpo L.*

Exemplo 1.38. *Considerando $\mathbb{K}[x]$, o $\mathbb{K}$-espaço vetorial dos polinômios na variável x com o produto usual de polinômios, temos que $\mathbb{K}[x]$ é uma $\mathbb{K}$-álgebra associativa, comutativa e com unidade.*

Exemplo 1.39. *Sejam V um $\mathbb{K}$-espaço vetorial e $\mathcal{L}(V)$ o espaço vetorial dos operadores lineares de V. Temos que $\mathcal{L}(V)$, munido da operação de composição, é uma $\mathbb{K}$-álgebra associativa e com unidade. É fato bastante conhecido que se $\dim_{\mathbb{K}} V = n$, então $\mathcal{L}(V) \simeq M_n(\mathbb{K})$ como anéis. Também são isomorfos como álgebras.*

Exemplo 1.40. ***(Álgebra de Grassmann)*** *Sejam $\mathbb{K}$ um corpo de característica diferente de 2, e V o espaço vetorial sobre $\mathbb{K}$ com base $\{e_1,e_2,e_3,\ldots\}$. Definimos a álgebra de Grassmann (ou álgebra exterior) de V, denotada por $E = E(V)$, como sendo a álgebra associativa e unitária com base*

$$\{1, e_{i_1}e_{i_2}\cdots e_{i_k} \mid i_1 < i_2 < \ldots < i_k; k \geq 1\},$$

através do produto induzido pela relação $e_ie_j = -e_je_i$, para quaisquer $i,\ j \in \mathbb{N}$. Também, $e_i^2 = 0$, para todo $i \in \mathbb{N}$. Destacamos em E os subespaços:

$$E_0 = span_{\mathbb{K}}\{1_E, e_{i_1}e_{i_2}\cdots e_{i_m} \mid m \text{ é par, } i_1 < i_2 < \ldots < i_m\}$$
$$e$$
$$E_1 = span_{\mathbb{K}}\{e_{i_1}e_{i_2}\cdots e_{i_m} \mid m \text{ é ímpar, } i_1 < i_2 < \ldots < i_m\}.$$

Claramente, $E = E_0 \oplus E_1$. Uma vez que $e_ie_j = -e_je_i$, temos

$$(e_{i_1}e_{i_2}\cdots e_{i_m})(e_{j_1}e_{j_2}\cdots e_{j_n}) = (-1)^{mn}(e_{j_1}e_{j_2}\cdots e_{j_n})(e_{i_1}e_{i_2}\cdots e_{i_m}),$$

para quaisquer $m,n \in \mathbb{N}$. Assim, podemos concluir que $ax = xa$, para quaisquer $a \in E_0$ e $x \in E$, e que $xy = -yx$ para quaisquer $x,y \in E_1$. Note que, se char $\mathbb{K} = 2$, então E é uma álgebra comutativa.

Definição 1.41. *Seja A uma $\mathbb{K}$-álgebra. Dizemos que:*

(a) um subespaço vetorial B de A é uma subálgebra de A se B é multiplicativamente fechado, isto é, $b_1b_2 \in B$ para quaisquer $b_1,b_2 \in B$;

(b) um subespaço vetorial I de A é um ideal de A se $xa, ax \in I$ para quaisquer $x \in I$ e $a \in A$.

De maneira análoga ao que foi definido para anéis, temos as seguintes definições para álgebras: ideal primo, álgebras quocientes, álgebras com divisão, álgebras simples, álgebras prima e homomorfismo de álgebras. Para estas definições, é necessário considerar a estrutura de $\mathbb{K}$-espaço vetorial de cada estrutura algébrica, garantindo que as operações de adição e multiplicação por escalares sejam compatíveis com a estrutura de álgebra. No caso de um homomorfismo de álgebras, além de preservar a adição e a multiplicação, devemos exigir a preservação da multiplicação por escalar, ou seja, o homomorfismo deve ser uma transformação linear.

1.3 Aplicações Comutantes

O principal objetivo deste trabalho de dissertação é estudar aplicações aditivas arbitrárias que possuem a propriedade de serem comutantes. Assim, nesta seção, apresentamos alguns conceitos e resultados sobre a teoria de aplicações comutantes, os quais servirão como base para a demonstração de alguns resultados nos próximos capítulos.

Definição 1.42. *Sejam X e Y conjuntos não vazios, munidos de uma operação de adição. Diremos que $f: X \to Y$ é uma aplicação aditiva, se $f(u+v) = f(u) + f(v)$, para quaisquer $u,v \in X$.*

Exemplo 1.43. *Homomorfismos de anéis e transformações lineares são exemplos de aplicações aditivas. No entanto, nem toda aplicação aditiva é um homomorfismo. Para ilustrar isso, considere a aplicação $\beta: M_n(\mathbb{K}) \to M_n(\mathbb{K})$ dada por $\beta(x) = xy$, para alguma matriz y em $M_n(\mathbb{K})$ fixa, diferente da matriz nula e da matriz identidade.*

Com efeito, considere $n = 2$ e $y = e_{21}$. Se β fosse um homomorfismo, deveríamos ter $\beta(x_1x_2) = \beta(x_1)\beta(x_2)$ para quaisquer $x_1, x_2 \in M_2(\mathbb{K})$. No entanto, tomando $x_1 = I_2$ (Identidade de ordem 2) e $x_2 = e_{12}$ temos que $\beta(x_1x_2) \neq \beta(x_1)\beta(x_2)$ (Veja que $e_{12}e_{21} \neq e_{21}e_{12}e_{21}$).

Exemplo 1.44. *Considere A um anel. Para cada $a \in A$, defina a aplicação $f_a : A \to A$ dada por $f_a(x) = [a,x]$. Temos que f_a é uma aplicação aditiva. De maneira análoga, verifica-se que $g_b : A \to A$ dada por $g_b(x) = [x,b]$ é uma aplicação aditiva.*

Exemplo 1.45. *Agora sejam p e q matrizes de ordem n invertíveis em $M_n(\mathbb{K})$. Defina a aplicação $\varphi_{p,q} \colon M_n(\mathbb{K}) \to M_n(\mathbb{K})$ dada por $\varphi_{p,q}(x) = pxq$. Temos que $\varphi_{p,q}$ é uma aplicação aditiva.*

Definição 1.46. *Dizemos que duas matrizes $a,b \in M_n(\mathbb{K})$ são semelhantes se existe $p \in GL_n(\mathbb{K})$ tal que $a = p^{-1}bp$.*

Vamos agora definir o que são matrizes equivalentes e relacioná-las com o problema de preservação linear.

Definição 1.47. *Dizemos que duas matrizes quadradas $a,b \in M_n(\mathbb{K})$ são equivalentes se existem $p,q \in GL_n(\mathbb{K})$ tais que $a = pbq$.*

Da Álgebra Linear básica, podemos relacionar matrizes quadradas a operadores lineares de um determinado espaço vetorial de dimensão finita. Assim, sendo V um espaço vetorial de dimensão n, podemos traduzir a definição acima para operadores lineares de V. Diremos que $T,S \in \mathcal{L}(V)$ são *operadores lineares equivalentes* se existem operadores $P,Q \in GL(V)$ tais que $PSQ = T$. Observe que matrizes semelhantes são matrizes equivalentes. Ademais, temos a seguinte caracterização para essa definição:

Proposição 1.48. *Duas matrizes $a,b \in M_n(\mathbb{K})$ são equivalentes se, e somente se, a tem o mesmo posto que b.*

Demonstração. Seja V um $\mathbb{K}$-espaço vetorial de dimensão finita n. Considere a identificação de a e b por T e S, operadores lineares de V, respectivamente. Sabe-se que o posto de um operador é a dimensão da imagem. Neste caso, $dim\, T(V)$ e $dim\, S(V)$ são finitas.

Desse modo, suponhamos que $T,S \in \mathcal{L}(V)$ sejam operadores equivalentes, isto é, existem $P,Q \in GL(V)$ tais que $PSQ = T$. Mostraremos que, nestas condições, S e T devem ter o mesmo posto. Inicialmente, vejamos que SQ tem o mesmo posto de S. De fato, como $V = Q(V)$ temos $S(V) = S(Q(V))$, ou seja, S e SQ devem ter o mesmo posto.

Agora, veja que PSQ tem o mesmo posto de S. Suponha que $dim\, SQ(V) = r = dim\, S(V)$ e considere $\beta = \{v_1, \ldots, v_r\}$ uma base de $SQ(V)$. Dessa forma, sendo P um isomorfismo, segue que $\{P(v_1), \ldots, P(v_r)\}$ é um conjunto gerador e LI de $P(SQ(V))$. Daí,

$$\{P(v_1), \ldots, P(v_r)\}$$

é uma base de $PSQ(V)$ com r elementos. Logo, $dim\ PSQ(V) = dim\ SQ(V) = dim\ S(V)$. Por fim, como $PSQ(V) = T(V)$, devemos ter $dim\ S(V) = dim\ PSQ(V) = dim\ T(V)$, isto é, S e T possuem o mesmo posto.

Reciprocamente, suponha que $dim\ T(V) = m = dim\ S(V)$. Seja $Q \colon V \to V$ um isomorfismo. Daí, $Q(V) = V$ donde obtemos $S(Q(V)) = S(V)$. Tomando $\beta_1 = \{S(v_1), \ldots, S(v_m)\}$ uma base para $S(V)$, em que $v_i \in V = Q(V)$, existem $u_1, \ldots, u_m \in V$ elementos linearmente independentes tais que $v_i = Q(u_i)$, para $1 \leq i \leq m$. Assim,

$$\beta_1 = \{S(Q(u_1)), \ldots, S(Q(u_m))\}.$$

Agora, considere $\beta_2 = \{T(w_1), \ldots, T(w_m)\}$ uma base de $T(V)$. Considere, então, uma base de V dada por

$$\beta = \{T(w_1), \ldots, T(w_m), z_{m+1}, \ldots, z_n\}$$

obtida completando-se a base β_2. Completando a base β_1 e reordenando se necessário, pelo Teorema Fundamental da Álgebra Linear, existe um único isomorfismo $P_1 \colon V \to V$ tal que $P_1(T(w_i)) = S(Q(u_i))$ para $1 \leq i \leq m$. Nestas condições, temos que $P_1(T(V)) = SQ(V)$. Tomando, $P = (P_1)^{-1}$ segue que $T = PSQ$. ■

O próximo exemplo é um típico caso da área de pesquisa de Problemas de Preservadores Lineares.

Exemplo 1.49. *Considere o anel $M_n(\mathbb{K})$. Suponha $p, q \in GL_n(\mathbb{K})$ satisfazendo* $\det(pq) = 1$. *Considere $\varphi : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ dada por $\varphi(x) = pxq$. Já vimos que φ é aditiva e é fácil ver que também é linear. Ademais, temos que* $\det(\varphi(x)) = \det(x)$*, para todo $x \in M_n(\mathbb{K})$.*

Neste caso, φ é um operador linear que denominaremos de *preservador linear da função determinante* ou, de forma simplificada, de *preservador de determinante*. Na mesma linha de raciocínio, sendo $\psi : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ dada por $\psi(x) = px^tq$, em que x^t denota a transposta da matriz x e $p, q \in GL_n(\mathbb{K})$ com $\det(pq) = 1$, temos que ψ também é um preservador linear da função determinante, uma vez que $\det(x) = \det(x^t)$.

Um resultado interessante provado por Frobenius [10, apud Pierce e Li [21]] diz que todo preservador de determinante tem a forma pxq ou px^tq, para $p, q \in GL_n(\mathbb{K})$ com $\det(pq) = 1$.

Vamos agora adicionar mais um adjetivo para aplicações aditivas.

Definição 1.50. *Sejam A um anel e X um subconjunto de A. Uma aplicação $f : X \to A$ é dita ser aplicação comutante em X se*

$$f(x)x = xf(x),\ \forall x \in X,$$

ou, equivalentemente, se $[f(x), x] = 0$, para todo $x \in X$.

Diremos que f é uma aplicação aditiva comutante em X se é aditiva e comutante em X.

Exemplo 1.51. *Seja A um anel. Observe que a aplicação* $Id_A : A \to A$ *dada por* $Id_A(x) = x$ *(identidade de A) é uma aplicação aditiva comutante em A. De maneira similar, a aplicação nula de A em A é uma aplicação aditiva comutante em A.*

Exemplo 1.52. *Seja* $f \colon M_n(\mathbb{K}) \to M_n(\mathbb{K})$ *dada por* $f(x) = ax + tr(x)I$*, para algum* $a \in \mathcal{Z}$*, em que I denota a matriz identidade de* $M_n(\mathbb{K})$*. Temos que f é uma aplicação aditiva comutante em* $M_n(\mathbb{K})$*.*

Antes de prosseguir, mencionaremos uma identidade que será útil neste trabalho. Seja A um anel, é fácil verificar que

$$[ab,c] = a[b,c] + [a,c]b, \quad \text{para } a,\ b,\ c \in A. \tag{1.1}$$

Fazendo indução sobre n, podemos mostrar que

$$[a_1a_2\cdots a_n, c] = \sum_{i=1}^{n} a_1\cdots a_{i-1}[a_i,c]a_{i+1}\cdots a_n, \tag{1.2}$$

para todos $a_i, c \in A$.

Vamos agora retornar a alguns exemplos.

Exemplo 1.53. *Seja A um anel. Para cada* $b \in A$*, definimos* $E_b \colon A \to A$ *dada por* $E_b(a) = ba$*. Temos que* E_b *é uma aplicação aditiva. Agora, supondo que* $b \in Z(A)$*, não é difícil ver que* $[E_b(a), a] = 0$*, para todo* $a \in A$*, isto é,* E_b *é uma aplicação aditiva comutante. De maneira análoga, temos as mesmas observações sobre a aplicação* D_b *de A em A dada por* $D_b(a) = ab$*.*

Para se convencer dessas duas últimas afirmações, basta aplicar a Eq. (1.1). Porém, isso deixa de ser verdadeiro se b não for central. Para ver isso, considere $A = M_n(\mathbb{K})$ *e tome a aplicação* $E_{e_{ij}} \colon A \to A$ *dada por* $E_{e_{ij}}(a) = e_{ij}a$*, para i e j fixos em* $\{1,2,\ldots,n\}$*. Notemos que* $E_{e_{ij}}(e_{ji})e_{ji} = e_{ij}e_{ji}e_{ji} = 0$*, mas* $e_{ji}E_{e_{ij}}(e_{ji}) = e_{ji}e_{ij}e_{ji} = e_{ji}$ *sempre que i e j são distintos. Esse último exemplo nos mostra que nem toda aplicação aditiva é comutante.*

Exemplo 1.54. *Seja A um anel. Toda aplicação aditiva* $f \colon A \to A$ *é comutante em* $Z(A)$*. Na verdade, a aplicação não precisa ser aditiva para satisfazer a propriedade de ser comutante. Para se convencer dessa última afirmação, considere* $A = \mathbb{R}$ *e tome* $f(x) = x^2$*. Claramente, qualquer elemento de* $\mathbb{R}$ *é central, porém f definida dessa maneira não é aditiva.*

Exemplo 1.55. *Seja* $f \colon M_n(\mathbb{K}) \to M_n(\mathbb{K})$ *dada por* $f(x) = ax + \det(x)I$*, para algum* $a \in \mathcal{Z}$*, em que I denota a matriz identidade de* $M_n(\mathbb{K})$*. Temos que f é uma aplicação comutante em* $M_n(\mathbb{K})$*, no entanto não é aditiva.*

Finalizaremos esta seção com um resultado simples, mas que será uma ferramenta fundamental para nossos resultados.

Proposição 1.56. *Sejam A um anel e* $f : A \to A$ *uma aplicação aditiva comutante em A. Então,* $[f(x), y] = [x, f(y)]$*, para quaisquer* $x, y \in A$*.*

Demonstração. De fato, pela aditividade de f e a definição de aplicação comutante, dada acima, tem-se

$$\begin{aligned} f(x+y)(x+y) = (x+y)f(x+y) &\Rightarrow (f(x)+f(y))(x+y) = (x+y)(f(x)+f(y)) \\ &\Rightarrow f(x)y+f(y)x = xf(y)+yf(x) \\ &\Rightarrow f(x)y-yf(x) = xf(y)-f(y)x \\ &\Rightarrow [f(x),y] = [x,f(y)], \end{aligned}$$

para quaisquer $x,y \in A$. ■

1.4 Derivações e Biderivações

Nesta seção, traremos as definições sobre aplicações chamadas de derivações e biderivações, além de apresentarmos alguns resultados inerentes ao seu estudo. Chamamos a atenção do leitor que esta seção é de suma importância em nosso trabalho, pois confere um suporte para os resultados que serão apresentados no Capítulo 2, os quais foram obtidos por França em [8]. Iniciemos definindo tais aplicações e fornecendo alguns exemplos.

Na texto redigido abaixo, quando não especificado, considere A um anel.

Definição 1.57. *Uma aplicação aditiva $\delta : A \to A$ é chamada de **derivação** se*

$$\delta(xy) = \delta(x)y + x\delta(y), \ \forall x,y \in A.$$

Claramente, a derivada de funções proveniente do cálculo diferencial é um exemplo de derivação. Vamos ver outro exemplo.

Exemplo 1.58. *No Exemplo 1.44 temos aplicações aditivas que são derivações. Com efeito, considere A um anel e $a \in A$, arbitrário e fixado. Sendo $f_a : A \to A$ dada por $f_a(x) = [a,x]$, para $x \in A$, segue que*

$$\begin{aligned} f_a(xy) = [a,xy] = axy - xya &= axy - xay + xay - xya \\ &= (ax - xa)y + x(ay - ya) \\ &= [a,x]y + x[a,y] \\ &= f_a(x)y + xf_a(y). \end{aligned}$$

De maneira análoga, tem-se que g_b (dada no Exemplo 1.44) é uma derivação.

Vamos agora introduzir uma pequena generalização de aplicações aditivas.

Uma aplicação **biaditiva** refere-se a uma aplicação que é aditiva em relação a cada uma das suas variáveis independentes, em um contexto algébrico. Formalmente, sejam X e Y conjuntos não vazios, munidos de uma operação de adição. Uma função $f\colon X\times X\to Y$ é chamada de biaditiva se satisfaz as seguintes condições para quaisquer $x,y,z\in X$:

(a) $f(x+y,z)=f(x,z)+f(y,z)$;

(b) $f(z,x+y)=f(z,x)+f(z,y)$.

Essencialmente, isso significa que f preserva a adição separadamente em cada argumento de $X\times X$.

Definição 1.59. *Uma aplicação biaditiva $\Delta : A^2\to A$ é dita ser uma **biderivação** em A se é uma derivação em cada argumento, isto é, se para todo $y\in A$ fixado, tem-se que $x\mapsto\Delta(x,y)$ e $x\mapsto\Delta(y,x)$ são derivações.*

Exemplo 1.60. *Não é difícil ver que $h:A^2\to A$ dada por $h(x,y)=[x,y]$, para quaisquer $x,y\in A$, é uma biderivação.*

Veja que, para todo $\lambda\in Z(A)$, a aplicação $f : A^2\to A$ dada por $f(x,y)=\lambda[x,y]$ é uma biderivação. Denominaremos tais aplicações de *biderivações internas*.

Se A for um anel não comutativo onde todas as biderivações são internas, então toda aplicação aditiva comutante f é da forma

$$f(x)=\lambda x+\mu(x),$$

com $\lambda\in Z(A)$ e $\mu:A\to Z(A)$ sendo uma aplicação aditiva.

Com efeito, observe que $\delta(x,y)=[f(x),y]$, com $x,y\in A$ é uma biderivação. Não é difícil ver que δ é biaditiva, pois o comutador é biaditivo e f é aditiva por hipótese. Ademais, fixe $y_0\in A$, arbitrário. Dados $x_1,x_2\in A$ temos

$$\delta(x_1x_2,y_0)=[f(x_1x_2),y_0].$$

Da Proposição 1.56 e propriedade (1.1) temos

$$\begin{aligned}[f(x_1x_2),y_0]&=[x_1x_2,f(y_0)]\\&=x_1[x_2,f(y_0)]+[x_1,f(y_0)]x_2\\&=x_1[f(x_2),y_0]+[f(x_1),y_0]x_2\\&=x_1\delta(x_2,y_0)+\delta(x_1,y_0)x_2.\end{aligned}$$

Fixado $x_0\in A$, arbitrário, não é difícil ver que $\delta(x_0,y)=[f(x_0),y]$ é uma derivação.

Sendo assim, existe $\lambda\in Z(A)$ tal que $\delta(x,y)=[f(x),y]=\lambda[x,y]$, para quaisquer $x,y\in A$. Daí, segue que $[f(x)-\lambda x,y]=0$, para todo $y\in A$, isto é, $f(x)-\lambda x\in Z(A)$, para todo $x\in A$. Assim, fica bem definida $\mu:A\to Z(A)$ dada por $\mu(x)=f(x)-\lambda x$.

Portanto, para mostrarmos que uma aplicação f aditiva comutante em um anel A tenha a forma $f(x) = \lambda x + \mu(x)$, com $\lambda \in Z(A)$ e $\mu : A \to Z(A)$ é suficiente mostrarmos que toda biderivação em A é interna.

Lema 1.61. *Seja Δ uma biderivação em um anel A. Então, para quaisquer $x, y, z, u, v \in A$ tem-se*

$$\Delta(x,y)z[u,v] = [x,y]z\Delta(u,v).$$

Demonstração. Seja Δ uma biderivação, isto é, uma aplicação que é uma derivação em cada argumento. Considere $\Delta(xu, yv)$ para $x, y, u, v \in A$ arbitrários. Aplicando a definição de derivação no primeiro argumento para $\Delta(xu, yv)$, obtemos

$$\Delta(xu,yv) = \Delta(x,yv)u + x\Delta(u,yv).$$

Similarmente, aplicando a definição de derivação no segundo argumento para cada parcela da soma, segue que

$$\Delta(x,yv)u + x\Delta(u,yv) = \Delta(x,y)vu + y\Delta(x,v)u + x\Delta(u,y)v + xy\Delta(u,v).$$

Logo,

$$\Delta(xu,yv) = \Delta(x,y)vu + y\Delta(x,v)u + x\Delta(u,y)v + xy\Delta(u,v). \tag{1.3}$$

Agora, aplicando primeiramente a definição de derivação no segundo argumento em $\Delta(xu, yv)$, obtem-se

$$\Delta(xu,yv) = \Delta(xu,y)v + y\Delta(xu,v).$$

Daí, aplicando a definição de derivação no primeiro argumento de cada parcela da soma, tem-se

$$\Delta(xu,yv) = \Delta(x,y)uv + x\Delta(u,y)v + y\Delta(x,v)u + yx\Delta(u,v).$$

Por conseguinte, de (1.3) e a igualdade citada imediatamente acima, segue que

$$\Delta(x,y)uv + yx\Delta(u,v) = \Delta(x,y)vu + xy\Delta(u,v),$$

ou seja,

$$\Delta(x,y)[u,v] = [x,y]\Delta(u,v), \tag{1.4}$$

para quaisquer $x, y, u, v \in A$.

Por fim, substituindo v por zv em $[u, v]$ e $\Delta(u, v)$, para $z \in A$ arbitrário, tem-se

$$[u,zv] = [u,z]v + z[u,v] \quad \text{e} \quad \Delta(u,zv) = \Delta(u,z)v + z\Delta(u,v).$$

Deste modo, em (1.4), obtemos

$$\Delta(x,y)[u,z]v+\Delta(x,y)z[u,v]=[x,y]\Delta(u,z)v+[x,y]z\Delta(u,v).$$

Lembre que $\Delta(x,y)[u,z]v=[x,y]\Delta(u,z)v$, uma vez que, por (1.4) vale $\Delta(x,y)[u,z]=[x,y]\Delta(u,z)$. Portanto,

$$\Delta(x,y)z[u,v]=[x,y]z\Delta(u,v),$$

para quaisquer $x,y,z,u,v\in A$. ■

Vamos agora aplicar nossa afirmação anterior em um caso concreto.

Teorema 1.62. *Seja A um anel com unidade tal que o ideal gerado por todos os comutadores em A seja igual a A. Então, toda biderivação em A é interna. Consequentemente, toda aplicação aditiva comutante f em A é da forma*

$$f(x)=\lambda x+\mu(x), \tag{1.5}$$

com $\lambda\in Z(A)$ e $\mu:A\to Z(A)$ sendo uma aplicação aditiva.

Demonstração. Seja $\Delta:A^2\to A$ uma biderivação. Por hipótese, sendo A um anel com unidade gerado pelos comutadores como ideal, devem existir $z_i,u_i,v_i,w_i\in A$, com $i\in I$ tais que $\sum_i z_i[u_i,v_i]w_i=1$. Deste modo, pelo Lema 1.61, observe que

$$\begin{aligned}\Delta(x,y)=\Delta(x,y)\sum_i z_i[u_i,v_i]w_i&=\sum_i \Delta(x,y)z_i[u_i,v_i]w_i\\&=\sum_i [x,y]z_i\Delta(u_i,v_i)w_i\\&=[x,y]\sum_i z_i\Delta(u_i,v_i)w_i.\end{aligned}$$

Como $z_i,u_i,v_i,w_i\in A$ são fixos, tem-se que $\Delta(x,y)=[x,y]\lambda$, para quaisquer $x,y\in A$, em que $\lambda=\sum_i z_i\Delta(u_i,v_i)w_i\in A$.

Afirmação: $\lambda\in Z(A)$.

De fato, por um lado tem-se

$$\Delta(x,yz)=[x,yz]\lambda=[x,y]z\lambda+y[x,z]\lambda$$

e, por outro lado, tem-se

$$\Delta(x,yz)=\Delta(x,y)z+y\Delta(x,z)=[x,y]\lambda z+y[x,z]\lambda.$$

Considerando as duas últimas igualdades, obtemos que $[x,y]z\lambda=[x,y]\lambda z$. Daí,

$$[x,y]z\lambda-[x,y]\lambda z=0,$$

ou seja,

$$[x,y][z,\lambda] = 0, \tag{1.6}$$

para quaisquer $x,y,z \in A$.

Agora, substituindo z por zw, com $w \in A$ arbitrário, em $[z,\lambda]$ tem-se

$$[zw,\lambda] = [z,\lambda]w + z[w,\lambda]. \tag{1.7}$$

Sendo assim, utilizando (1.7) em (1.6), segue-se que

$$\begin{aligned}[x,y][zw,\lambda] = 0 \Rightarrow & \, [x,y]\left([z,\lambda]w + z[w,\lambda]\right) \\ \Rightarrow & \, [x,y][z,\lambda]w + [x,y]z[w,\lambda] = 0.\end{aligned}$$

Ora, por (1.6) tem-se $[x,y][z,\lambda] = 0$, para quaisquer $x,y,z \in A$, donde obtém-se

$$[x,y]z[w,\lambda] = 0,$$

para quaisquer $x,y,z,w \in A$. Portanto, $[A,A]A[A,\lambda] = 0$. Agora, para todo $x \in A$, observe que

$$[x,\lambda] = \left(\sum_i z_i[u_i,v_i]w_i\right)[x,\lambda] = \sum_i z_i[u_i,v_i]w_i[x,\lambda].$$

Sendo $[A,A]A[A,\lambda] = 0$, segue-se que $[u_i,v_i]w_i[x,\lambda] = 0$, donde obtemos $[x,\lambda] = 0$, para todo $x \in A$, isto é, $[A,\lambda] = 0$, concluindo que $\lambda \in Z(A)$.

Portanto, dadas as condições do enunciado, toda biderivação Δ em A é interna. Por conseguinte, toda aplicação aditiva comutante f é da forma (1.5). ■

Corolário 1.63. *Seja A um anel simples com unidade. Então, toda aplicação aditiva comutante f em A tem a forma dada em* (1.5).

Demonstração. Se A é um anel comutativo, então $Z(A) = A$. Nestas condições, tomando $\lambda = 0$ e $\mu = f$, para qualquer aplicação f aditiva e comutante em A, segue o resultado.

Agora, se A é um anel não comutativo, então $[A,A] \neq \{0\}$. Como, por hipótese, A é um anel simples, tem-se que os únicos ideais bilaterais de A são os triviais. Daí, resta-nos que A e o ideal gerado por todos os comutadores em A coincidem. O resultado segue aplicando o Teorema 1.62. ■

Nos resultados acima, não podemos retirar a hipótese da unidade. Com efeito, tomando A um anel simples sem unidade com $Z(A) = \{0_A\}$, perceba que a aplicação identidade de A em A é certamente comutante, no entanto não pode ser expressa por $\lambda x + \mu(x)$, com $\lambda \in Z(A)$ e $\mu : A \to Z(A)$, haja vista que o $Z(A)$ é nulo.

1.5 PI-álgebras

Conforme já foi mencionado na Introdução, PI-álgebras e a FI-teoria estão relacionadas. Nesta ordem, os conceitos de PI são cruciais para os resultados apresentados no nosso trabalho, especialmente em relação às propriedades das matrizes e suas aplicações. Assim, dedicamos esta seção à descrição de alguns conceitos sobre álgebras com identidades polinomiais (PI-álgebras), pois há conceitos que aparecem em alguns resultados que utilizaremos como suporte. Por exemplo, no Capítulo 3, mais especificamente no Teorema 3.11, temos o polinômio *standard* St_4, o qual, pelos resultados relacionados ao Teorema de Amitsur-Levitzki[1], sabemos que a álgebra das matrizes $M_n(\mathbb{K})$, para $n = 3$, não satisfaz. Este último é um exemplo importante que utilizamos para demonstrar certas propriedades das aplicações comutantes. Além disso, o processo de linearização é uma técnica recorrente nas provas dos principais teoremas apresentados.

Diante disso, resolvemos trazer nesta seção, de forma breve e objetiva, uma noção básica sobre PI-álgebras. Com essa breve introdução, esperamos fornecer o embasamento necessário para a compreensão dos conceitos de PI que serão utilizados ao longo do nosso trabalho. Aqui nos baseamos nas referências [7, 12].

Observação 1.64. *Salvo menção em contrário, consideraremos no texto abaixo A uma álgebra associativa.*

Seja X um conjunto enumerável e não vazio. Os elementos x_i de X, com $i \in I$ (I denota um conjunto enumerável de índices), são chamados de variáveis. Uma palavra em X é uma sequência formada pela justaposição de variáveis de X. Por exemplo, dado $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, o elemento $x_{i_1}x_{i_2}\cdots x_{i_n}$, com $x_{i_j} \in X$, é uma palavra de tamanho n. Quando $n = 0$, chamaremos tal palavra de "palavra vazia" e denotaremos por 1. Além disso, tais palavras são não comutativas. Denote por $S(X)$ o conjunto das palavras em X.

Seja $\mathbb{K}$ um corpo. Desse modo, para qualquer conjunto X, não vazio, podemos definir a $\mathbb{K}$-álgebra $\mathbb{K}\langle X\rangle$ com base $S(X)$ e multiplicação estabelecida pela concatenação de palavras em X dada por

$$(x_{i_1}x_{i_2}\cdots x_{i_m})(x_{j_1}x_{j_2}\cdots x_{j_n}) = x_{i_1}x_{i_2}\cdots x_{i_m}x_{j_1}x_{j_2}\cdots x_{j_n}.$$

Dessa forma, dizemos que $\mathbb{K}\langle X\rangle$ é a *álgebra associativa livre unitária*, *livremente gerada por* X.

Agora, dado $f \in \mathbb{K}\langle X\rangle$, tem-se

$$f = \sum_{m\in S(X)} \lambda_m m,$$

onde $\lambda_m \in \mathbb{K}$ e o conjunto $\{\lambda_m \mid \lambda_m \neq 0, m \in S(X)\}$ é finito. Denominaremos os elementos de $\mathbb{K}\langle X\rangle$ de polinômios em variáveis não comutativas.

[1] Vide [7, p. 37]

Devemos considerar também a álgebra associativa livre não unitária, a qual denotaremos por $\mathbb{K}_0\langle X\rangle$, que consiste dos polinômios de $\mathbb{K}\langle X\rangle$ gerados por $S(X)\setminus\{1\}$.

Seja A uma álgebra com unidade. Defina $\varphi : K\langle X\rangle \to A$ tal que

$$\varphi(1) = 1_A \text{ e } \varphi(x_{i_1}x_{i_2}\cdots x_{i_m}) = a_{i_1}a_{i_2}\cdots a_{i_m}.$$

Não é difícil ver que φ é um homomorfismo de álgebras.

Dado um polinômio $f = f(x_1,x_2,\ldots,x_n) \in \mathbb{K}\langle X\rangle$, denotaremos por $f(a_1,a_2,\ldots,a_n)$ a imagem de f por φ. Observe que $f(a_1,a_2,\ldots,a_n)$ é o elemento de A obtido substituindo-se x_i por a_i em f.

Definição 1.65. *Sejam A uma álgebra e $f = f(x_1,x_2,\ldots,x_n) \in \mathbb{K}_0\langle X\rangle$, com $n \in \mathbb{N}$. Diremos que f é uma identidade polinomial de A, se $f(a_1,a_2,\ldots,a_n) = 0$, para quaisquer $a_1,a_2,\ldots,a_n \in A$.*

Podemos dizer que o polinômio nulo é uma identidade polinomial trivial. Agora, se A é uma álgebra que satisfaz alguma identidade polinomial não trivial $f \in \mathbb{K}_0\langle X\rangle$, dizemos que A é uma *PI-álgebra*.

Exemplo 1.66. *Álgebras comutativas são exemplos de PI-álgebras, já que tais álgebras satisfazem $f(x_1,x_2) = [x_1,x_2] = x_1x_2 - x_2x_1$ como uma identidade polinomial.*

Observação 1.67. *Seja A uma álgebra nilpotente. Definiremos como índice de nilpotência de A o menor $n \in \mathbb{N}$ tal que $a_1a_2\cdots a_n = 0$, para quaisquer $a_1,a_2,\ldots,a_n \in A$.*

Exemplo 1.68. *Álgebras nilpotentes de índice n também são exemplos de PI-álgebras. Tais álgebras satisfazem a identidade polinomial $f(x_1,\ldots,x_n) = x_1\cdots x_n$. Isso ocorre porque, em uma álgebra nilpotente de índice n, qualquer produto de n ou mais elementos é igual a zero.*

Um exemplo concreto é a álgebra das matrizes triangulares superiores de ordem n com diagonal nula, denotada por $NT_n(\mathbb{K})$. Em $NT_n(\mathbb{K})$, todos os elementos são matrizes triangulares superiores com zeros na diagonal, e o produto de quaisquer $n-1$ matrizes desse tipo resulta na matriz nula. Portanto, $NT_n(\mathbb{K})$ é nilpotente de índice $n-1$ e satisfaz a identidade polinomial $f(x_1,\ldots,x_n) = x_1\cdots x_{n-1}$, confirmando que é uma PI-álgebra.

Exemplo 1.69. *Seja E a álgebra de Grassmann. O polinômio $f(x_1,x_2,x_3) = [[x_1,x_2],x_3]$ é de fato uma identidade polinomial de E. Para entender isso, basta aplicar f nos elementos da base de E, visto no Exemplo 1.40, e estender por linearidade.*

Definição 1.70. *Considere o polinômio $f(x_1,\ldots,x_m) = \sum_{m\in S(X)} \lambda_m m \in \mathbb{K}\langle X\rangle$. Diremos que f é um **polinômio homogêneo** em x_i se o número de ocorrências da variável x_i em todas as suas palavras, com $\lambda_m \neq 0$, for igual. Quando f é homogêneo em todas as suas variáveis, diremos que f é **multi-homogêneo** e, denotando por α_i o número de ocorrências de x_i em f, para cada $i \in \{1,2,\ldots,m\}$, a m-upla $(\alpha_1,\ldots,\alpha_m)$ é chamada de **multigrau** de f.*

Exemplo 1.71. *Considere $m_1 = x_1^3x_2x_3x_2x_5^2$, $m_2 = x_2^2x_3x_4^5$ e $m_3 = x_1x_2x_3x_4x_5$ palavras em $\mathbb{K}\langle X\rangle$. Defina o polinômio $f = \lambda_1m_1 + \lambda_2m_2 + \lambda_3m_3 \in \mathbb{K}\langle X\rangle$, com $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$, não todos nulos. Temos que f é homogêneo em x_3, mas não multi-homogêneo.*

Exemplo 1.72. *O polinômio comutador $[x_1,x_2] = x_1x_2 - x_2x_1 \in \mathbb{K}\langle X\rangle$ é um polinômio multi-homogêneo.*

É importante mencionar que nem todo polinômio em $\mathbb{K}\langle X\rangle$ é multi-homogêneo. No entanto, qualquer polinômio em $\mathbb{K}\langle X\rangle$ pode ser escrito como uma soma de polinômios multi-homogêneos, agrupando todas as palavras em f de mesmo multigrau cujo escalar é não nulo. Tais parcelas serão chamadas de *componentes multi-homogêneas* de f. Dessa forma, f é multi-homogêneo se, e somente se, f possui uma única componente multi-homogênea. Por fim, caso f seja multi-homogêneo de multigrau $(1,\dots,1)$, diremos que f é um *polinômio multilinear*.

Um fato interessante, cuja demonstração é simples e pode ser encontrada no livro de Giambruno e Zaicev [12, pág. 19], diz o seguinte: seja A uma $\mathbb{K}$-álgebra gerada como espaço vetorial por um conjunto B sobre $\mathbb{K}$. Se um polinômio multilinear f se anula em B, então f é uma identidade polinomial de A. Assim, para polinômios multilineares, temos uma restrição de verificação de elementos da álgebra, o que nos permite identificar se um dado polinômio é ou não uma identidade para a álgebra.

Exemplo 1.73. *Uma álgebra associativa A de dimensão finita, digamos $\dim A < n$, satisfaz a identidade standard de grau n:*

$$St_n(x_1,\dots,x_n) = \sum_{\sigma\in S_n} (-1)^\sigma x_{\sigma(1)}\dots x_{\sigma(n)} \in \mathbb{K}\langle X\rangle,$$

onde S_n é o grupo simétrico das permutações de $\{1,2,\dots,n\}$ e $(-1)^\sigma$ é o sinal da permutação $\sigma \in S_n$. Para entender isso, basta considerar que o polinômio dado é multilinear e aplicar o comentário anterior utilizando como conjunto gerador uma base qualquer para A (para detalhes vide [12, pág. 12]).

Portanto, toda álgebra de dimensão finita é uma PI-álgebra. Em particular, $M_n(\mathbb{K})$ é uma PI-álgebra.

Exemplo 1.74. *(**Teorema de Amistsur e Levitzki**) A álgebra $M_n(K)$ das matrizes de ordem n satisfaz a identidade standard de grau $2n$. Para mais detalhes veja [12, Teorema 1.7.2, pág. 16]. Ainda mais, em [7, Lemma 3.1.1., pág. 37] é provado que a álgebra das matrizes $M_n(\mathbb{K})$ não satisfaz uma identidade polinomial de grau menor do que $2n$. Por exemplo, $M_3(\mathbb{K})$ não satisfaz o polinômio standard St_4, que é uma das hipóteses presentes no Teorema 3.11.*

Para concluir esta seção, abordaremos o *processo de linearização* de um polinômio. Segundo Brešar [4, pág. 147], esse conceito é aplicável em diversas situações na Matemática. Aqui, o utilizaremos para mostrar que ele pode ser empregado na transformação de uma identidade polinomial arbitrária em uma identidade multilinear.

Dado um polinômio $f(x_1,x_2,\ldots,x_n) \in \mathbb{K}\langle X\rangle$ multi-homogêneo, podemos obter um polinômio linear em uma variável x_i por meio do processo de linearização. Suponhamos que $\deg_{x_1} f > 1$. Consideremos y_1 e y_2 como variáveis distintas de $x_1,x_2,\ldots,x_n$. Definimos

$$h(y_1,y_2,x_2,\ldots,x_n) = f(y_1+y_2,x_2,\ldots,x_n) - f(y_1,x_2,\ldots,x_n) - f(y_2,x_2,\ldots,x_n).$$

Neste caso, como h é não nulo, temos $\deg_{x_1} f > \deg_{y_1} h, \deg_{y_2} h$. Podemos realizar esse procedimento para cada variável x_i até obtermos um polinômio de multigrau $(1,1,\ldots,1)$, ou seja, um polinômio multilinear. Neste caso, se f é uma identidade polinomial, então h também é. Esse comentário nos leva ao fato de que toda PI-álgebra satisfaz uma identidade polinomial multilinear.

O próximo exemplo servirá para ilustrar o processo de multilinearização, mas também há muitos exercícios contidos nas referências utilizadas.

Exemplo 1.75. *Consideremos o polinômio $f(x,y,z) = x^2yz + yzx^2$. Vejamos como linearizar o polinômio f. Considere $h_1(x_1,x_2,y,z) = f(x_1+x_2,y,z) - f(x_1,y,z) - f(x_2,y,z)$. Temos*

$$\begin{aligned}
h_1(x_1,x_2,y,z) &= (x_1+x_2)^2yz + yz(x_1+x_2)^2 - (x_1^2yz + yzx_1^2) - (x_2^2yz + yzx_2^2)\\
&= x_1^2yz + yzx_1^2 + x_2^2yz + yzx_2^2 + (x_1x_2)yz + yz(x_1x_2) + (x_2x_1)yz + yz(x_2x_1)\\
&- (x_1^2yz + yzx_1^2 + x_2^2yz + yzx_2^2)\\
&= x_1x_2yz + yzx_1x_2 + x_2x_1yz + yzx_2x_1
\end{aligned}$$

é um polinômio multilinear.

Agora, para dar uma noção do que será trabalhado do processo de linearização em aplicações multiaditivas em nossa redação à frente, temos os seguintes exemplos.

Exemplo 1.76. *Considere A um anel e $G : A^2 \to A$ uma aplicação biaditiva. Agora, considere $T : A \to A$ dada por $T(x) = G(x,x)$ (maiores detalhes serão vistos no Capítulo 3). Esta aplicação é o que denominaremos de traço de G. Quando $T(x)$ for nula podemos linearizar T obtendo a identidade $G(x_1,x_2) + G(x_2,x_1) = 0$. Com efeito, se $T(x) = 0$ para todo $x \in A$, então $G(x_1+x_2,x_1+x_2), G(x_1,x_1)$ e $G(x_2,x_2)$ são todos nulos, para quaisquer $x_1,x_2 \in A$. Daí, sendo G uma aplicação biaditiva, segue que*

$$\begin{aligned}
0 &= G(x_1+x_2,x_1+x_2) - G(x_1,x_1) - G(x_2,x_2)\\
&= G(x_1,x_1+x_2) + G(x_2,x_1+x_2) - G(x_1,x_1) - G(x_2,x_2)\\
&= [G(x_1,x_1) + G(x_1,x_2) + G(x_2,x_1) + G(x_2,x_2)] - G(x_1,x_1) - G(x_2,x_2)\\
&= G(x_1,x_2) + G(x_2,x_1).
\end{aligned}$$

Exemplo 1.77. *Similarmente, sejam A um anel e $G : A^3 \to A$ uma aplicação triaditiva (aditiva em cada entrada). Considere $T : A \to A$ dada por $T(x) = G(x,x,x)$. Quando $T(x)$ for nula* *obtemos a identidade*

$$\sum_{\sigma\in S_3} G(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)})=0.$$

Com efeito, dados $x_1,x_2\in A$ temos

$$G(x_1+x_2,x_1+x_2,x_1+x_2)=0.$$

Agora, utilizando a aditividade de G em cada entrada, segue que

$$\begin{aligned}0&=G(x_1+x_2,x_1+x_2,x_1+x_2)\\&=G(x_1,x_1,x_2)+G(x_1,x_2,x_1)+G(x_2,x_1,x_1)+G(x_1,x_2,x_2)+G(x_2,x_1,x_2)+G(x_2,x_2,x_1).\end{aligned}$$

Usando o fato que $G(x_1,x_1,x_1)=G(x_2,x_2,x_2)=0$ e substituindo x_2 por x_2+x_3, para $x_3\in A$ arbitrário, temos

$$\begin{aligned}0&=G(x_1,x_1,x_2+x_3)+G(x_1,x_2+x_3,x_1)+G(x_2+x_3,x_1,x_1)\\&+G(x_1,x_2+x_3,x_2+x_3)+G(x_2+x_3,x_1,x_2+x_3)+G(x_2+x_3,x_2+x_3,x_1)\\&=[G(x_1,x_1,x_2)+G(x_1,x_1,x_3)]+[G(x_1,x_2,x_1)+G(x_1,x_3,x_1)]+[G(x_2,x_1,x_1)+G(x_3,x_1,x_1)]\\&+[G(x_1,x_2,x_2+x_3)+G(x_1,x_3,x_2+x_3)]+[G(x_2,x_1,x_2+x_3)+G(x_3,x_1,x_2+x_3)]\\&+[G(x_2,x_2+x_3,x_1)+G(x_3,x_2+x_3,x_1)]\\&=[G(x_1,x_1,x_2)+G(x_1,x_1,x_3)]+[G(x_1,x_2,x_1)+G(x_1,x_3,x_1)]+[G(x_2,x_1,x_1)+G(x_3,x_1,x_1)]\\&+[G(x_1,x_2,x_2)+G(x_1,x_2,x_3)+G(x_1,x_3,x_2)+G(x_1,x_3,x_3)]\\&+[G(x_2,x_1,x_2)+G(x_2,x_1,x_3)+G(x_3,x_1,x_2)+G(x_3,x_1,x_3)]\\&+[G(x_2,x_2,x_1)+G(x_2,x_3,x_1)+G(x_3,x_2,x_1)+G(x_3,x_3,x_1)].\end{aligned}$$

Desse modo, realizando algumas contas segue que

$$\begin{aligned}0&=G(x_1+x_2+x_3,x_1+x_2+x_3,x_1+x_2+x_3)-G(x_1,x_1,x_1)-G(x_2,x_2,x_2)-G(x_3,x_3,x_3)\\&-([G(x_1,x_1,x_2)+G(x_1,x_1,x_3)]+[G(x_1,x_2,x_1)+G(x_1,x_3,x_1)]+[G(x_2,x_1,x_1)+G(x_3,x_1,x_1)])\\&-[G(x_1,x_2,x_2)+G(x_1,x_2,x_3)+G(x_1,x_3,x_2)+G(x_1,x_3,x_3)]\\&-[G(x_2,x_1,x_2)+G(x_2,x_1,x_3)+G(x_3,x_1,x_2)+G(x_3,x_1,x_3)]\\&-[G(x_2,x_2,x_1)+G(x_2,x_3,x_1)+G(x_3,x_2,x_1)+G(x_3,x_3,x_1)]\\&=\sum_{\sigma\in S_3} G(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)}).\end{aligned}$$

E a afirmação segue.

Esse procedimento pode ser aplicado indutivamente para $G: A^m\to A$ sendo uma aplicação m-aditiva. Nos resultados do Capítulo 3 usaremos esse procedimento de linearização.

1.6 Anéis de Frações de Martindale

Nesta última seção do capítulo de preliminares, nosso objetivo é estabelecer algumas noções básicas e apresentar resultados sobre *Martindale Rings of Quotients*, que traduziremos por Anéis de Frações de Martindale, sem nos aprofundarmos em demonstrações específicas dessa construção. Segundo Brešar em [4], a teoria de anéis de frações para anéis não comutativos generaliza o estudo da álgebra comutativa sobre anéis de frações. Na construção de anéis de frações, a propriedade de comutatividade é crucial e não pode ser desprezada.

No contexto de um anel não comutativo A, a construção do anel de frações de Martindale de A envolve considerações essenciais sobre os elementos do centro $Z(A)$, que desempenham o papel de "denominadores". Não nos aprofundaremos na construção detalhada desse processo aqui, pois nosso objetivo é oferecer uma introdução sucinta à construção do Anel de Frações de Martindale, com o propósito de familiarizar o leitor com os conceitos que serão utilizados ao longo deste trabalho.

É importante observar que todos os conceitos e resultados referentes à construção para anéis não comutativos, assim como outros detalhes desta seção, são abordados por Brešar em [4]. Por esse motivo, optamos por omitir demonstrações e alguns pormenores da construção.

Dos conceitos a serem tratados temos como objetivo definir o *Extended Centroid* (Centroide Estendido), o qual aparece em alguns resultados que foram utilizados para demonstrar os teoremas principais dos Capítulos 3 e 4, e dizer qual o centroide estendido de $M_n(\mathbb{K})$. Veremos que os conceitos estudados aqui podem ser vistos como uma generalização dos conceitos no estudo de Álgebras Centrais Simples. Sem mais, partimos para a construção.

Seja A um anel primo não nulo. Considere Σ o conjunto de todos os ideais não nulos de A. Desta forma, Σ é não vazio, pois $A \neq \{0_A\}$, isto é, $A \in \Sigma$. Ademais, Σ é um conjunto fechado ao produto de ideais e, por conseguinte, à interseção finita de ideais. Com efeito, sendo A um anel primo segue que $IJ = \{0_A\}$ se $I = \{0_A\}$ ou $J = \{0_A\}$, consequentemente, $IJ \neq \{0_A\}$ para $I \neq \{0_A\}$ e $J \neq \{0_A\}$. Como $IJ \subset I \cap J$, tem-se que $I \cap J \neq \{0_A\}$ quando $I \neq \{0_A\}$ e $J \neq \{0_A\}$.

Antes de seguirmos adiante, é importante mencionar que um A-módulo M é uma estrutura algébrica que generaliza a estrutura de espaço vetorial para anéis, não necessariamente comutativos, permitindo que um anel aja sobre um conjunto de forma semelhante à multiplicação por escalar em um espaço vetorial. Já um A-homomorfismo f é uma aplicação entre dois A-módulos que preserva a ação do anel A, ou seja, mantém a compatibilidade com as operações de módulo. Observando um anel A como um A-módulo (à direta ou à esquerda), temos que um ideal de A é um A-módulo (à direta ou à esquerda respectivamente). Um A-homomorfismo é uma generalização da ideia de transformação linear. Indicamos ao leitor as referências [4, 15] para uma conversa mais detalhada sobre módulos.

Dando continuidade, considere $I \in \Sigma$ e $f : I \to A$ um homomorfismo de A-módulos à direita.

Desse modo, considere o conjunto

$$X = \{(f,I) \mid f : I \to A \text{ é um homomorfismo de } A\text{-módulos à direita}, I \in \Sigma\}.$$

Defina a relação "$\sim$" em X dada por

$$(f,I) \sim (g,J) \text{ se } f \text{ e } g \text{ coincidem em algum } K \in \Sigma \text{ tal que } K \subseteq I \cap J.$$

Não é difícil ver que "$\sim$" é uma relação de equivalência. Com efeito, $(f,I) \sim (f,I)$ (reflexividade) é imediato e que se $(f,I) \sim (g,J)$, então $(g,J) \sim (f,I)$ (simetria). Agora, mostremos a transitividade. Suponha que $(f,I) \sim (g,J)$ e $(g,J) \sim (h,K)$. Então, existem $H_1, H_2 \in \Sigma$, com $H_1 \subseteq I \cap J$ e $H_2 \subseteq J \cap K$, tais que $f(x) = g(x)$ para todo $x \in H_1$ e $g(y) = h(y)$ para todo $y \in H_2$. Como $H_1, H_2 \in \Sigma$, tem-se $H_3 = H_1 \cap H_2 \in \Sigma$, com $H_3 \subseteq H_1 \subseteq I$ e $H_3 \subseteq H_2 \subseteq K$. Note que se $z \in H_3$, temos $z \in H_1$ e $z \in H_2$, donde $f(z) = g(z) = h(z)$. Daí, $f(z) = h(z)$, para todo $z \in H_3$. Como $H_3 \subseteq I \cap K$, temos que $(f,I) \sim (h,K)$.

Denotaremos por $[f,I]$ a classe de equivalência determinada por (f,I) e por $Q_r(A)$ o conjunto das classes de equivalência. Defina em $Q_r(A)$ as operações $+ : Q_r(A) \times Q_r(A) \to Q_r(A)$, dada por

$$[f,I] + [g,J] = [f+g, I \cap J]$$

e $\cdot : Q_r(A) \times Q_r(A) \to Q_r(A)$, dada por

$$[f,I] \cdot [g,J] = [f \circ g, JI].$$

Nestas condições, temos que "$+$" e "$\cdot$" são, respectivamente, as operações de adição e multiplicação de $Q_r(A)$. Vejamos que ambas estão bem definidas. Com efeito, considere $[f_1,I_1] + [f_2,I_2] \in Q_r(A)$. Observe que $f_1 \circ f_2$ está definida em $I_2 I_1 \subset A$. Ora, dado xy, com $x \in I_2$ e $y \in I_1$, desde que f_2 é um homomorfismo de A-módulo à direita, temos $f_2(xy) = f_2(x)y \in I_1$. Como f_2 é uma aplicação aditiva, tem-se $f_2(I_2 I_1) \subseteq I_1$.

Sendo assim, tome $(f_1,I_1) \sim (g_1,J_1)$ e $(f_2,I_2) \sim (g_2,J_2)$. Daí, existem $K_1, K_2 \in \Sigma$ tais que $K_1 \subseteq I_1 \cap J_1$, $K_2 \subseteq I_2 \cap J_2$, $f_1 = g_1$ em K_1 e $f_2 = g_2$ em K_2. Observe que $K_1 \cap K_2 \in \Sigma$. Assim, é imediato que $f_1 + f_2 = g_1 + g_2$ em $K_1 \cap K_2$, ou seja $(f_1 + f_2, K_1 \cap K_2) \sim (g_1 + g_2, K_1 \cap K_2)$, donde

$$[f_1,I_1] + [f_2,I_2] = [f_1 + f_2, K_1 \cap K_2] = [g_1 + g_2, K_1 \cap K_2] = [g_1,J_1] + [g_2,J_2].$$

Ademais, sendo $K_1, K_2 \in \Sigma$, tem-se que $K_2 K_1 \in \Sigma$, pois $K_2 K_1$ é não nulo. Agora, sendo $f_2 = g_2$ em K_2 e f_2 e g_2 homomorfismos de A-módulo à direita, temos que

$$f_2(K_2) = g_2(K_2) \Rightarrow f_2(K_2)K_1 = g_2(K_2)K_1 \subseteq K_1 \Rightarrow f_2(K_2K_1) = g_2(K_2K_1) \subseteq K_1.$$

Como $f_1 = g_1$ em K_1 e $f_2(K_2K_1) = g_2(K_2K_1) = Y \subseteq K_1$ temos que $f_1(Y) = g_1(Y)$, isto é,

$f_1(f_2(K_2K_1)) = g_1(g_2(K_2K_1))$, ou seja, $(f_1 \circ f_2)(K_2K_1) = (g_1 \circ g_2)(K_2K_1)$, donde concluímos que $f_1 \circ f_2 = g_1 \circ g_2$ em K_2K_1, ou seja, $(f_1 \circ f_2, I_2I_1) \sim (g_1 \circ g_2, J_2J_1)$. Daí,

$$[f_1, I_1][f_2, I_2] = [f_1 \circ f_2, I_2I_1] = [g_1 \circ g_2, J_2J_1] = [g_1, J_1][g_2, J_2].$$

Não é difícil de verificar que, sendo 0 o homomorfismo nulo de A em A, tem-se que $[0, A]$ é o neutro aditivo (zero) de $Q_r(A)$ e que, sendo Id_A o homomorfismo identidade de A em A, $[Id_A, A]$ é a unidade de $Q_r(A)$.

Com essas operações temos que $Q_r(A)$ é um anel com unidade.

Definição 1.78. *O anel $Q_r(A)$ é chamado de **Anel de Frações de Martindale à Direita** de A.*

De forma análoga pode-se construir o **Anel de Frações de Martindale à Esquerda** de A, o qual denotamos por $Q_l(A)$. Em geral, tem-se que $Q_r(A) \not\simeq Q_l(A)$.

Doravante, todos os resultados desta seção têm suas respectivas demonstrações em [4, Chapter 7, pág. 171].

Teorema 1.79. *Seja $A \neq \{0_A\}$ um anel primo e Σ o conjunto de todos os ideais não nulos de A. Então, $Q_r(A)$ tem as seguintes propriedades:*

i. $Q_r(A)$ é um anel unitário contendo A como "subanel";

ii. Para todo $q \in Q_r(A)$, existe $I \in \Sigma$ tal que $qI \subseteq A$;

iii. Para todo $q \in Q_r(A)$ e $I \in \Sigma$, $qI = 0$ implica $q = 0$;

iv. Se $I \in \Sigma$ e e $f : I \to A$ é um homomorfismo A-módulos à direita, então existe $q \in Q_r(A)$ tal que $f(x) = qx$ para todo $x \in I$.

Além disso, se Q é um anel com as propriedades (a)-(d), então $Q \simeq Q_r(A)$.

Proposição 1.80. *Se A é um anel simples com unidade, então $A \simeq Q_r(A)$.*

Demonstração. Suponhamos que A é um anel simples com unidade. Vejamos que A satisfaz às propriedades (a)-(d) do Teorema 1.79, donde concluiremos que $A \simeq Q_r(A)$.

Com efeito, é imediato que A satisfaz a propriedade (a). Como A é um anel simples tem-se que $\Sigma = \{A\}$. Daí, dado $q \in A$ é imediato que $qA \subseteq A$, donde obtemos a propriedade (b). Agora, veja que para todo $q \in A$ tal que $qA = \{0_A\}$, segue do fato de A ter unidade que $q \in qA = \{0_A\}$, ou seja, $q = 0_A$ e obtemos a propriedade (c).

Por fim, considere $f : A \to A$ um homomorfismo de A como A-módulo à direita. Tem-se que $f(x) = f(1_A x) = f(1_A)x$ para todo $x \in A$. Tomando $q = f(1_A)$ obtemos a propriedade (d). Concluímos pelo Teorema 1.79 que $A \simeq Q_r(A)$. ■

Corolário 1.81. *Seja $M_n(\mathbb{K})$ o anel das matrizes quadradas de ordem n sobre um corpo $\mathbb{K}$. Então, $M_n(\mathbb{K}) \simeq Q_r(M_n(\mathbb{K}))$.*

1.6.1 Centroide Estendido

Aqui ainda estamos considerando A um anel primo não nulo e continuaremos denotando por Σ o conjunto dos ideais não nulos de A. Também, quando necessário, evocaremos as propriedades do Teorema 1.79.

Definição 1.82. *O centro do anel $Q_r(A)$ é o que chamaremos de **centroide estendido** de A.*

Denotaremos o centroide estendido de A por $\mathcal{C}$. Voltando para matrizes, temos que $\mathcal{C} = \mathcal{Z}$, onde $\mathcal{Z}$ denota o centro de $M_n(\mathbb{K})$. Mais geralmente, é possível demonstrar que o centroide estendido de um anel primo é um corpo, o que nos motiva a fazer as seguintes definições.

Definição 1.83. *Seja A um anel primo não nulo. Então:*

*(a) Definimos o **fecho central** de A como sendo a $\mathcal{C}$-subálgebra de $Q_r(A)$ gerada por A, e o denotaremos por $A_{\mathcal{C}}$;*

*(b) Dizemos que A é **centralmente fechado** se $A = A_{\mathcal{C}}$.*

Por fim, entenderemos por álgebra prima centralmente fechada um anel primo centralmente fechado visto como $\mathcal{C}$-álgebra, e assim dizemos que uma $\mathbb{K}$-álgebra prima A é uma **álgebra prima centralmente fechada** *sobre $\mathbb{K}$ se é unitária e $\mathcal{C} = Z(A) = \mathbb{K} \cdot 1_A$.*

Entendemos que existem várias vertentes e resultados que podemos abordar nesta teoria. Entretanto, mencionaremos um último resultado, lembrando que esses e muitos outros resultados podem ser encontrados na referência [4].

Proposição 1.84. *A $\mathbb{K}$-álgebra das matrizes quadradas de ordem n é uma álgebra prima centralmente fechada.*

Este último resultado informa-nos que uma álgebra prima centralmente fechada pode, assim, ser considerada uma generalização da noção de álgebra central simples.

CAPÍTULO 2

Aplicações Comutantes Sobre Matrizes

Sejam A e B anéis, e J um subconjunto não vazio de A. Uma aplicação $\alpha\colon J \to B$ é chamada **preservadora da comutatividade** se, para quaisquer $x, y \in J$, $[x, y] = 0$ implica $[\alpha(x), \alpha(y)] = 0$. Observe que os homomorfismos de Lie são exemplos de aplicações que preservam a comutatividade. No problema que estudaremos agora, buscaremos descrever aplicações que possuem a propriedade comutante, o que é, em princípio, mais difícil do que descrever os homomorfismos de Lie. Mas, é claro, nos limitaremos a algumas situações menos gerais do que no caso dos homomorfismos de Lie.

A partir de agora, concentraremos nossos estudos a cerca de aplicações aditivas definidas sobre a álgebra de matrizes $M_n(\mathbb{K})$ em si mesma, com a propriedade de serem comutantes, a qual denominaremos de *aplicações comutantes*, em subconjuntos de matrizes que não são fechados sob a adição. A saber, temos como propósito descrever tais aplicações comutantes no subconjunto das matrizes singulares e também no subconjunto das matrizes invertíveis. Neste capítulo, apresentaremos os resultados que foram obtidos por França em [8]. Ademais, o leitor pode recordar sobre aplicações aditivas e comutantes na Seção 1.3.

França destaca em [8] que os resultados da teoria de identidades funcionais apresentada por Brešar, et al. em [5] foram obtidos apenas para conjuntos que são fechados sob a adição. Desta forma, o que vamos apresentar neste capítulo tem como objeto de estudo uma extensão de resultados da teoria de Identidades Funcionais[1] para subconjuntos da álgebra de matrizes $M_n(\mathbb{K})$ que não são fechados sob a adição.

[1] Para o estudo de *Functional identities* indicamos ao leitor a referência [5]

2.1 Aplicações Comutantes em Matrizes Singulares

O teorema a seguir é o primeiro resultado que apresentaremos e diz respeito a aplicações comutantes sobre o conjunto das matrizes singulares, as quais podemos descrever sua forma. Lembramos que, no que se segue, $\mathcal{Z}$ denota o centro da álgebra $M_n(\mathbb{K})$.

Teorema 2.1. *Seja $G : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ uma aplicação aditiva tal que*

$$G(x)x = xG(x),\ \forall x \in M_n(\mathbb{K}),\ singular.$$

Então, existe um elemento $\lambda \in \mathcal{Z}$ e uma aplicação aditiva $\mu : M_n(\mathbb{K}) \to \mathcal{Z}$ tal que

$$G(x) = \lambda x + \mu(x),\ \forall x \in M_n(\mathbb{K}).$$

Demonstração. Suponhamos que $G(x)x = xG(x)$ para toda matriz singular x de ordem n. Considere $z,w \in \mathcal{Z}$ arbitrários. Note que $(zI)\cdot e_{ij} = ze_{ij}$, com $z \in \mathbb{K}$, é uma matriz singular, para quaisquer $i, j \in \{1,\dots,n\}$. Ademais, observe que $ze_{ij} + we_{kl}$ é sempre uma matriz singular para $n \geq 3$ e $i, j,k,l \in \{1,\dots,n\}$. Logo, para $n \geq 3$, tem-se

$$G(ze_{ij} + we_{kl})(ze_{ij} + we_{kl}) = (ze_{ij} + we_{kl})G(ze_{ij} + we_{kl}).$$

Usando a distributividade na última igualdade, obtemos

$$G(ze_{ij} + we_{kl})ze_{ij} + G(ze_{ij} + we_{kl})we_{kl} = ze_{ij}G(ze_{ij} + we_{kl}) + we_{kl}G(ze_{ij} + we_{kl}).$$

Utilizando a aditividade de G, por um lado da igualdade supracitada obtemos

$$G(ze_{ij})ze_{ij} + G(ze_{ij})we_{kl} + G(we_{kl})ze_{ij} + G(we_{kl})we_{kl}$$

e, por outro lado, obtemos

$$ze_{ij}G(ze_{ij}) + we_{kl}G(ze_{ij}) + ze_{ij}G(we_{kl}) + we_{kl}G(we_{kl}).$$

Comparando as expressões obtidas e usando a hipótese sobre matrizes singulares, ou seja, o fato que $G(ze_{ij})ze_{ij} = ze_{ij}G(ze_{ij})$ e $G(we_{kl})we_{kl} = we_{kl}G(we_{kl})$ tem-se a seguinte igualdade

$$G(ze_{ij})we_{kl} + G(we_{kl})ze_{ij} = ze_{ij}G(we_{kl}) + we_{kl}G(ze_{ij}). \tag{2.1}$$

Provaremos que tal igualdade obtida ainda é válida quando $n = 2$. De fato, não é difícil ver que $ze_{ii} + we_{ip}$ e $ze_{ii} + we_{pi}$ são singulares quando $p \neq i$. Logo, aplicando a hipótese, tem-se $G(ze_{ii} + we_{ip})(ze_{ii} + we_{ip}) = (ze_{ii} + we_{ip})G(ze_{ii} + we_{ip})$. Observe que vale (2.1) para este caso,

ou seja,

$$G(ze_{ii})we_{ip} + G(we_{ip})ze_{ii} = ze_{ii}G(we_{ip}) + we_{ip}G(ze_{ii}),$$

quando $p \neq i$. Procedemos de maneira inteiramente análoga para $ze_{ii} + we_{pi}$.

Agora, para qualquer $y \in \mathcal{Z}$ tem-se ye_{11} é uma matriz singular. Logo, devemos ter que $G(ye_{11})ye_{11} = ye_{11}G(ye_{11})$. Daí, como $e_{11} \cdot e_{22} = 0 = e_{22} \cdot e_{11}$ segue que

$$0 = G(ye_{11})ye_{11}e_{22} = ye_{11}G(ye_{11})e_{22}.$$

Como

$$e_{22}G(ye_{11})ye_{11} = e_{22}ye_{11}G(ye_{11}) = 0,$$

tem-se $e_{22}ye_{11} = y(e_{22} \cdot e_{11})$, uma vez que $y \in \mathcal{Z}$.

Ademais, usando o fato de y ser invertível, segue que $e_{22}G(ye_{11})e_{11} = e_{11}G(ye_{11})e_{22} = 0$, donde

$$\begin{aligned}
G(ye_{11}) = I_2G(ye_{11})I_2 &= (e_{11} + e_{22})G(ye_{11})(e_{11} + e_{22}) \\
&= e_{11}G(ye_{11})e_{11} + e_{11}G(ye_{11})e_{22} + e_{22}G(ye_{11})e_{11} + e_{22}G(ye_{11})e_{22} \\
&= e_{11}G(ye_{11})e_{11} + e_{22}G(ye_{11})e_{22}.
\end{aligned}$$

Repetindo de forma análoga a argumentação anterior, tem-se

$$G(ye_{22}) = e_{11}G(ye_{22})e_{11} + e_{22}G(ye_{22})e_{22},$$

para qualquer $y \in \mathcal{Z}$.

Assim, veja que $G(ye_{11})$ comuta com xe_{22} e $G(ye_{22})$ comuta com xe_{11}, para quaisquer $x, y \in \mathcal{Z}$. Ora, lembrando que $(e_{ii})^2 = e_{ii}$, segue que

$$\begin{aligned}
G(ye_{11})xe_{22} &= (e_{11}G(ye_{11})e_{11} + e_{22}G(ye_{11})e_{22})xe_{22} \\
&= (e_{22}G(ye_{11})e_{22})xe_{22} \\
&= xe_{22}G(ye_{11})(e_{22})^2 \\
&= xe_{22}G(ye_{11})e_{22} \\
&= x(e_{22})^2G(ye_{11})e_{22} \\
&= xe_{22}(e_{22}G(ye_{11})e_{22}) \\
&= xe_{22}(e_{11}G(ye_{11})e_{11} + e_{22}G(ye_{11})e_{22}) = xe_{22}G(ye_{11}).
\end{aligned}$$

A conta é inteiramente análoga para ver que $[G(ye_{22}), xe_{11}] = 0$. Sendo assim, usando que $[G(ye_{11}), xe_{22}] = [G(ye_{22}), xe_{11}] = 0$ e a hipótese de que $[G(xe_{22}), xe_{22}] = [G(xe_{11}), xe_{11}] = 0$, para quaisquer $x,y \in \mathcal{Z}$, segue que

$$\begin{aligned}
G(ze_{11}+we_{22})(ze_{11}+we_{22}) &= G(ze_{11}+we_{22})ze_{11}+G(ze_{11}+we_{22})we_{22}\\
&= G(ze_{11})ze_{11}+G(ze_{11})we_{22}+G(we_{22})ze_{11}+G(we_{22})we_{22}\\
&= ze_{11}G(ze_{11})+we_{22}G(ze_{11})+ze_{11}G(we_{22})+we_{22}G(we_{22})\\
&= ze_{11}G(ze_{11}+we_{22})+we_{22}G(ze_{11}+we_{22})\\
&= (ze_{11}+we_{22})G(ze_{11}+we_{22}).
\end{aligned}$$

Por conseguinte, nós obtemos que

$$G(ze_{11})we_{22}+G(we_{22})ze_{11} = ze_{11}G(we_{22})+we_{22}G(ze_{11}).$$

Agora, considere a matriz $B = ze_{11}+we_{12}+ze_{21}+we_{22}$, com $z,w \in \mathcal{Z}$ arbitrários. É notório que B é singular. Logo, vale que $G(B)B = BG(B)$, isto é,

$$\begin{aligned}
&G(ze_{11}+we_{12}+ze_{21}+we_{22})(ze_{11}+we_{12}+ze_{21}+we_{22}) =\\
&\qquad (ze_{11}+we_{12}+ze_{21}+we_{22})G(ze_{11}+we_{12}+ze_{21}+we_{22}).
\end{aligned}$$

Por um lado, o primeiro membro da igualdade anterior tem a forma

$$\begin{aligned}
&G(ze_{11})(ze_{11}+we_{12}+ze_{21}+we_{22})+G(we_{12})(ze_{11}+we_{12}+ze_{21}+we_{22})+\\
&G(ze_{21})(ze_{11}+we_{12}+ze_{21}+we_{22})+G(we_{22})(ze_{11}+we_{12}+ze_{21}+we_{22}).
\end{aligned}$$

Já o outro membro tem a forma

$$\begin{aligned}
&(ze_{11}+we_{12}+ze_{21}+we_{22})G(ze_{11})+(ze_{11}+we_{12}+ze_{21}+we_{22})G(we_{12})+\\
&(ze_{11}+we_{12}+ze_{21}+we_{22})G(ze_{21})+(ze_{11}+we_{12}+ze_{21}+we_{22})G(we_{22}).
\end{aligned}$$

Pelo que já foi argumentado para $n = 2$, sabe-se que

$$\begin{aligned}
&G(ze_{ii})we_{ip}+G(we_{ip})ze_{ii} = ze_{ii}G(we_{ip})+we_{ip}G(ze_{ii}), \quad \text{quando} \quad p \neq i,\\
&G(ze_{11})we_{22}+G(we_{22})ze_{11} = ze_{11}G(we_{22})+we_{22}G(ze_{11})
\end{aligned}$$

e, também das hipóteses, que $[G(ye_{ij}), ye_{ij}] = 0$ para quaisquer $z,w,y \in \mathcal{Z}$. Mediante ao que foi obtido, fazendo a distributividade dos dois lados da igualdade, ver-se que alguns termos se cancelam e não é difícil ver que

$$G(we_{12})ze_{21}+G(ze_{21})we_{12} = we_{12}G(ze_{21})+ze_{21}G(we_{12}).$$

Deste modo, (2.1) vale para $n = 2$ e, consequentemente, para todo $n \in \mathbb{N}$. Agora, considerando uma matriz $x \in M_n(\mathbb{K})$ dada por $x = \sum x_{ij}e_{ij}$, temos que

$$G(x)x = G\left(\sum x_{ij}e_{ij}\right)\left(\sum x_{ij}e_{ij}\right) = \left(\sum G\left(x_{ij}e_{ij}\right)\right)\left(\sum x_{ij}e_{ij}\right).$$

Neste ponto, utilizaremos as igualdades

$$G(ze_{ij})ze_{ij} = ze_{ij}G(ze_{ij});$$
$$G(ze_{ij})we_{kl} + G(we_{kl})ze_{ij} = ze_{ij}G(we_{kl}) + we_{kl}G(ze_{ij}),$$

para se obter $G(x)x = xG(x)$, para toda $x \in M_n(\mathbb{K})$.

Portanto, sendo G uma aplicação aditiva comutante em $M_n(\mathbb{K})$, que é um anel simples com unidade, o resultado segue pelo Corolário 1.63. ■

2.2 Aplicações Comutantes em Matrizes Invertíveis

Agora, temos como objetivo estudar aplicações comutantes sobre o conjunto das matrizes invertíveis. Para início de conversa, vamos a um resultado auxiliar.

Proposição 2.2. *Seja $\mathbb{K}$ um corpo com mais de dois elementos, ou seja, $|\mathbb{K}| > 2$. Considere $G : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ uma aplicação aditiva tal que*

$$G(x)x = xG(x),\ \forall x \in GL_n(\mathbb{K}).$$

Então, $G(z) \in \mathcal{Z}$, para todo $z \in \mathcal{Z}$.

Demonstração. Considere e_{ij}, com $i \neq j$, isto é, uma matriz unitária não diagonal e, desde que $\mathbb{K} \neq \{0\}$ considere $z \in \mathcal{Z}$ um elemento não nulo. Observe que a matriz $I + e_{ij}$ é uma matriz invertível. Ora, sendo $|\mathbb{K}| > 2$ segue-se que existe $\lambda \in \mathbb{K} \setminus \{0\}$ tal que $u = \lambda(I + e_{ij})$ e $v = z + u = z + \lambda(I + e_{ij})$ são matrizes invertíveis. Perceba que no caso em que $|\mathbb{K}| = 3$, ou seja, $\mathbb{K} \simeq \mathbb{Z}_3$, bastaria tomar $\lambda I = z \neq 0$ e teríamos $\lambda I + z \neq 0$.

Desta forma, por hipótese, tem-se $[G(u), u] = 0 = [G(z), z] = [G(v), v]$. Logo, substituindo $v = z + u$, da hipótese de G ser aditiva e do fato de $z \in \mathcal{Z}$, segue que

$$G(z+u)(z+u) = (z+u)G(z+u),$$

donde temos $[G(z) + G(u)](z+u) = (z+u)[G(z) + G(u)]$. Daí, resulta que

$$G(z)u + G(u)z = uG(z) + zG(u),$$

isto é, $G(z)u = uG(z)$.

Substituindo $u = \lambda(I + e_{ij}) = \lambda I + \lambda e_{ij}$, com $i \neq j$, temos $G(z)(\lambda I + \lambda e_{ij}) = (\lambda I + \lambda e_{ij})G(z)$.

Logo,

$$G(z)\lambda I + G(z)\lambda e_{ij} = \lambda I G(z) + \lambda e_{ij} G(z),$$

isto é, $G(z)\lambda e_{ij} = \lambda e_{ij} G(z)$. Daí,

$$G(z)e_{ij} = e_{ij}G(z)$$

pois $\lambda I \in \mathcal{Z}$ e $\lambda \in \mathbb{K}$ são invertíveis. Em outras palavras, $[G(z), e_{ij}] = 0$.

Agora, veja que

$$[G(z), e_{ii}] = [G(z), e_{ij}e_{ji}] = [G(z), e_{ij}]e_{ji} + e_{ij}[G(z), e_{ji}]$$

onde $j \neq i$, ou seja, $[G(z), e_{ij}] = [G(z), e_{ji}] = 0$. Portanto, $[G(z), e_{ii}] = 0$. As duas últimas afirmações nos levam à conclusão de que $G(z)$ comuta com qualquer matriz elementar e, por conseguinte, $[G(z), \lambda] = 0$ para qualquer $\lambda \in M_n(\mathbb{K})$, o que conclui o resultado desejado. ■

Caso o corpo base $\mathbb{K}$ contenha elementos suficientes, ou seja, mais elementos que a ordem das matrizes, a descrição das aplicações comutantes sobre o conjunto das matrizes invertíveis pode ser obtida quase que imediatamente. Destacamos isso separadamente, pois a técnica utilizada traz uma prova rápida e simples para o resultado que apresentamos.

Proposição 2.3. *Sejam $n \in \mathbb{N}$ e $\mathbb{K}$ um corpo de cardinalidade $|\mathbb{K}| > n \geq 2$. Considere uma aplicação aditiva $G : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ satisfazendo*

$$G(x)x = xG(x), \ \forall x \in GL_n(\mathbb{K}).$$

Então, existe um elemento $\lambda \in \mathcal{Z}$ e uma aplicação aditiva $\mu : M_n(\mathbb{K}) \to \mathcal{Z}$ tal que

$$G(x) = \lambda x + \mu(x), \ \forall x \in M_n(\mathbb{K}).$$

Demonstração. Considere $x \in M_n(\mathbb{K})$ arbitrária. Se x for uma matriz invertível, é imediato da hipótese que $G(x)x = xG(x)$. Agora, sendo $|\mathbb{K}| > n \geq 2$ e supondo que x seja uma matriz singular, tem-se que existe $z \in \mathcal{Z}$ tal que $z + x$ é uma matriz invertível. Com efeito, considerando $p_x(t)$ o polinômio característico da matriz x, tem-se que

$$p_x(t) = \det(x - tI).$$

Como $p_x(t)$ tem grau n, podem existir, no máximo, n raízes distintas (no caso em que $p_x(t)$ tiver todas as raízes com multiplicidade 1 em $\mathbb{K}$) de $p_x(t)$ em $\mathbb{K}$, isto é, $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tais que $p_x(\lambda_j) = \det(x - \lambda_j I) = 0$, com $1 \leq j \leq n$. Daí, como $|\mathbb{K}| > n$ segue que existe $\lambda \in \mathbb{K}$ tal que $\det(x - \lambda I) \neq 0$. Logo, tomando $z = -\lambda I$, tem-se que $x + z$ é uma matriz invertível.

Deste modo, aplicando a hipótese, veja que

$$\begin{aligned} G(z+x)(z+x) &= (z+x)G(z+x) \\ &\Rightarrow G(z)z+G(z)x+G(x)z+G(x)x = zG(z)+xG(z)+zG(x)+xG(x). \end{aligned}$$

Da Proposição 2.2 tem-se $G(z) \in \mathcal{Z}$, e usando que $z \in \mathcal{Z}$, obtemos que

$$G(x)x = xG(x),$$

quando x é singular. Portanto, o resultado segue pelo Teorema 2.1. ■

Veja que, sob as hipóteses dadas na proposição acima, na argumentação utilizada não precisamos nos preocupar com o fato de x ser uma matriz invertível ou não invertível, pois o fato de que $p_x(t)$ tem grau n, para qualquer matriz $x \in M_n(\mathbb{K})$, e $|\mathbb{K}| > n$, garante a existência de $\lambda \in \mathbb{K}$ tal que $x + \lambda I$ é uma matriz invertível.

Provaremos agora um resultado mais geral, assumindo apenas que $|\mathbb{K}| > 2$.

Observação 2.4. *Antes de prosseguirmos, observemos que, sob a hipótese de p ser um número primo, se $\mathbb{K} = \mathbb{Z}_p$, então uma aplicação aditiva $G : M_n(\mathbb{Z}_p) \to M_n(\mathbb{Z}_p)$ é também linear. Com efeito, dado $n \in \mathbb{Z}_p$ temos que*

$$G(nx) = G(\underbrace{x+\cdots+x}_{(n-vezes)}) = nG(x), \forall\, x \in M_n(\mathbb{K}),\ n \in \mathbb{Z}_p.$$

Teorema 2.5. *Sejam $\mathbb{K}$ um corpo de cardinalidade $|\mathbb{K}| > 2$ e $n > 1$ um número natural. Considere $G : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ uma aplicação aditiva tal que*

$$G(x)x = xG(x),\ \forall x \in GL_n(\mathbb{K}).$$

Então, existe um elemento $\lambda \in \mathcal{Z}$ e uma aplicação aditiva $\mu : M_n(\mathbb{K}) \to \mathcal{Z}$ tal que

$$G(x) = \lambda x + \mu(x),\ \forall x \in M_n(\mathbb{K}).$$

Demonstração. Considere $z \in \mathcal{Z}$, arbitrário fixo. Como $|\mathbb{K}| > 2$, é possível obter $a = a(z) \in \mathbb{K}$, não nulo, tal que $ze_{ij} + aI$ é uma matriz invertível. Na condição em que $i \neq j$ é fácil observar tal afirmação. Na condição em que $|\mathbb{K}| > 3$ não é difícil observar tal afirmação, mesmo para $i = j$, pois $\mathbb{K}$ possui uma boa quantidade de elementos. Agora, se $|\mathbb{K}| = 3$ e $i = j$, então tem-se $\mathbb{K} \simeq \mathbb{Z}_3$ e daí, dado $z \in \{\overline{0}, \overline{1}, \overline{2}\}$, não é difícil obter $a \in \{\overline{1}, \overline{2}\}$ de tal sorte que $a + z \neq \overline{0}$, o que nos permite observar que $ze_{ii} + aI$ é uma matriz invertível, com $i \in \{1, \ldots, n\}$.

Como $aI \in \mathcal{Z}$ tem-se, da Proposição 2.2, que $G(aI) \in \mathcal{Z}$. Com isso, lançando mão da hipótese e da aditividade de G, temos que $G(ze_{ij} + aI)(ze_{ij} + aI) = (ze_{ij} + aI)G(ze_{ij} + aI)$

resulta em:

$$G(ze_{ij})ze_{ij} + G(ze_{ij})aI + G(aI)ze_{ij} + G(aI)aI = ze_{ij}G(ze_{ij}) + aIG(ze_{ij}) + ze_{ij}G(aI) + aIG(aI).$$

Assim, $G(ze_{ij})ze_{ij} = ze_{ij}G(ze_{ij})$ para quaisquer $i, j \in \{1, \ldots, n\}$ e $z \in \mathcal{Z}$, arbitrário fixo.

Agora, considere $i, j \in \{1, \ldots, n\}$ e $z, w \in \mathcal{Z}$ arbitrários. Achamos interessante excluir de nossa análise o caso $n = 2$ por dois motivos: primeiro, ele é obtido de forma alternativa na proposição anterior, e o outro motivo é que pode acontecer alguns problemas na utilização dessa técnica, como veremos no parágrafo posterior. Assim, tomando $n > 2$ e supondo, inicialmente, que $i \neq j$, desde que $|\mathbb{K}| > 2$, existe $a = a(z, w) \in \mathbb{K} \setminus \{0\}$ tal que $(ze_{ij} + we_{kl}) + aI$ é uma matriz invertível, com $k, l \in \{1, \ldots, n\}$. Pode-se fazer uma análise semelhante à anterior para a matriz $we_{kl} + aI$ e observar que esta é uma matriz invertível, para $k, l \in \{1, \ldots, n\}$.

Vamos dedicar um tempo a explicar o motivo da retirada de nossa análise do caso em que $n = 2$. Para este caso, tome $\mathbb{K} \simeq \mathbb{Z}_3$ e observe que a matriz $(ze_{ij} + we_{kl}) + aI$ possui uma das seguintes formas:

$$A = \begin{pmatrix} a+w & z \\ \overline{0} & a \end{pmatrix} \quad \text{ou} \quad B = \begin{pmatrix} a & w \\ z & a \end{pmatrix}.$$

O caso das demais possibilidades de matrizes quadradas de ordem 2 envolvendo $z, w, a \in \mathbb{Z}_3$, com $a \neq \overline{0}$, resume-se a analisar os casos anteriores. Recorde que $a \in \{\overline{1}, \overline{2}\}$. Assim, $a^2 = \overline{1}$. Observe que a escolha de $w = -a$ implica que a matriz A não é invertível, o que nos dá um problema para seguir com a demonstração. No caso da matriz B se z ou w for nulo, então $\det B = a^2 = \overline{1} \neq \overline{0}$ e B é invertível. Logo, suponha w e z não nulos. Deste modo, temos algum problema nos casos $z = w = \overline{1}$ ou $z = w = \overline{2}$. Note que $zw = \overline{1}$ e daí $\det B = a^2 - z^2 = \overline{0}$.

Então, quando $n = 2$, temos que $|\mathbb{K}| > n = 2$ e o resultado segue pela Proposição 2.3. Portanto, devemos apenas considerar $n \geq 3$ e, consequentemente, a matriz $(ze_{ij} + we_{kl}) + aI$ é invertível.

Devido aos comentários anteriores, segue por hipótese que

$$G((ze_{ij} + we_{kl}) + aI)((ze_{ij} + we_{kl}) + aI) = ((ze_{ij} + we_{kl}) + aI)G((ze_{ij} + we_{kl}) + aI).$$

Da aditividade de G, por um lado da igualdade, obtemos

$$G(ze_{ij} + we_{kl})(ze_{ij} + we_{kl}) + G(ze_{ij} + we_{kl})aI + G(aI)(ze_{ij} + we_{kl}) + G(aI)aI.$$

Por outro lado,

$$(ze_{ij} + we_{kl})G(ze_{ij} + we_{kl}) + aIG(ze_{ij} + we_{kl}) + (ze_{ij} + we_{kl})G(aI) + aIG(aI).$$

Agora, do fato de que $[G(ze_{ij}), ze_{ij}] = 0$, $aI \in \mathcal{Z}$ e da Proposição 2.2, resulta

$$G(we_{kl})ze_{ij} + G(ze_{ij})we_{kl} = we_{kl}G(ze_{ij}) + ze_{ij}G(we_{kl}), \tag{2.2}$$

para quaisquer $k, l \in \{1, \ldots, n\}$ e quaisquer $z, w \in \mathcal{Z}$.

Mostraremos que a Equação (2.2) vale quando $i = j$. Sendo $i = j$, quando $k \neq l$ não há nada o que provar, basta observar o que foi feito anteriormente. Logo, suponha que $i = j$ e $k = l$. A princípio, sem perda de generalidade, considere $k \neq i$. Veja que, quando $|\mathbb{K}| \geq 4$, tomando $z, w \in \mathcal{Z}$, existe $a(z,w) \in \mathbb{K}$ não nulo tal que $ze_{ii} + we_{kk} + aI$ é uma matriz invertível. A última observação segue facilmente escolhendo um elemento não nulo a diferente dos opostos aditivos de z e w. Desta forma, seguindo passo a passo o que foi feito no caso em que $i \neq j$, tem-se que vale a Equação (2.2) quando $i = j$, $k = l$, $i \neq k$ e $|\mathbb{K}| \geq 4$.

Sendo assim, vejamos o caso em que $|\mathbb{K}| = 3$, ou seja, $\mathbb{K} \simeq \mathbb{Z}_3$. Inicialmente, observe que $e_{ii} + e_{kk} + I$ é uma matriz invertível. Desta forma, segue que

$$G(e_{ii} + e_{kk} + I)(e_{ii} + e_{kk} + I) = (e_{ii} + e_{kk} + I)G(e_{ii} + e_{kk} + I).$$

Da aditividade de G tem-se

$$\begin{aligned} &G(e_{ii} + e_{kk})(e_{ii} + e_{kk}) + G(e_{ii} + e_{kk})I + G(I)(e_{ii} + e_{kk}) + G(I)I = \\ &(e_{ii} + e_{kk})G(e_{ii} + e_{kk}) + IG(e_{ii} + e_{kk}) + (e_{ii} + e_{kk})G(I) + IG(I). \end{aligned}$$

Da Proposição 2.2, concluímos que $G(e_{ii} + e_{kk})(e_{ii} + e_{kk}) = (e_{ii} + e_{kk})G(e_{ii} + e_{kk})$. Por conseguinte,

$$G(e_{ii})e_{kk} + G(e_{kk})e_{ii} = e_{ii}G(e_{kk}) + e_{kk}G(e_{ii}).$$

Sabendo que $z \in \mathcal{Z} \simeq \mathbb{K} \simeq \mathbb{Z}_3$ segue que $G(zx) = zG(x)$, para quaisquer $x \in M_n(\mathbb{K})$ e $z \in \mathcal{Z}$. Sendo assim, multiplicando ambos os lados da equação acima por zw, com $z, w \in \mathcal{Z}$, segue que

$$\begin{aligned} zw[G(e_{ii})e_{kk} + G(e_{kk})e_{ii}] &= zw[e_{ii}G(e_{kk}) + e_{kk}G(e_{ii})] \\ &\Rightarrow zwG(e_{ii})e_{kk} + zwG(e_{kk})e_{ii} = zwe_{ii}G(e_{kk}) + zwe_{kk}G(e_{ii}) \\ &\Rightarrow zG(e_{ii})we_{kk} + wG(e_{kk})ze_{ii} = ze_{ii}wG(e_{kk}) + we_{kk}zG(e_{ii}) \\ &\Rightarrow G(ze_{ii})we_{kk} + G(we_{kk})ze_{ii} = ze_{ii}G(we_{kk}) + we_{kk}G(ze_{ii}). \end{aligned}$$

Assim,

$$G(we_{kl})ze_{ij} + G(ze_{ij})we_{kl} = we_{kl}G(ze_{ij}) + ze_{ij}G(we_{kl})$$

é válida para quaisquer $i, j, k, l \in \{1, \ldots, n\}$. Portanto, da aditividade de G e do fato de $M_n(\mathbb{K})$ ser aditivamente gerada como espaço vetorial pelas matrizes elementares e_{ij}, concluímos que $G(x)x = xG(x)$, para todo $x \in M_n(\mathbb{K})$. Portanto, do Corolário 1.63, tem-se o resultado. ■

O próximo exemplo mostra a importância da exigência, no Teorema 2.5 e na Proposição 2.2, do corpo $\mathbb{K}$ ter pelo menos três elementos. Vejamos:

Exemplo 2.6. *Seja $\mathbb{K} = \mathbb{Z}_2$ e considere $M_2(\mathbb{K})$. Desta forma, o conjunto de matrizes invertíveis de $M_2(\mathbb{K})$ é composto pelos seguintes elementos:*

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \; e \; A_6 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Não é difícil ver que $\{A_1, A_2, A_3, A_5\}$ é uma base para o $\mathbb{K}$-espaço vetorial $M_2(\mathbb{K})$. Deste modo, pelo Teorema Fundamental da Álgebra Linear, existe uma única transformação linear $G : M_2(\mathbb{K}) \to M_2(\mathbb{K})$ dada por $G(A_1) = G(A_5) = A_5$ e $G(A_2) = G(A_3) = 0_2$. Nestas condições, G é uma aplicação aditiva e tem-se que

$$G(A_4) = G(A_2 + A_3) = G(A_2) + G(A_3) = 0_2 \text{ e } G(A_6) = G(A_1 + A_5) = G(A_1) + G(A_5) = 0_2.$$

Não é difícil ver que $[G(A_1), A_1]$, $[G(A_2), A_2]$, $[G(A_3), A_3]$, $[G(A_4), A_4]$, $[G(A_5), A_5]$ e $[G(A_6), A_6]$ são todos nulos, isto é, G é uma aplicação comutante nos invertíveis de $M_2(\mathbb{K})$. Entretanto, $G(A_1)$ não é um elemento do centro $\mathcal{Z}$ de $M_2(\mathbb{K})$ e, por maior razão, G não assume a forma $G(x) = \lambda x + \mu(x)$ para todo $x \in M_2(\mathbb{K})$.

Concluamos este capítulo com um corolário fácil, apenas para ilustrar como o Teorema 2.5 pode ser aplicado a algumas questões de Álgebra Linear.

Corolário 2.7. *Seja $\mathbb{K}$ um corpo de cardinalidade $|\mathbb{K}| > 2$ e $n > 1$. Considere uma aplicação aditiva $G : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ tal que para todo automorfismo interno $\varphi : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ as aplicações G e φ comutam, isto é, $G(\varphi(x)) = \varphi(G(x))$ para todo $x \in M_n(\mathbb{K})$. Então, existe um elemento $\lambda \in \mathcal{Z}$ e uma aplicação aditiva $\mu : M_n(\mathbb{K}) \to \mathcal{Z}$ tal que*

$$G(x) = \lambda x + \mu(x), \; \forall x \in M_n(\mathbb{K}).$$

Demonstração. Dado $\varphi : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ um automorfismo interno, existe $y \in GL_n(\mathbb{K})$, tal que $\varphi(x) = y^{-1}xy$, para todo $x \in M_n(\mathbb{K})$. Denotemos φ por φ_y com $y \in M_n(\mathbb{K})$. Desta forma, para todo $y \in GL_n(\mathbb{K})$, segue por hipótese que

$$G(y^{-1}xy) = G(\varphi_y(x)) = \varphi_y(G(x)) = y^{-1}G(x)y$$

para todo $x \in M_n(\mathbb{K})$. Logo, considerando $x = y$ segue que $G(y) = G(y^{-1}yy) = y^{-1}G(y)y$ e daí $yG(y) = G(y)y$, para todo $y \in M_n(\mathbb{K})$ invertível.

O resultado segue do Teorema 2.5, uma vez que G é uma aplicação aditiva comutante sobre o conjunto de matrizes invertíveis de $M_n(\mathbb{K})$. ∎

CAPÍTULO 3

Traços Comutantes de Aplicações m-aditivas em Matrizes Especiais

O capítulo anterior descreve a obtenção completa de aplicações aditivas comutantes sobre a álgebra de matrizes $M_n(\mathbb{K})$, considerando apenas seus elementos invertíveis ou singulares. Um resultado geral relacionado pode ser encontrado nos trabalhos de Brešar [1]. Seguindo essa linha de raciocínio, podemos também considerar aplicações multiaditivas. Em particular, destacamos as aplicações traços, que consistem em uma aplicação sobre algum anel A definida por $q\colon A \to A$ tal que $q(x) = \mathcal{B}(x,x)$, para $x \in A$, onde $\mathcal{B}\colon A \times A \to A$ é uma aplicação bilinear. A descrição completa dessa última aplicação foi obtida por Brešar em [2].

Naturalmente, um questionamento factível é o de como obter o último resultado citado de Brešar nas condições do capítulo anterior, ou seja, considerando aplicações traços sobre matrizes invertíveis ou singulares. Também, seguindo a ideia anterior, podemos generalizar a noção de traço para aplicações multiaditivas. Neste capítulo, apresentaremos os resultados obtidos por França em [9].

3.1 Aplicações Multiaditivas

Nesta seção, consideraremos algumas noções iniciais e resultados preliminares que serão importantes para o desenvolvimento deste capítulo. Faremos uma generalização dos conceitos de aplicações aditivas e aplicações comutantes vistos na Seção 1.3 para aplicações multiaditivas, as quais trabalharemos sob a condição de serem também comutantes.

Inicialmente, sejam A um anel e B um subgrupo aditivo de A. Recordemos que uma aplicação f de A em B é chamada de **comutante em** B se $[f(x),x]=0$, para todo $x\in B$. Aqui, $[x,y]$ denota o comutador $xy-yx$, para todo $x,y\in B$.

Definição 3.1. *Sejam A um anel e m um inteiro positivo. Uma aplicação $G:A^m\to A$ é dita m-aditiva se G é uma aplicação aditiva em cada uma de suas componentes, ou seja, se para $a_1,\dots,a_i,x_i,y_i,a_{i+1},\dots,a_m\in A$, vale*

$$G(a_1,\dots,x_i+y_i,\dots,a_m)=G(a_1,\dots,x_i,\dots,a_m)+G(a_1,\dots,y_i,\dots,a_m),$$

para $1\leq i\leq m$.

Exemplo 3.2. *Sendo A um anel, considere $g:A^m\to A$ dada por $g(a_1,\dots,a_m)=a_1a_2\cdots a_m$. Não é difícil ver que g é uma aplicação m-aditiva.*

Exemplo 3.3. *Seja A um anel. Considere a aplicação $f:A^2\to A$ dada por $f(a,b)=[a,b]$, para $a,b\in A$. Temos que f é uma aplicação biaditiva. De fato, veja que*

$$f(x+y,b)=[x+y,b]=(x+y)b-b(x+y)=xb-bx+yb-by=[x,b]+[y,b]=f(x,b)+f(y,b).$$

De forma análoga, tem-se $f(a,x+y)=f(a,x)+f(a,y)$.

Exemplo 3.4. *Considere a aplicação biaditiva f dada no exemplo anterior. Defina $G_f:A^3\to A$ dada por $G_f(a,b,c)=[f(a,b),c]$, com $a,b,c\in A$. Temos que G_f é uma aplicação triaditiva. Com efeito, observe que*

$$\begin{aligned}G_f(x+y,b,c)=[f(x+y,b),c]&=[f(x,b)+f(y,b),c]\\&=[f(x,b),c]+[f(y,b),c]=G_f(x,b,c)+G_f(y,b,c),\end{aligned}$$

para quaisquer $x,y,b,c\in A$. De maneira análoga, ver-se que

$$G_f(a,x+y,c)=G_f(a,x,c)+G_f(a,y,c)\quad e\quad G_f(a,b,x+y)=G_f(a,b,x)+G_f(a,b,y).$$

Observação 3.5. *Esta ideia pode ser utilizada para qualquer aplicação f biaditiva e, ainda mais, ela pode ser generalizada para aplicações multiaditivas. Por exemplo, podemos considerar $G_g:A^{m+1}\to A$ dada por $G_g(a_1,\dots,a_m,b)=[a_1a_2\cdots a_m,b]$. Temos que G_g é uma aplicação $(m+1)$-aditiva. Desse modo, dada f uma aplicação m-aditiva podemos associar a ela a aplicação G_f $(m+1)$-aditiva dada por $G_f(a_1,\dots,a_m,a_{m+1})=[f(a_1,\dots,a_m),a_{m+1}]$.*

Exemplo 3.6. *Seja $a\in M_n(\mathbb{K})$. Tome $f\colon M_n(\mathbb{K})^2\to M_n(\mathbb{K})$ dada por $f(x,y)=ax+tr(y)I$, onde I denota a matriz identidade. Temos que f é uma aplicação aditiva quando consideremos $x=y$, porém ela não é biaditiva.*

Um caso particular a ser considerado é quando todas as entradas de uma aplicação m-aditiva G são iguais. Isso nos motiva a fazer a seguinte definição.

Definição 3.7. *Seja $G : A^m \to A$ uma aplicação m-aditiva. A aplicação $T : A \to A$ definida por $T(x) = G(x,\ldots,x)$ é chamada de **traço de** G.*

Observação 3.8. *Voltando ao Exemplo 3.4, no caso considerado lá temos que a aplicação traço de G_f, dada por $T(x) = G_f(x,x,x)$, é nula, haja visto que $f(x,x) = [x,x] = 0$. No entanto, a depender da aplicação f adotada, podemos ter que o traço seja não nulo. Com efeito, considere $a \in M_n(\mathbb{K})$ uma matriz não central e considere f dada por $f(x) = ax + tr(x)I$. Observe que o traço de G_f é dado por $G_f(x,x) = [f(x),x] = [ax+tr(x)I,x]$ e isso é suficiente para observar que não é nulo (Veja a conta abaixo).*

Adicionando a definição de traço com a hipótese de que ele seja uma aplicação comutante em um subgrupo aditivo B de A, temos

$$G(x,\ldots,x)x = T(x)x = xT(x) = xG(x,\ldots,x),$$

para cada $x \in B$. Em outras palavras, T é comutante em um subgrupo aditivo B de A se $[T(x),x] = 0$, para todo $x \in B$. Em particular, considerando $m = 1$ e $B = A$, temos $T \equiv G$. Notemos que nem toda aplicação traço é comutante. Para se convencer dessa última afirmação, considere a função f dada por $f(x) = ax + tr(x)I$ nas condições da Observação 3.8. Neste exemplo, f é aditiva e T é igual a f. Daí,

$$G_f(x,x) = [T(x),x] = [ax+tr(x)I,x] = ax^2 - xax,$$

o qual não é uma aplicação nula, uma vez que

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{e} \quad x = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

tem-se $ax^2 \neq xax$.

Agora, falaremos de aplicações simétricas, que são aplicações que satisfazem certas condições de simetria. Por exemplo, uma aplicação biaditiva $\mathcal{B}$ satisfazendo $\mathcal{B}(x_1,x_2) = \mathcal{B}(x_2,x_1)$ é dita simétrica. Imediatamente, podemos considerar uma definição mais geral.

Definição 3.9. *Seja $G : A^m \to A$ uma aplicação m-aditiva. Dizemos que G é uma aplicação simétrica se vale*

$$G(x_1,\ldots,x_m) = G(x_{\sigma(1)},\ldots,x_{\sigma(m)}),$$

para toda permutação $\sigma \in S_m$.

Um exemplo simples de aplicação multiaditiva comutante e simétrica é o seguinte: sendo S um subgrupo aditivo de um anel A cujos elementos são comutativos, a aplicação $G \colon S^m \to A$, dada por

$$G(s_1, \ldots, s_m) = s_1 \cdots s_m$$

é um exemplo de tal aplicação. Trabalharemos com aplicações aditivas e simétricas na redação subsequente.

Os dois teoremas abaixo são importantes para o desenvolvimento do estudo que será feito neste capítulo, sendo utilizados nas demonstrações dos resultados que serão abordados. Entretanto, advertimos o leitor que não traremos as demonstrações destes dois teoremas, pois fogem ao nosso principal objetivo.

Teorema 3.10. *Seja A um anel primo. Considere $G : A^m \to A$ uma aplicação m-aditiva comutante em A e assuma que char $A = 0$ ou que char $A > m$, e que A não é algébrico de grau menor do que ou igual a m sobre seu centroide estendido $\mathcal{C}$. Então, existe $\mu_0 \in \mathcal{C}$ e $\mu_i : A \to \mathcal{C}$, com $i \in \{1, \ldots, m\}$, onde μ_i é o traço de uma aplicação i-aditiva e*

$$G(a, \ldots, a) = \mu_0 a^m + \mu_1(a)a^{m-1} + \cdots + \mu_{m-1}(a)a + \mu_m(a),$$

para todo $a \in A$.

Demonstração. Vide [18, Theorem 3.1]. ■

Teorema 3.11. *Sejam A e B álgebras primas centralmente fechadas sobre um corpo $\mathbb{K}$, com char $\mathbb{K} \neq 2, 3$, e suponha que nenhuma delas satisfaz St_4 (polinômio Standard). Seja $\theta : A \to B$ uma aplicação linear e bijetora satisfazendo $[\theta(x^2), \theta(x)] = 0$ para todo $x \in A$. Então, temos $\theta(x) = \lambda\phi(x) + \mu(x)1_B$, em que $\lambda \in \mathbb{K}$ é não nulo, μ é um funcional linear e ϕ, ou é um isomorfismo é um anti-isomorfismo de A em B.*

Demonstração. Vide [2, pág. 534] ■

3.2 Aplicação Traço Comutante em Matrizes Invertíveis

Seja G uma aplicação m-aditiva sobre um anel A. Observamos que a aplicação definida por

$$G'(x_1, \ldots, x_m) = \sum_{\sigma \in S_m} G(x_{\sigma(1)}, \ldots, x_{\sigma(m)})$$

é simétrica sobre A. Além disso, notavelmente temos

$$G'(x, \ldots, x) = \sum_{\sigma \in S_m} G(x, \ldots, x) = m! G(x, \ldots, x),$$

para todo $x \in A$. Assuma que A seja uma álgebra sobre um corpo $\mathbb{K}$, com *char* $\mathbb{K} = 0$ ou *char* $\mathbb{K} \geq m+1$. Assim, segue que $[G'(x, \ldots, x), x] = 0$ é equivalente a $[G(x, \ldots, x), x] = 0$. Isso nos diz que sob certas condições no corpo base podemos considerar, sem perda de generalidade, que G é uma aplicação simétrica.

No que segue, tomaremos $A = M_n(\mathbb{K})$ e podemos assumir sem perda de generalidade que G é simétrica. Além disso, não é difícil ver que G é também m-linear (linear em cada entrada) sobre o corpo $\mathbb{Q}$, quando *char* $\mathbb{K} = 0$ ou, sobre $\mathbb{Z}_p$, quando *char* $\mathbb{K} = p > 0$. Este fato será utilizado na demonstração dos resultados principais deste capítulo. Inicialmente, vamos verificar o resultado que envolve traços comutantes de aplicações m-aditivas em conjuntos de matrizes invertíveis. Antes, precisamos de um resultado auxiliar. Sendo assim, vamos ao resultado.

Proposição 3.12. *Sejam $\mathbb{K}$ um corpo e $n > m > 1$ naturais fixados. Seja $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ uma aplicação m-aditiva simétrica tal que*

$$[G(x,x,\ldots,x),x] = 0,\ \forall x \in GL_n(\mathbb{K}).$$

Considere char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$, e que $|\mathbb{K}| \geq m+3$. Então, $G(z,\ldots,z) \in \mathcal{Z}$, para todo $z \in \mathcal{Z}$. Aqui $\mathcal{Z}$ denota o centro $\mathbb{K} \cdot I_n$ de $M_n(\mathbb{K})$, onde I_n é a matriz identidade de ordem n.

Demonstração. Seja s o menor número par tal que $s \geq m$, isto é, ou $s = m$, se m é par, ou $s = m+1$, se m é ímpar. Agora, fixemos $z \in \mathcal{Z}$ e uma matriz elementar e_{ij}, com $i \neq j$. Considere $u = k(I_n + e_{ij})$, com $k \in \mathcal{Z}$. Defina, para cada $a \in \left\{\pm 1, \ldots, \pm \frac{s}{2}\right\}$, o elemento $y_a = az + u$. Observe que y_a é invertível se, e somente se, $az + k \neq 0_n$, ou seja, se $-az \neq k$. Como $|\mathbb{K}| \geq m+3$, podemos encontrar um $k \in \mathcal{Z} \setminus \{0_n\}$ tal que y_a é invertível para cada $a \in \left\{\pm 1, \ldots, \pm \frac{s}{2}\right\}$. Com efeito, observe que

$$y_a = az + u = az + k(I_n + e_{ij}) = (az + kI_n) + ke_{ij}.$$

Observemos que para cada $z \in \mathcal{Z}$, não nulo, tem-se que o conjunto $\{-az \mid a \in \left\{\pm 1, \ldots, \pm \frac{s}{2}\right\}\}$ tem cardinalidade igual a s. Notemos que $|K \setminus \{0\}| \geq m+2$, o que nos rende que $(az + kI_n)$ é uma matriz diagonal cujo produto de seus elementos diagonais é não nulo, ou seja, $(az + kI_n)$ é invertível para alguma escolha de k. Da última informação, se $|\mathbb{K}| > m+2$, então existe um $k \in \mathcal{Z}$ tal que y_a é invertível para cada $a \in \left\{\pm 1, \ldots, \pm \frac{s}{2}\right\}$.

Ademais, sabe-se que $z \in \mathcal{Z} \setminus \{0_n\}$ é invertível. Considerando $k \in \mathcal{Z}$, não nulo, nas condições acima, obtemos que u é também invertível e, consequentemente, a matriz y_a é invertível, para todo $a \in \left\{\pm 1, \ldots, \pm \frac{s}{2}\right\}$. Por G ser comutante sobre o grupo das matrizes invertíveis $GL_n(\mathbb{K})$, segue que

$$0 = [G(u,u,\ldots,u),u] = [G(z,z,\ldots,z),z] = [G(y_a,y_a,\ldots,y_a),y_a].$$

Sendo $y_a = az + u$ e $z \in \mathcal{Z}$, tem-se que $0 = [G(y_a,y_a,\ldots,y_a),y_a] = [G(y_a,y_a,\ldots,y_a),u]$. Em particular, tomando $a \in \left\{1, \ldots, \frac{s}{2}\right\}$, tem-se que $[G(y_a,y_a,\ldots,y_a) + G(y_{-a},y_{-a},\ldots,y_{-a}),u] = 0$.

Agora, por G ser uma aplicação m-aditiva simétrica e $y_a = az + u$, tem-se

$$G(y_a,\dots,y_a) = \sum_{\zeta=0}^{m} a^{m-\zeta}\binom{m}{\zeta} G(z,\dots,z,\underbrace{u,\dots,u}_{\zeta})$$

e

$$G(y_{-a},\dots,y_{-a}) = \sum_{\zeta=0}^{m} (-1)^{m-\zeta} a^{m-\zeta}\binom{m}{\zeta} G(z,\dots,z,\underbrace{u,\dots,u}_{\zeta}),$$ [1]

para cada $a \in \{1,\dots,\frac{s}{2}\}$. Expandindo as igualdades anteriores, obtém-se

$$\begin{aligned}
G(y_a,\dots,y_a) &= \sum_{\zeta=0}^{m} a^{m-\zeta}\binom{m}{\zeta} G(z,\dots,z,\underbrace{u,\dots,u}_{\zeta}) \\
&= a^m\binom{m}{0}G(z,\dots,z) + a^{m-1}\binom{m}{1}G(z,\dots,z,u) + a^{m-2}\binom{m}{2}G(z,\dots,z,u,u) + \\
&\quad + \cdots + a^2\binom{m}{m-2}G(z,z,u,\dots,u) + a\binom{m}{m-1}G(z,u,\dots,u) + \\
&\quad + \binom{m}{m}G(u,\dots,u)
\end{aligned}$$

e

$$\begin{aligned}
G(y_{-a},\dots,y_{-a}) &= \sum_{\zeta=0}^{m} (-1)^{m-\zeta} a^{m-\zeta}\binom{m}{\zeta} G(z,\dots,z,\underbrace{u,\dots,u}_{\zeta}) \\
&= (-1)^m a^m\binom{m}{0}G(z,\dots,z) + (-1)^{m-1}a^{m-1}\binom{m}{1}G(z,\dots,z,u) + \\
&\quad + (-1)^{m-2}a^{m-2}\binom{m}{2}G(z,\dots,z,u,u) + \cdots + \\
&\quad (-1)^2a^2\binom{m}{m-2}G(z,z,u,\dots,u) \\
&\quad - a\binom{m}{m-1}G(z,u,\dots,u) + \binom{m}{m}G(u,\dots,u).
\end{aligned}$$

Dessa forma, o somatório

$$G(y_a,y_a,\dots,y_a) + G(y_{-a},y_{-a},\dots,y_{-a}) = *$$

resume-se em

$$* = 2\left[\sum_{\zeta=0}^{\frac{s-2}{2}} (-1)^{m-2\zeta}a^{m-2\zeta}\binom{m}{2\zeta}G(z,\dots,z,\underbrace{u,\dots,u}_{2\zeta})\right]$$

[1] Ao leitor interessado, verificamos ambas as igualdades nas Proposições A.1 e A.2 do Apêndice A.

quando m é par, e

$$* = 2\left[\sum_{\zeta=0}^{\frac{s-4}{2}} (-1)^{m-(2\zeta+1)} a^{m-(2\zeta+1)} \binom{m}{2\zeta+1} G(z,\ldots,z,\underbrace{u,\ldots,u}_{2\zeta+1})\right],$$

quando m é ímpar.

Recorde que, sendo $[G(u,\ldots,u),u] = 0$, independente de m ser par ou ímpar, vale

$$\left[2\binom{m}{m} G(u,\ldots,u),u\right] = 2\binom{m}{m}[G(u,\ldots,u),u] = 0,$$

e daí

$$\binom{m}{m}[G(u,\ldots,u),u] = 0,$$

pois *char* $\mathbb{K} > 2$. Deste modo, para m par, segue que $s = m$ e obtemos

$$0 = [G(y_a,y_a,\ldots,y_a) + G(y_{-a},y_{-a},\ldots,y_{-a}),u] = 2\left[\sum_{\zeta=0}^{\frac{s-2}{2}} a^{m-2\zeta}\binom{m}{2\zeta}[G(z,\ldots,z,\underbrace{u,\ldots,u}_{2\zeta}),u]\right],$$

ou seja,

$$\sum_{\zeta=0}^{\frac{s-2}{2}} a^{m-2\zeta}\binom{m}{2\zeta}[G(z,\ldots,z,\underbrace{u,\ldots,u}_{2\zeta}),u] = 0.$$

Para m ímpar, segue que $s = m+1$ e obtemos que

$$\begin{aligned} 0 &= [G(y_a,y_a,\ldots,y_a) + G(y_{-a},y_{-a},\ldots,y_{-a}),u] \\ &= 2\left[\sum_{\zeta=0}^{\frac{s-4}{2}} a^{m-(2\zeta+1)}\binom{m}{2\zeta+1}[G(z,\ldots,z,\underbrace{u,\ldots,u}_{2\zeta+1}),u]\right], \end{aligned}$$

ou seja,

$$\sum_{\zeta=0}^{\frac{s-4}{2}} a^{m-(2\zeta+1)}\binom{m}{2\zeta+1}[G(z,\ldots,z,\underbrace{u,\ldots,u}_{2\zeta+1}),u] = 0. \tag{3.1}$$

Observe que para este último caso, quando m é ímpar, pode-se utilizar as identidades

$$[G(y_a,y_a,\ldots,y_a),u] = 0 \quad \text{e} \quad [G(u,\ldots,u),u] = 0$$

para se obter

$$
\begin{aligned}
0=[G(y_a,y_a,\dots,y_a),u] &= \sum_{\zeta=0}^{m} a^{m-\zeta}\binom{m}{\zeta}[G(z,\dots,z,\underbrace{u,\dots,u}_{\zeta}),u]\\
&= \sum_{\zeta=0}^{\frac{s-4}{2}} a^{m-(2\zeta+1)}\binom{m}{2\zeta+1}[G(z,\dots,z,\underbrace{u,\dots,u}_{2\zeta+1}),u]\\
&+ \sum_{\zeta=0}^{\frac{s-2}{2}} a^{m-2\zeta}\binom{m}{2\zeta}[G(z,\dots,z,\underbrace{u,\dots,u}_{2\zeta}),u].
\end{aligned}
$$

A igualdade (3.1) implica

$$
\sum_{\zeta=0}^{\frac{s-2}{2}} a^{m-2\zeta}\binom{m}{2\zeta}[G(z,\dots,z,\underbrace{u,\dots,u}_{2\zeta}),u]=0. \tag{3.2}
$$

Por conseguinte, para cada $a\in\{1,\dots,\frac{s}{2}\}$, obtemos uma equação da forma (3.2). Essa informação independe se m é par ou ímpar. Desta forma, temos um sistema de equações com $\frac{s}{2}$ equações e $\frac{s}{2}$ incógnitas. Explicitamente

$$
\binom{m}{2\zeta}[G(z,\dots,z,\underbrace{u,\dots,u}_{2\zeta}),u]
$$

onde u aparece exatamente 2ζ nas componentes de G, com $\zeta\in\left\{0,1,2,\dots,\frac{s-2}{2}\right\}$. Então, para cada $a\in\left\{1,\dots,\frac{s}{2}\right\}$, podemos reescrever o sistema de equações na forma matricial:

$$
\begin{pmatrix}
1 & 1 & 1 & \cdots & 1\\
2^m & 2^{m-2} & 2^{m-4} & \cdots & 2^{m-(s-2)}\\
3^m & 3^{m-2} & 3^{m-4} & \cdots & 3^{m-(s-2)}\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
\left(\frac{s}{2}\right)^m & \left(\frac{s}{2}\right)^{m-2} & \left(\frac{s}{2}\right)^{m-4} & \cdots & \left(\frac{s}{2}\right)^{m-(s-2)}
\end{pmatrix}
\begin{pmatrix}
\binom{m}{0}[G(z,\dots,z),u]\\
\vdots\\
\binom{m}{2\zeta}[G(z,\dots,z,u,\dots,u),u]\\
\vdots\\
\binom{m}{s-2}[G(z,u,\dots,u),u]
\end{pmatrix}
=
\begin{pmatrix}
0\\ \vdots\\ 0\\ \vdots\\ 0
\end{pmatrix}.
$$

Agora, observe que

$$
\det\begin{pmatrix}
1 & 1 & 1 & \cdots & 1\\
2^m & 2^{m-2} & 2^{m-4} & \cdots & 2^{m-(s-2)}\\
3^m & 3^{m-2} & 3^{m-4} & \cdots & 3^{m-(s-2)}\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
\left(\frac{s}{2}\right)^m & \left(\frac{s}{2}\right)^{m-2} & \left(\frac{s}{2}\right)^{m-4} & \cdots & \left(\frac{s}{2}\right)^{m-(s-2)}
\end{pmatrix}
$$

é igual a

$$\prod_{i=1}^{\frac{s}{2}} i^{-m} \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & (2^{-2})^1 & (2^{-2})^2 & \cdots & (2^{-2})^{\frac{s-2}{2}} \\ 1 & (3^{-2})^1 & (3^{-2})^2 & \cdots & (3^{-2})^{\frac{s-2}{2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \left(\left(\frac{s}{2}\right)^{-2}\right)^1 & \left(\left(\frac{s}{2}\right)^{-2}\right)^2 & \cdots & \left(\left(\frac{s}{2}\right)^{-2}\right)^{\frac{s-2}{2}} \end{pmatrix} \neq 0,$$

pois

$$\prod_{i=1}^{\frac{s}{2}} i^{-m} \neq 0$$

uma vez que $char\ \mathbb{K} = 0$ ou $char\ \mathbb{K} > m+1$, e a matriz a direita é uma matriz de Vandermonde, cujo determinante é não nulo[2]. Assim, concluímos que o sistema tem solução trivial, isto é, o sistema que se encontra em (3.2) resultará em

$$[G(z,\ldots,z,\underbrace{u,\ldots,u}_{2\zeta}),u] = 0$$

para qualquer $\zeta \in \left\{0,1,2,\ldots,\frac{s-2}{2}\right\}$. Em particular, $[G(z,\ldots,z),u] = 0$, para $\zeta = 0$.

Sendo $u = k(I+e_{ij})$, com $k \in \mathbb{K}$ um elemento não nulo do corpo, vejamos que

$$\begin{aligned} 0 = [G(z,\ldots,z),u] = [G(z,\ldots,z),k(I+e_{ij})] &= k[G(z,\ldots,z),I+e_{ij}] \\ &= k([G(z,\ldots,z),I]+[G(z,\ldots,z),e_{ij}]). \end{aligned}$$

Como $[G(z,\ldots,z),I] = 0$, segue-se que $[G(z,\ldots,z),e_{ij}] = 0$ para $i \neq j$.

Por fim, observe que

$$[G(z,\ldots,z),e_{ii}] = [G(z,\ldots,z),e_{ij}e_{ji}] = [G(z,\ldots,z),e_{ij}]e_{ji} + e_{ij}[G(z,\ldots,z),e_{ji}] = 0,$$

com $i \neq j$.

Deste modo, $\left[G(z,\ldots,z),e_{ij}\right] = 0$, para quaisquer $i,j \in \{1,\ldots,n\}$. Desta forma, tomando arbitrariamente $x \in M_n(\mathbb{K})$, temos $x = \sum x_{ij}e_{ij}$, com $x_{ij} \in \mathbb{K}$. Assim,

$$\begin{aligned} [G(z,\ldots,z),x] = \left[G(z,\ldots,z), \sum_{1\leq i,j\leq n} x_{ij}e_{ij}\right] &= \sum_{1\leq i,j\leq n} \left[G(z,\ldots,z),x_{ij}e_{ij}\right] \\ &= \sum_{1\leq i,j\leq n} x_{ij}\left[G(z,\ldots,z),e_{ij}\right] = 0. \end{aligned}$$

Portanto, pela arbitrariedade de $z \in \mathcal{Z}$, segue que $G(z,\ldots,z) \in \mathcal{Z}$ para todo $z \in \mathcal{Z}$. ■

[2] Vide a Seção A.3 do Apêndice.

Observação 3.13. *As hipóteses sobre o corpo no resultado anterior não podem ser relaxadas. Para verificar isso, basta relembrar o Exemplo 2.6.*

Agora estamos preparados para enunciar e provar o primeiro resultado principal deste capítulo, que descreverá as aplicações traço de aplicações m-aditivas sobre matrizes de ordem n, sob certas condições no corpo base.

Teorema 3.14. *Sejam $\mathbb{K}$ um corpo e n e m inteiros satisfazendo $n > m > 1$. Tome uma aplicação m-aditiva $G\colon M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ tal que*

$$[G(x,x,\ldots,x),x] = 0, \ \forall x \in GL_n(\mathbb{K}).$$

Além disso, assuma que char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$, e que $|\mathbb{K}| \geq m^2+2m+3$. Então, existem $\mu_0 \in \mathcal{Z}$ e $\mu_i : M_n(\mathbb{K}) \to \mathcal{Z}$ tais que cada μ_i é o traço de uma aplicação i-aditiva para $i \in \{1,\ldots,m\}$ e

$$G(x,\ldots,x) = \mu_0 x^m + \mu_1(x)x^{m-1} + \cdots + \mu_{m-1}(x)x + \mu_m(x), \ \forall x \in M_n(\mathbb{K}).$$

Demonstração. Considere, mais uma vez, s o menor número par tal que $s \geq m$. Logo, $s = m$ se m é par, ou $s = m+1$ se m é ímpar. Para cada $r \in \{1,\ldots,m+1\}$, tome $z_r \in \mathbb{K}$ e $e_{i_r j_r} \in M_n(\mathbb{K})$, com $i_r, j_r \in \{1,\ldots,n\}$, e defina a matriz $b = \sum_{r=1}^{m+1} z_r e_{i_r j_r}$.

Para aprimorar a apresentação dos resultados, decidimos dividi-los em algumas afirmações.

Afirmação 1. Existe $k \in \mathbb{K}\setminus\{0\}$ tal que $y_a = akI + b = akI + \sum_{r=1}^{m+1} z_r e_{i_r j_r}$ é invertível, para todo $a \in \left\{\pm 1, \pm 2, \ldots, \pm \frac{s}{2}\right\}$.

Com efeito, seja $\mathcal{A}(b)$ o conjunto de todos os autovalores não nulos da matriz b. Suponha, por contradição, que para cada $k \in \mathbb{K}\setminus\{0\}$ exista $a_k \in \left\{\pm 1, \pm 2, \ldots, \pm \frac{s}{2}\right\}$ tal que $-a_k k \in \mathcal{A}(b)$. Defina a seguinte aplicação:

$$\begin{aligned} \varphi : \{-a_k k \mid k \in \mathbb{K}\setminus\{0\}\} \times \left\{\pm 1, \pm 2, \ldots, \pm \frac{s}{2}\right\} &\to \mathbb{K}\setminus\{0\} \\ (x,y) &\mapsto y^{-1}x. \end{aligned}$$

Inicialmente, veja que podemos tomar y^{-1}, pois *char* $\mathbb{K} = 0$ ou *char* $\mathbb{K} \geq m+1$. Além disso, não é difícil ver que φ é sobrejetora, pois tomando $-a_k = y_0$, teríamos $y_0^{-1}x = y_0^{-1}(-a_k k) = k$, para todo $k \in \mathbb{K}\setminus\{0\}$. Sendo assim,

$$|\mathbb{K}\setminus\{0\}| \leq |\{-a_k k \mid k \in \mathbb{K}\setminus\{0\}\} \times \left\{\pm 1, \pm 2, \ldots, \pm \frac{s}{2}\right\}|$$

implica que

$$|\mathbb{K}\setminus\{0\}| \leq |\{-a_k k \mid k \in \mathbb{K}\setminus\{0\}\}| \cdot s,$$

e daí, $\frac{|\mathbb{K}\setminus\{0\}|}{s} \leq |\{-a_k k \mid k \in \mathbb{K}\setminus\{0\}\}|$. Agora note que $|\{-a_k k \mid k \in \mathbb{K}\setminus\{0\}\}| \leq |\mathcal{A}(b)|$, pois o conjunto da esquerda é um conjunto de autovalores não nulos de b e, consequentemente, estará contido em $\mathcal{A}(b)$. Desta forma, tem-se

$$\frac{m^2+2m+2}{m+1} \leq \frac{|\mathbb{K}\setminus\{0\}|}{s} \leq |\{-a_k k \mid k \in \mathbb{K}\setminus\{0\}\}| \leq |\mathcal{A}(b)|.$$

Por outro lado, por b ser uma soma de $m+1$ matrizes, tem-se $|\mathcal{A}(b)| < rank(b)+1 \leq m+2$ (em que $rank(b)$ denota o posto da matriz b), isto é, $|\mathcal{A}(b)| \leq m+1$. Entretanto, teríamos que

$$m^2+2m+2 \leq (m+1)^2$$

o que é uma contradição. Logo, segue a Afirmação 1.
Afirmação 2. Para cada $A \subset \{1,\ldots,m+1\}$, vale a identidade

$$\left[G\left(\sum_{r\in A} z_r e_{i_r j_r},\ldots,\sum_{r\in A} z_r e_{i_r j_r}\right),\sum_{r\in A} z_r e_{i_r j_r}\right] = 0.$$

De fato, da afirmação anterior podemos encontrar $k \in \mathbb{K}\setminus\{0\}$ tal que $y_a = akI+b$ é invertível para todo $a \in \left\{\pm 1,\pm 2,\ldots,\pm\frac{s}{2}\right\}$. Por hipótese $[G(y_a,\ldots,y_a),y_a] = 0$. Dessa forma, como $akI \in \mathcal{Z}$ observamos que $[G(y_a,\ldots,y_a),akI] = 0$, donde

$$\begin{aligned} 0 = [G(y_a,\ldots,y_a),y_a] &= [G(y_a,\ldots,y_a),akI+b] \\ &= [G(y_a,\ldots,y_a),akI] + [G(y_a,\ldots,y_a),b], \end{aligned}$$

isto é, $[G(y_a,\ldots,y_a),b] = 0$, para todo $a \in \left\{\pm 1,\pm 2,\ldots,\pm\frac{s}{2}\right\}$. Em particular, observa-se que

$$[G(y_a,\ldots,y_a)+G(y_{-a},\ldots,y_{-a}),b] = 0, \tag{3.3}$$

para todo $a \in \left\{1,2,\ldots,\frac{s}{2}\right\}$.

Deste modo, sendo G uma aplicação simétrica, m-aditiva, m-linear sobre o menor corpo contido em $\mathbb{K}$ (se $char\ \mathbb{K} = 0$, G é m-linear sobre $\mathbb{Q}$; se, $char\ \mathbb{K} = p$, G é m-linear sobre $\mathbb{Z}_p$) e $y_a = akI+b$ segue que

$$G(y_a,\ldots,y_a) = \sum_{r=0}^{m} a^r \binom{m}{r} G(\underbrace{kI,\ldots,kI}_{r},b,\ldots,b)$$

e

$$G(y_{-a},\ldots,y_{-a}) = \sum_{r=0}^{m} (-1)^r a^r \binom{m}{r} G(\underbrace{kI,\ldots,kI}_{r},b,\ldots,b),[3]$$

para cada $a \in \left\{1,2,\ldots,\frac{s}{2}\right\}$.

A princípio, considere $m = 2$. Lançando mão do fato que $G(kI,\ldots,kI) \in \mathcal{Z}$ (Proposição

[3] Ao leitor interessado, verificamos ambas as igualdades nas Proposições A.3 e A.4 do apêndice A.

3.12) e da Igualdade (3.3) tem-se

$$
\begin{aligned}
[G(y_a,y_a)+G(y_{-a},y_{-a}),b]=0 \Rightarrow & \left[\left(a^2G(kI,kI)+2aG(kI,b)+G(b,b)\right)\right.\\
& \left.+\left(a^2G(kI,kI)-2aG(kI,b)+G(b,b)\right),b\right]=0\\
& \Rightarrow \left[2a^2G(kI,kI)+2G(b,b),b\right]=0\\
& \Rightarrow \left[2a^2G(kI,kI),b\right]+[2G(b,b),b]=0\\
& \Rightarrow 2a^2\left[G(kI,kI),b\right]+2\left[G(b,b),b\right]=0\\
& \Rightarrow [G(b,b),b]=0,
\end{aligned}
$$

visto que $G(kI,kI)\in \mathcal{Z}$, ou seja, $[G(kI,kI),b]=0$.

Agora, para $m\geq 3$ e tomando as igualdades acima para $G(y_a,\ldots,y_a)$ e $G(y_{-a},\ldots,y_{-a})$, a soma $G(y_a,\ldots,y_a)+G(y_{-a},\ldots,y_{-a})$ resulta em:

- Quando m é par

$$
\begin{aligned}
G(y_a,\ldots,y_a)+G(y_{-a},\ldots,y_{-a}) = & \, 2\binom{m}{0}G(b,\ldots,b)+2a^2\binom{m}{2}G(kI,kI,b,\ldots,b)+\cdots+\\
& +2a^{m-2}\binom{m}{m-2}G(kI,\ldots,kI,b,b)\\
& +2a^{m}\binom{m}{m}G(kI,\ldots,kI)\\
& =2\sum_{r=0}^{\frac{s}{2}}a^{2r}\binom{m}{2r}G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b).
\end{aligned}
$$

- Quando m é ímpar

$$
\begin{aligned}
G(y_a,\ldots,y_a)+G(y_{-a},\ldots,y_{-a}) = & \, 2\binom{m}{0}G(b,\ldots,b)+2a^2\binom{m}{2}G(kI,kI,b,\ldots,b)+\cdots+\\
& +2a^{m-3}\binom{m}{m-3}G(kI,\ldots,kI,b,b,b)+\\
& +2a^{m-1}\binom{m}{m-1}G(kI,\ldots,kI,b)\\
& =2\sum_{r=0}^{\frac{s-2}{2}}a^{2r}\binom{m}{2r}G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b).
\end{aligned}
$$

Da Proposição 3.12 temos $G(akI,\ldots,akI)\in\mathcal{Z}$, e sendo $[G(y_a,\ldots,y_a)+G(y_{-a},\ldots,y_{-a}),b]=0$, com m par, obtemos

$$
\begin{aligned}
0 &= \left[2\left(\sum_{r=0}^{\frac{s}{2}-1} a^{2r}\binom{m}{2r} G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b)\right) + 2a^m\binom{m}{m}G(kI,\ldots,kI),b\right]\\
&= \left[2\left(\sum_{r=0}^{\frac{s-2}{2}} a^{2r}\binom{m}{2r} G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b)\right),b\right] + \left[2a^m\binom{m}{m}G(kI,\ldots,kI),b\right]\\
&= 2\sum_{r=0}^{\frac{s-2}{2}} a^{2r}\binom{m}{2r}\left[G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b),b\right] + 2a^m\binom{m}{m}[G(kI,\ldots,kI),b]\\
&\Rightarrow 2\sum_{r=0}^{\frac{s-2}{2}} a^{2r}\binom{m}{2r}\left[G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b),b\right] = 0\\
&\Rightarrow \sum_{r=0}^{\frac{s-2}{2}} a^{2r}\binom{m}{2r}\left[G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b),b\right] = 0.
\end{aligned}
$$

Por conseguinte, para $m \geq 3$ segue-se que

$$\sum_{r=0}^{\frac{s-2}{2}} 2a^{2r}\binom{m}{2r}\left[G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b),b\right] = 0 \Rightarrow \sum_{r=0}^{\frac{s-2}{2}} a^{2r}\binom{m}{2r}\left[G(\underbrace{kI,\ldots,kI}_{2r},b,\ldots,b),b\right] = 0,$$

para cada $a \in \left\{1,2,\ldots,\frac{s}{2}\right\}$. Nestas condições, obtemos novamente um sistema de $\frac{s}{2}$ equações em $\frac{s}{2}$ incógnitas. De maneira similar ao que foi feito na demonstração da Proposição 3.12 tem-se um sistema na sua forma matricial

$$
\begin{pmatrix}
1 & 1 & 1 & \cdots & 1\\
1 & 2^2 & 2^4 & \cdots & 2^{(s-2)}\\
1 & 3^2 & 3^4 & \cdots & 3^{(s-2)}\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
1 & \left(\frac{s}{2}\right)^2 & \left(\frac{s}{2}\right)^4 & \cdots & \left(\frac{s}{2}\right)^{(s-2)}
\end{pmatrix}
\begin{pmatrix}
\binom{m}{0}[G(b,\ldots,b),b]\\
\vdots\\
\binom{m}{2r}[G(kI,\ldots,kI,\underbrace{b,\ldots,b}_{m-2r}),b]\\
\vdots\\
\binom{m}{s-2}[G(kI,\ldots,kI,\underbrace{b,\ldots,b}_{m-(s-2)}),b]
\end{pmatrix}
=
\begin{pmatrix}
0\\0\\0\\\vdots\\0
\end{pmatrix}.
$$

Assim, como o determinante da matriz de Vandermonde formada pelos coeficientes não é zero, concluímos que o sistema tem solução trivial, isto é,

$$\binom{m}{2r}[G(kI,\ldots,kI,\underbrace{b,\ldots,b}_{m-2r}),b] = 0 \Rightarrow [G(kI,\ldots,kI,\underbrace{b,\ldots,b}_{m-2r}),b] = 0,$$

para qualquer $r \in \left\{0,1,2,\ldots,\frac{s-2}{2}\right\}$. Em particular, para $r = 0$ segue-se que $[G(b,\ldots,b),b] = 0$.

Logo,

$$\left[G\left(\sum_{r=1}^{m+1} z_r e_{i_r j_r}, \ldots, \sum_{r=1}^{m+1} z_r e_{i_r j_r}\right), \sum_{r=1}^{m+1} z_r e_{i_r j_r}\right] = 0,$$

para $m \geq 2$, uma vez que $b = \sum_{r=1}^{m+1} z_r e_{i_r j_r}$.

Finalmente, observe que o resultado anterior pode ser obtido de maneira análoga substituindo $b = \sum_{r=1}^{m+1} z_r e_{i_r j_r}$ por $c_A = \sum_{r\in A} z_r e_{i_r j_r}$, onde $A \subseteq \{1, \ldots, m+1\}$ e z_r, i_r e j_r são os mesmos. Enfim,

$$\left[G\left(\sum_{r\in A} z_r e_{i_r j_r}, \ldots, \sum_{r\in A} z_r e_{i_r j_r}\right), \sum_{r\in A} z_r e_{i_r j_r}\right] = [G(c_A, \ldots, c_A), c_A] = 0$$

e isso nos rende a Afirmação 2.

Nestas condições, utilizando a identidade $[G(c_A, \ldots, c_A), c_A] = 0$, para $A \subsetneq \{1, \ldots, m+1\}$, podemos linearizar a identidade $[G(b, \ldots, b), b] = 0$. Daí, por meio do processo de linearização, sendo G uma aplicação m-aditiva, obtemos que

$$\sum_{\sigma\in S_{m+1}} \left[G\left(z_{\sigma(1)} e_{i_{\sigma(1)} j_{\sigma(1)}}, \ldots, z_{\sigma(m)} e_{i_{\sigma(m)} j_{\sigma(m)}}\right), z_{\sigma(m+1)} e_{i_{\sigma(m+1)} j_{\sigma(m+1)}}\right] = 0. \tag{3.4}$$

Afirmação 3. $[G(x, \ldots, x), x] = 0$ para todo $x \in M_n(\mathbb{K})$.

Considere $\{1, \ldots, n^2\}^{m+1} = \{1, \ldots, n^2\} \times \cdots \times \{1, \ldots, n^2\}$ ($(m+1)$-vezes) e considere o elemento $(i_1, \ldots, i_{m+1}) \in \{1, \ldots, n^2\}^{m+1}$. Defina a relação "$\sim$" na qual

$$(i_1, \ldots, i_{m+1}) \sim (j_1, \ldots, j_{m+1}),$$

se $(j_1, \ldots, j_{m+1}) = (i_{\sigma(1)}, \ldots, i_{\sigma(m+1)})$, com $\sigma \in S_{m+1}$. Não é difícil verificar que esta é uma relação de equivalência. Denote por Δ um conjunto de $(m+1)$-uplas representantes das distintas classes de equivalência.

Dado $x \in M_n(\mathbb{K})$, tem-se que podemos escrevê-lo da forma

$$x = \sum_{i=1}^{n^2} x_i,$$

onde $x_i = z_i e_{r_i s_i}$, para algum $z_i \in \mathbb{K}$ e $r_i, s_i \in \{1, \ldots, n\}$.

Aqui, $\beta = \{e_{11}, \ldots, e_{nn}\}$ denota a base canônica de $M_n(\mathbb{K})$. Desse modo,

$$\begin{aligned}
[G(x, \ldots, x), x] &= \left[G\left(\sum_{i=1}^{n^2} x_i, \ldots, \sum_{i=1}^{n^2} x_i\right), \sum_{i=1}^{n^2} x_i\right] \\
&= \sum_{i_1, i_2, \ldots, i_{m+1}=1}^{n^2} \left[G\left(x_{i_1}, \ldots, x_{i_m}\right), x_{i_{m+1}}\right] \\
&= \sum_{(i_1, i_2, \ldots, i_{m+1})\in\Delta} \left(\sum_{\sigma\in S_{m+1}} \left[G\left(x_{i_{\sigma(1)}}, \ldots, x_{i_{\sigma(m)}}\right), x_{i_{\sigma(m+1)}}\right]\right).
\end{aligned}$$

Sendo assim, da relação obtida em (3.4) acima, concluímos que $[G(x,\ldots,x),x]=0$. O resultado desejado segue do Teorema 3.10. ■

3.3 Aplicação Traço Comutante em Matrizes Singulares

O objetivo desta seção é realizar uma análise semelhante à seção anterior, porém considerando matrizes singulares. Mais especificamente, estudaremos aplicações traço de aplicações m-aditivas comutantes no conjunto de matrizes singulares, que sob certas hipóteses podem ser escritas da seguinte forma:

$$G(x,\ldots,x)=\mu_0 x^m+\mu_1(x)x^{m-1}+\cdots+\mu_{m-1}(x)x+\mu_m(x), \quad \forall x\in M_n(\mathbb{K}).$$

Nessa expressão, $\mu_0\in\mathcal{Z}$ e $\mu_i : M_n(\mathbb{K})\to\mathcal{Z}$ são tais que cada μ_i é o traço de uma aplicação i-aditiva para $i\in\{1,\ldots,m\}$.

Conforme mencionado em situações anteriores, nesta seção reservamos o símbolo $\mathcal{Z}$ para denotar o centro $\mathbb{K}\cdot I_n$ de $M_n(\mathbb{K})$, onde I_n é a matriz identidade de ordem n.

A ideia da prova do próximo resultado é semelhante a prova do Teorema 3.14. Em resumo, mostraremos que $G(x,\ldots,x)$ é comutante em $M_n(\mathbb{K})$ e concluiremos usando o Teorema 3.10. Enfim, podemos enunciar e provar o segundo resultado principal.

Teorema 3.15. *Sejam $\mathbb{K}$ um corpo e n e m inteiros positivos satisfazendo $n>m+1$ e $m>1$. Seja $G : M_n(\mathbb{K})^m\to M_n(\mathbb{K})$ uma aplicação m-aditiva simétrica tal que*

$$[G(x,x,\ldots,x),x]=0,$$

para toda matriz singular $x\in M_n(\mathbb{K})$. Assuma char $\mathbb{K}=0$ ou char $\mathbb{K}\geq m+1$. Então, existem $\mu_0\in\mathcal{Z}$ e $\mu_i : M_n(\mathbb{K})\to\mathcal{Z}$, tal que cada μ_i é o traço de uma aplicação i-aditiva para $i\in\{1,\ldots,m\}$ e

$$G(x,\ldots,x)=\mu_0 x^m+\mu_1(x)x^{m-1}+\cdots+\mu_{m-1}(x)x+\mu_m(x),\ \forall x\in M_n(\mathbb{K}).$$

Demonstração. Para cada $r\in\{1,\ldots,m+1\}$ considere $z_r\in\mathcal{Z}$ e $i_r, j_r\in\{1,\ldots,n\}$. Sabendo que as matrizes têm ordem $n>m+1$, é fácil perceber que, para cada $A\subseteq\{1,\ldots,m+1\}$, $c_A=\sum_{r\in A} z_r e_{i_r j_r}$ é uma matriz singular. Deste modo, aplicando a hipótese sobre G para c_A, segue que $[G(c_A,\ldots,c_A),c_A]=0$, para cada $A\subseteq\{1,\ldots,m+1\}$. Logo, tem-se

$$\left[G(\sum_{r\in A} z_r e_{i_r j_r},\ldots,\sum_{r\in A} z_r e_{i_r j_r}),\sum_{r\in A} z_r e_{i_r j_r}\right]=0, \tag{3.5}$$

para todo $A \subset \{1,\ldots,m+1\}$. Particularmente, quando $A = \{1,\ldots,m+1\}$ tem-se

$$\left[G(\sum_{r=1}^{m+1} z_r e_{i_r j_r},\ldots,\sum_{r=1}^{m+1} z_r e_{i_r j_r}),\sum_{r=1}^{m+1} z_r e_{i_r j_r}\right] = 0.$$

Conforme foi feito antes de (3.4), podemos utilizar a m-aditividade da aplicação G quando $A = \{1,\ldots,m+1\}$, juntamente com a identidade obtida em (3.5) e a linearização da identidade $[G(c_A,\ldots,c_A),c_A] = 0$, para se obter

$$\sum_{\sigma\in S_{m+1}} \left[G\left(z_{\sigma(1)}e_{i_{\sigma(1)}j_{\sigma(1)}},\ldots,z_{\sigma(m)}e_{i_{\sigma(m)}j_{\sigma(m)}}\right),z_{\sigma(m+1)}e_{i_{\sigma(m+1)}j_{\sigma(m+1)}}\right] = 0.$$

Portanto, seguindo os passos da Afirmação 3 do teorema anterior mais uma vez, segue que $[G(x,x,\ldots,x),x] = 0$, para todo $x \in M_n(\mathbb{K})$. Novamente, pelo Teorema 3.10, obtemos o resultado desejado. ■

3.4 Aplicações

Dedicamos essa seção para uma aplicação interessante do Teorema 3.14. Fazendo uso do resultado citado e da técnica desenvolvida por Brešar em [3] obtemos, de forma simples, um resultado creditado a Cao e Zhang em [6]. Mais precisamente, aplicaremos a teoria desenvolvida na Seção 3.2 no próximo resultado.

Teorema 3.16. *Sejam $\mathbb{K}$ um corpo com char $\mathbb{K} \neq 2,3$, cuja cardinalidade satisfaz $|\mathbb{K}| \geq 11$. Seja $\theta : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ uma aplicação linear tal que $\theta : GL_n(\mathbb{K}) \to GL_n(\mathbb{K})$ é uma bijeção, para algum número natural $n > 2$. Considere ainda que θ satisfaz a condição $[\theta(x^2),\theta(x)] = 0$, para todo $x \in GL_n(\mathbb{K})$. Então, $\theta(x) = \lambda\phi(x)$, onde $\lambda \in \mathbb{K}\setminus\{0\}$ e ϕ ou é um isomorfismo ou um anti-isomorfismo de $M_n(\mathbb{K})$.*

Demonstração. Para resolver tal problema utilizando o Teorema 3.14, é suficiente que encontremos uma aplicação $G : M_n(\mathbb{K})^2 \to M_n(\mathbb{K})$ bilinear tal que $[G(x,x),x] = 0$, para todo $x \in GL_n(\mathbb{K})$. Para este fim, defina $G(x,y) = \theta(\theta^{-1}(x)\theta^{-1}(y))$, para $x,y \in M_n(\mathbb{K})$. Primeiramente, observe que G é uma forma bilinear bem definida, uma vez que θ é uma aplicação linear bijetora em $M_n(\mathbb{K})$. Com efeito, tome uma matriz elementar e_{ij} em $M_n(\mathbb{K})$. Caso $i \neq j$, tem-se que $I_n + e_{ij}$ é uma matriz invertível, onde I_n é a matriz identidade de ordem n. E o caso $i = j$ segue de modo análogo, uma vez que *char* $\mathbb{K} \neq 2$. Por θ ser linear e bijetora sobre $GL_n(\mathbb{K})$, existem matrizes invertíveis A e B em $M_n(\mathbb{K})$ tais que

$$e_{ij} = (e_{ij}+I_n) - I_n = \theta(A) - \theta(B) = \theta(A-B).$$

Isso implicará que θ é sobrejetiva sobre $M_n(\mathbb{K})$. Agora, a injetividade segue pelo clássico Teorema do Núcleo e da Imagem da Álgebra Linear. Desse modo, segue a boa definição da aplicação G.

O fato de $G(x,y)$ ser uma aplicação bilinear deve ser verificado. Sendo θ uma aplicação linear de $M_n(\mathbb{K})$ em si próprio, segue que

$$\begin{aligned} G(x+y,z) = \theta\left(\theta^{-1}(x+y)\theta^{-1}(z)\right) &= \theta\left(\left[\theta^{-1}(x)+\theta^{-1}(y)\right]\theta^{-1}(z)\right) \\ &= \theta\left(\theta^{-1}(x)\theta^{-1}(z)+\theta^{-1}(y)\theta^{-1}(z)\right) \\ &= \theta\left(\theta^{-1}(x)\theta^{-1}(z)\right)+\theta\left(\theta^{-1}(y)\theta^{-1}(z)\right) \\ &= G(x,z)+G(y,z). \end{aligned}$$

De forma análoga obtém-se $G(x,y+z) = G(x,y)+G(x,z)$. Além disso, para $\lambda \in \mathbb{K}$ tem-se

$$\begin{aligned} G(\lambda x,y) = \theta\left(\theta^{-1}(\lambda x)\theta^{-1}(y)\right) &= \theta\left(\lambda\theta^{-1}(x)\theta^{-1}(y)\right) \\ &= \lambda\theta\left(\theta^{-1}(x)\theta^{-1}(y)\right) \\ &= \lambda G(x,y). \end{aligned}$$

De forma análoga mostra-se que $G(x,\lambda y) = \lambda G(x,y)$.

Agora, considere $x \in GL_n(\mathbb{K})$ fixado. Por hipótese, existe um único $u \in GL_n(\mathbb{K})$ de modo que $\theta(u) = x$. Sendo assim, note que

$$G(x,x) = \theta\left(\theta^{-1}(x)\theta^{-1}(x)\right) = \theta\left(\theta^{-1}(\theta(u))\theta^{-1}(\theta(u))\right) = \theta(u^2).$$

Logo, lembrando que $[\theta(y^2),\theta(y)] = 0$, para todo $y \in GL_n(\mathbb{K})$, temos

$$G(x,x)x = \theta(u^2)\theta(u) = \theta(u)\theta(u^2) = xG(x,x),$$

isto é, $[G(x,x),x] = 0$, para todo $x \in GL_n(\mathbb{K})$. Deste modo, segue pelo Teorema 3.14 que existem $\mu_0 \in \mathbb{K}$, $\mu_1,\mu_2 : M_n(\mathbb{K}) \to \mathcal{Z}$, onde μ_1 é uma aplicação aditiva e μ_2 é uma aplicação biaditiva tais que

$$G(x,x) = \theta\left(\left(\theta^{-1}(x)\right)^2\right) = \mu_0 x^2 + \mu_1(x)x + \mu_2(x,x),$$

para todo $x \in M_n(\mathbb{K})$.

Deste modo, substituindo $\theta^{-1}(x) = y$, com $y \in M_n(\mathbb{K})$, segue que $x = \theta(y)$ e

$$\theta\left(y^2\right) = \mu_0\theta(y)^2 + \mu_1(\theta(y))\theta(y) + \mu_2(\theta(y),\theta(y)).$$

É notável que $[\theta(y^2),\theta(y)] = 0$, uma vez que $\mu_0 \in \mathbb{K}$ e $\mu_1,\mu_2 : M_n(\mathbb{K}) \to \mathcal{Z}$. Desde que θ é uma bijeção, tem-se que θ^{-1} também é, e assim vale que $[\theta(y^2),\theta(y)] = 0$, para todo $y \in M_n(\mathbb{K})$.

Devido ao Teorema 3.11, $\theta(x) = \lambda\phi(x) + \mu(x)I$, onde $\lambda \in \mathbb{K} \setminus \{0\}$, μ é um funcional linear de $M_n(\mathbb{K})$ em $\mathbb{K}$ e ϕ ou é um isomorfismo ou é um anti-isomorfismo. Dessa forma, para concluirmos nosso resultado, basta provarmos que μ é o funcional nulo. Notemos que é suficiente provar que $\mu(e_{ij}) = 0$, para todo $i, j \in \{1, \dots, n\}$, uma vez que μ é linear e o conjunto formado pelas matrizes elementares e_{ij} é uma base para $M_n(\mathbb{K})$.

Vamos primeiramente considerar $a \in M_n(\mathbb{K})$ não nula e nilpotente de índice dois. Deste modo, $a^2 = 0$. Sendo ϕ isomorfismo ou antisomorfismo, tem-se que $\phi(a)^2 = \phi\left(a^2\right) = 0$. Como $\phi(a) \neq 0$, pois a é não nula, segue-se que $\phi(a)$ é também uma matriz nilpotente de índice dois. Por a ser nilpotente, tem-se que a é também uma matriz singular. Daí, utilizando o fato de $\theta : GL_n(\mathbb{K}) \to GL_n(\mathbb{K})$ ser uma bijeção segue que $\theta(a)$ é uma matriz singular, do contrário teríamos que a seria invertível, o que não é o caso. Sendo assim,

$$\det(\lambda\phi(a) + \mu(a)I_n) = \det(\theta(a)) = 0,$$

donde concluímos que $-\mu(a)$ é um autovalor para a matriz $\lambda\phi(a)$, que é nilpotente. Consequentemente, $\mu(a) = 0$. Em particular, $\mu(e_{ij}) = 0$, para $i \neq j$, com $i, j \in \{1, \dots, n\}$.

Agora, considere $a \in M_n(\mathbb{K})$ uma matriz idempotente singular, isto é, $a^2 = a$ e $a \neq I_n$. Nestas condições, o fato de ϕ ou ser um isomorfismo ou um anti-isomorfismo, implica que $\phi(a)$ é uma matriz idempotente. Novamente, atentando-se ao fato de que θ é uma bijeção de $GL_n(\mathbb{K})$ nele mesmo, obtemos que $\theta(a)$ é uma matriz singular, do contrário a seria invertível, o que não é o caso. Por conseguinte, a equação

$$\det(\lambda\phi(a) + \mu(a)I_n) = \det(\theta(a)) = 0,$$

nos permite dizer que $-\mu(a)$ é um autovalor da matriz $\lambda\phi(a)$.

Afirmação: $\mu(a)$ ou é $-\lambda$ ou 0.

De fato, basta notar que $\lambda^{-1}\theta(a)$ ainda é uma matriz singular. Ademais,

$$\begin{aligned}\theta(a) = \lambda\phi(a) + \mu(a)I_n &\Rightarrow \lambda^{-1}\theta(a) = \phi(a) + \lambda^{-1}\mu(a)I_n \\ &\Rightarrow \theta_0(a) = \phi(a) - \lambda_0 I_n,\end{aligned}$$

em que $\lambda_0 = -\left(\lambda^{-1}\mu(a)\right)$ e $\theta_0(a) = \lambda^{-1}\theta(a)$. Nestas condições, tem-se

$$\det(\phi(a) - \lambda_0 I_n) = \det(\theta_0(a)) = 0,$$

donde concluímos que λ_0 é um autovalor associado à matriz idempotente $\phi(a)$. Assim, tomando E o operador associado à matriz $\phi(a)$, tem-se que E é um operador idempotente ($E^2 \equiv E$) e que λ_0 é um autovalor de E. Desta forma, tomando v um autovetor associado a λ_0, tem-se que

$E(v) = \lambda_0 v$. Agora, observe que

$$\begin{aligned} E(v) = \lambda_0 v \Rightarrow E^2(v) = E(\lambda_0 v) = \lambda_0 E(v) = \lambda_0^2 v \\ \Rightarrow E(v) = \lambda_0^2 v \\ \Rightarrow \lambda_0 v = \lambda_0^2 v \\ \Rightarrow (\lambda_0 - \lambda_0^2) v = 0. \end{aligned}$$

Sendo v um autovetor, segue que $\lambda_0(1-\lambda_0) = 0$, isto é, ou $\lambda_0 = 0$ ou $\lambda_0 = 1$. Sendo assim, temos $-\left(\lambda^{-1}\mu(a)\right) = 0$ ou $-\left(\lambda^{-1}\mu(a)\right) = 1$, de onde obtemos que $\mu(a)$ ou é $-\lambda$ ou 0, e concluímos a nossa afirmação.

Em particular, sendo e_{ii} uma matriz idempotente para $i \in \{1, \ldots, n\}$, tem-se que $\mu(e_{ii})$ é $-\lambda$ ou 0. Agora, para mostrar que μ é um funcional nulo basta provarmos que $\mu(e_{ii}) = 0$, para todo $i \in \{1, \ldots, n\}$. Com efeito, suponhamos por contradição que exista $k \in \{1, \ldots, n\}$ tal que $\mu(e_{kk}) = -\lambda$. Veja que $a_j = e_{kk} + e_{jj}$ é uma matriz singular e idempotente para todo $j \in \{1, \ldots, n\} \setminus \{k\}$, visto que $n > 2$. Nestas condições, $\mu(e_{jj}) = 0$, caso contrário teríamos $\mu(a_j) = \mu(e_{kk} + e_{jj}) = \mu(e_{kk}) + \mu(e_{jj}) = -2\lambda \neq 0$, pois *char* $\mathbb{K} \neq 2$, o que contradiria o fato de que $\mu(a_j)$ ou é 0 ou é $-\lambda$. Agora, sendo ϕ um isomorfismo ou anti-isomorfismo, segue que $\phi(I_n) = I_n$. Entretanto, veja que

$$\begin{aligned} \theta(I_n) = \lambda\phi(I_n) + \sum_{i=1}^{n} \mu(e_{ii}) I_n &= \lambda I_n + \sum_{i=1}^{n} \mu(e_{ii}) I_n \\ &= \lambda I_n + \left(\sum_{i \in \{1,\ldots,n\} \setminus \{k\}} \mu(e_{ii}) I_n \right) + \mu(e_{kk}) I_n \\ &= \lambda I_n + (-\lambda) I_n \\ &= 0_n, \end{aligned}$$

onde 0_n denota a matriz nula em $M_n(\mathbb{K})$, contradizendo a hipótese de que $\theta(I_n)$ é invertível. Assim, $\mu(e_{ii}) = 0$, para todo $i \in \{1, \ldots, n\}$. Portanto, $\mu(e_{ij}) = 0$ para todo $i, j \in \{1, \ldots, n\}$, o que conclui a prova do corolário. ■

CAPÍTULO 4

Traços de Aplicações Multiaditivas Comutantes em Matrizes Invertíveis: uma nova perspectiva

Em meio ao estudo e à pesquisa para o nosso trabalho nos deparamos com um resultado interessante dado por Xu e Zhu [23], o qual fornece uma nova prova para o Teorema 3.14. Por conseguinte, decidimos dedicar este capítulo ao estudo de tal resultado e, como aplicação, obter uma prova alternativa para o Teorema 3.14.

4.1 Conceitos e Resultados Introdutórios

Antes de irmos para a demonstração do resultado principal deste capítulo (Teorema 4.6), introduziremos um conceito relacionado a aplicações m-aditivas, o qual nos possibilitará uma melhor compreensão da prova dada. Ademais, também devemos abordar alguns lemas que nos auxiliarão na demonstração do resultado principal e, posteriormente, obter uma demonstração alternativa do Teorema 3.14 como uma aplicação. Doravante, no decorrer do texto, sempre que abordarmos o termo "uma aplicação m-aditiva G", estaremos fazendo referência a uma aplicação $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ que preserva soma em suas m entradas, com $m \geq 1$.

Definição 4.1. *Considere a aplicação $\delta_1 : M_n(\mathbb{K}) \to M_n(\mathbb{K})$, dada por $\delta_1(x_1) = G(x_1, x_1, \ldots, x_1)$, em que $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ é uma aplicação m-aditiva. Assim, para $k \geq 2$, denominaremos* *de k-**mapa** de G a aplicação* $\delta_k : M_n(\mathbb{K})^k \to M_n(\mathbb{K})$ *dada por*

$$\delta_k(x_1,x_2,\ldots,x_k) = \delta_1(x_1+x_2+\cdots+x_k) - \sum_{i=1}^{k-1} \sum_{1\le l_1<l_2<\cdots<l_i\le k} \delta_i(x_{l_1},x_{l_2},\ldots,x_{l_i}).$$

Observe que a aplicação 1-map δ_1 de G é exatamente a aplicação traço de G, que se encontra na Definição 3.7. Para $k=2$ temos

$$\begin{aligned}\delta_2(x_1,x_2) &= \delta_1(x_1+x_2) - \sum_{1\le l_1\le 2} \delta_1(x_{l_1})\\ &= G(x_1+x_2,\ldots,x_1+x_2) - G(x_1,\ldots,x_1) - G(x_2,\ldots,x_2).\end{aligned}$$

Para $k=3$ temos

$$\begin{aligned}\delta_3(x_1,x_2,x_3) &= \delta_1(x_1+x_2+x_3) - \sum_{i=1}^{2} \sum_{1\le l_1<l_2<\cdots<l_i\le 3} \delta_i(x_{l_1},x_{l_2},\ldots,x_{l_i})\\ &= \delta_1(x_1+x_2+x_3) - \sum_{1\le l_1\le 3}\delta_1(x_{l_1}) - \sum_{1\le l_1<l_2\le 3}\delta_2(x_{l_1},x_{l_2})\\ &= \delta_1(x_1+x_2+x_3) - \delta_1(x_1) - \delta_1(x_2) - \delta_1(x_3) - \delta_2(x_1,x_2) - \delta_2(x_1,x_3) - \delta_2(x_2,x_3)\\ &= G(x_1+x_2+x_3,\ldots,x_1+x_2+x_3) - G(x_1,\ldots,x_1) - G(x_2,\ldots,x_2) - G(x_3,\ldots,x_3)\\ &\quad - (G(x_1+x_2,\ldots,x_1+x_2) - G(x_1,\ldots,x_1) - G(x_2,\ldots,x_2))\\ &\quad - (G(x_1+x_3,\ldots,x_1+x_3) - G(x_1,\ldots,x_1) - G(x_3,\ldots,x_3))\\ &\quad - (G(x_2+x_3,\ldots,x_2+x_3) - G(x_2,\ldots,x_2) - G(x_3,\ldots,x_3)).\end{aligned}$$

Além disso, a k-mapa δ_k de G é uma aplicação simétrica, pois

$$\delta_k(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(k)}) = \delta_1(x_1+x_2+\cdots+x_k) - \sum_{i=1}^{k-1} \sum_{1\le l_1<l_2<\cdots<l_i\le k} \delta_i(x_{l_1},x_{l_2},\ldots,x_{l_i}),$$

para qualquer $\sigma \in S_k$. Deste modo, podemos caracterizar δ_k da seguinte forma:

Lema 4.2. *Sejam* $T_k = \{x_1,x_2,\ldots,x_k\}$ *o conjunto formado pelas k-variáveis de* δ_k*, G uma aplicação m-aditiva e*

$$T_k^s = \underbrace{T_k \times T_k \times \cdots \times T_k}_{s}.$$

Então,

$$\delta_k(x_1,x_2,\ldots,x_k) = \sum_{(y_1,y_2,\ldots,y_m)\in T_k^m} G(y_1,y_2,\ldots,y_m)$$

e $\{y_1,y_2,\ldots,y_m\} = T_k$.

Demonstração. Provaremos o resultado por indução em k. Para $k=1$, temos $T_1 = \{x_1\}$ e

$$\delta_1(x_1) = G(x_1, x_1, \ldots, x_1),$$

onde tem-se $(x_1, x_1, \ldots, x_1) \in T_1^m$ e $\{x_1\} = T_1$. Para $k=2$, tem-se $T_2 = \{x_1, x_2\}$ e

$$\begin{aligned}
\delta_2(x_1, x_2) &= \delta_1(x_1 + x_2) - \delta_1(x_1) - \delta_1(x_2) \\
&= G(x_1+x_2, x_1+x_2, \ldots, x_1+x_2) - G(x_1, x_1, \ldots, x_1) - G(x_2, x_2, \ldots, x_2) \\
&= \sum_{(y_1, y_2, \ldots, y_m) \in T_2^m} G(y_1, y_2, \ldots, y_m),
\end{aligned}$$

onde $\{y_1, y_2, \ldots, y_m\} = T_2 = \{x_1, x_2\}$. A última igualdade segue do fato de G ser uma aplicação m-aditiva.

Agora suponhamos que, para algum $k > 2$, tenhamos $\delta_1, \delta_2, \ldots, \delta_{k-1}$ satisfazendo a identidade enunciada no lema. Por definição veja que

$$\begin{aligned}
\delta_k(x_1, x_2, \ldots, x_k) &= \delta_1(x_1 + x_2 + \cdots + x_k) - \sum_{i=1}^{k-1} \sum_{1 \le l_1 < l_2 < \cdots < l_i \le k} \delta_i\left(x_{l_1}, x_{l_2}, \ldots, x_{l_i}\right) \\
&= \delta_1(x_1 + x_2 + \cdots + x_k) - \left[\sum_{1 \le l_1 \le k} \delta_1\left(x_{l_1}\right) + \sum_{1 \le l_1, l_2 \le k} \delta_2\left(x_{l_1}, x_{l_2}\right) + \cdots \right. \\
&\quad \left. + \sum_{1 \le l_1 < l_2 < \cdots < l_{k-1} \le k} \delta_{k-1}\left(x_{l_1}, x_{l_2}, \ldots, x_{l_{k-1}}\right)\right].
\end{aligned}$$

Fazendo uso da hipótese de indução, da definição de δ_1 nas parcelas do lado direito da soma, e considerando que G é uma aplicação m-aditiva, obtemos que

$$\begin{aligned}
\delta_k(x_1, x_2, \ldots, x_k) &= G\left(\sum_{i=1}^{k} x_i, \sum_{i=1}^{k} x_i, \ldots, \sum_{i=1}^{k} x_i\right) - \left[\sum_{1 \le l_1 \le k} \sum_{(y_{11}, y_{12}, \ldots, y_{1m}) \in \left\{x_{l_1}\right\}^m} G\left(y_{11}, y_{12}, \ldots, y_{1m}\right)\right. \\
&\quad + \sum_{1 \le l_1 < l_2 \le k} \sum_{(y_{21}, y_{22}, \ldots, y_{2m}) \in \left\{x_{l_1}, x_{l_2}\right\}^m} G\left(y_{21}, y_{22}, \ldots, y_{2m}\right) + \cdots \\
&\quad \left. + \sum_{1 \le l_1 < \cdots < l_{k-1} \le k} \sum_{\left(y_{(k-1)1}, y_{(k-1)2}, \ldots, y_{(k-1)m}\right) \in \left\{x_{l_1}, \ldots, x_{l_{k-1}}\right\}^m} G\left(y_{(k-1)1}, y_{(k-1)2}, \ldots, y_{(k-1)m}\right)\right]
\end{aligned}$$

onde

- $\{y_{11}, y_{12}, \ldots, y_{1m}\} = T_1 = \{x_{l_1}\}$, com $1 \le l_1 \le k$;
- $\{y_{21}, y_{22}, \ldots, y_{2m}\} = T_2 = \{x_{l_1}, x_{l_2}\}$, com $1 \le l_1 < l_2 \le k$;

  $\vdots$
- $\{y_{(k-1)1}, y_{(k-1)2}, \ldots, y_{(k-1)m}\} = T_{k-1} = \left\{x_{l_1}, x_{l_2}, \ldots, x_{l_{k-1}}\right\}$, $1 \le l_1 < l_2 < \ldots < l_{k-1} \le k$.

Por outro lado, observe que

$$G\left(\sum_{i=1}^{k} x_i, \sum_{i=1}^{k} x_i, \dots, \sum_{i=1}^{k} x_i\right) = \sum_{(y_{k1}, y_{k2}, \dots, y_{km}) \in \{x_1, \dots, x_k\}^m} G(y_{k1}, y_{k2}, \dots, y_{km}),$$

em que $\{y_{k1}, y_{k2}, \dots, y_{km}\} \subseteq \{x_1, \dots, x_k\} = T_k$. Dessa forma, observe que, quando o conjunto $\{y_{k1}, y_{k2}, \dots, y_{km}\}$ é um subconjunto próprio de T_k, as parcelas correspondentes se anulam com aquelas que aparecem com sinal negativo. Assim, as únicas parcelas restantes são indexadas pelo conjunto T_k, concluindo a prova do resultado. ■

Agora, observe que, sendo $k > m$, não existe $G(y_1, y_2, \dots, y_m)$ satisfazendo ambas as condições $(y_1, y_2, \dots, y_m) \in T_k^m$ e $\{y_1, y_2, \dots, y_m\} = T_k$, haja visto que $|\{y_1, y_2, \dots, y_m\}| \leq m < k = |T_k|$. Daí, para $k > m$, temos que $\delta_k \equiv 0$. Desse modo, temos o seguinte corolário.

Corolário 4.3.

$$\delta_1(x_1 + x_2 + \cdots + x_{m+1}) = \sum_{i=1}^{m} \sum_{1 \leq l_1 < \cdots < l_i \leq m+1} \delta_i(x_{l_1}, x_{l_2}, \dots, x_{l_i}).$$

Os próximos dois lemas, bem como o corolário anterior, serão utilizados na demonstração do Teorema 4.6.

Lema 4.4. *Considere $k \in \{1, 2, \dots, m\}$ fixado. Assuma que $A_1, A_2, \dots, A_k \in M_n(\mathbb{K})$ são tais que $A_{l_1} + A_{l_2} + \cdots + A_{l_i} \in GL_n(\mathbb{K})$, para cada $i \in \{1, 2, \dots, k\}$ e qualquer sequência dada por $1 \leq l_1 < l_2 < \cdots < l_i \leq k$. Se $\delta_1(A) = 0$ para todo $A \in GL_n(\mathbb{K})$, então $\delta_k(A_1, A_2, \dots, A_k) = 0$.*

Demonstração. Vamos provar aplicando indução sobre k. O caso $k = 1$ é imediato, uma vez que $A_1 \in GL_n(\mathbb{K})$ e por conseguinte $\delta_1(A_1) = 0$. Agora, para $k = 2$ segue que $A_1, A_2 \in M_n(\mathbb{K})$ são tais que $A_1, A_2, A_1 + A_2 \in GL_n(\mathbb{K})$ implicando, da Definição 4.1,

$$\delta_1(A_1 + A_2) = \delta_1(A_1) = \delta_1(A_2) = 0_n,$$

e daí $\delta_2(A_1, A_2) = 0_n$. Por fim, suponhamos que $\delta_1, \delta_2, \dots, \delta_{k-1}$ satisfazem a tese do lema, para as condições dadas. Daí, aplicando a definição de δ_k, segue que

$$\begin{aligned} \delta_k(A_1, \dots, A_k) &= \delta_1(A_1 + \cdots + A_k) - \sum_{i=1}^{k-1} \sum_{1 \leq l_1 < \cdots < l_i \leq m+1} \delta_i(A_{l_1}, A_{l_2}, \dots, A_{l_i}) \\ &= 0_n \end{aligned}$$

desde que, por hipótese de indução tem-se $\delta_i(A_{l_1}, A_{l_2}, \dots, A_{l_i}) = 0$, para $1 \leq i \leq k-1$, e sendo $A_1, A_2, \dots, A_k \in M_n(\mathbb{K})$ matrizes tais que $A_1 + \cdots + A_k \in GL_n(\mathbb{K})$, segue por hipótese que $\delta_1(A_1 + \cdots + A_k) = 0$, donde concluímos que $\delta_k \equiv 0$, para todo $k \in \mathbb{N}$. ■

Lema 4.5. *Se alguma das seguintes condições vale:*

i. *char* $\mathbb{K} = 0$;

ii. *char* $\mathbb{K} > m$;

iii. *char* $\mathbb{K} = m$ *e* $|\mathbb{K}| > m$;

iv. $|\mathbb{K}| \geq 2^m$,

então, para uma matriz singular $A \in M_n(\mathbb{K})$*, existem matrizes* $A_1, A_2, \ldots, A_{m+1}$ *em* $M_n(\mathbb{K})$ *tais que* $A_{l_1} + A_{l_2} + \cdots + A_{l_i} \in GL_n(\mathbb{K})$*, para cada* $i \in \{1,2,\ldots,m\}$ *e qualquer sequência dada por* $1 \leq l_1 < l_2 < \ldots < l_i \leq m+1$*, e* $A = \sum_{i=1}^{m+1} A_i$*.*

Demonstração. Seja $A \in M_n(\mathbb{K})$ uma matriz de posto $s < n$. Desse modo, pela Proposição 1.48, existem P, Q em $GL_n(\mathbb{K})$ tais que $P^{-1}AQ^{-1} = \sum_{j=1}^{s} e_{j(j+1)}$. Notavelmente, se $s = 0$, a matriz $\sum_{j=1}^{s} e_{j(j,+1)}$ será a matriz nula 0_n.

Inicialmente, suponhamos que *char* $\mathbb{K} = 0$ ou *char* $\mathbb{K} > m$. Sendo $P, Q \in GL_n(\mathbb{K})$, temos que $PQ \in GL_n(\mathbb{K})$. Agora, considere $A_1 = A_2 = \ldots = A_m = PQ$ e $A_{m+1} = P(-mI_n + \sum_{j=1}^{s} e_{j(j+1)})Q$. É imediato que A_i, para $1 \leq i \leq m$, é uma matriz invertível. Além disso, veja que A_{m+1} é uma matriz invertível, pois $-mI_n + \sum_{j=1}^{s} e_{j(j+1)}$ é uma matriz invertível, haja visto as hipóteses que estamos assumindo sobre a característica do corpo.

Neste momento, observe que $A_{l_1} + A_{l_2} + \cdots + A_{l_i} \in GL_n(\mathbb{K})$, para cada $i \in \{1,2,\ldots,m\}$, com $1 \leq l_1 < l_2 < \ldots < l_i \leq m+1$. De fato, se $l_k \neq m+1$ para todo $k \in \{1,2,\ldots,i\}$, então $A_{l_1} + A_{l_2} + \cdots + A_{l_i} = iPQ \in GL_n(\mathbb{K})$ segue da hipótese sobre a característica do corpo, pois $i \leq m$. Caso $l_k = m+1$ para algum $j \in \{1,2,\ldots,i\}$, tem-se

$$
\begin{aligned}
A_{l_1} + A_{l_2} + \cdots + A_{l_i} &= (i-1)PQ + P\left(-mI_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q \\
&= P((i-1)I_n)Q + P\left(-mI_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q \\
&= P\left((i-1)I_n - mI_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q \\
&= P\left((i-(m+1))I_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q \in GL_n(\mathbb{K}),
\end{aligned}
$$

uma vez que $-m \leq i-(m+1) \leq -1$.

Ademais, sendo $A_1 + \cdots + A_m = mPQ$ e $A_{m+1} = -mPQ + P\left(\sum_{j=1}^{s} e_{j(j+1)}\right)Q = -mPQ + A$, segue que

$$\begin{aligned}(A_1+\cdots+A_m)+A_{m+1} &= mPQ-mPQ+P\left(\sum_{j=1}^{s} e_{j(j+1)}\right)Q\\ &= P\left(\sum_{j=1}^{s} e_{j(j+1)}\right)Q\\ &= A.\end{aligned}$$

Agora, suponha que *char* $\mathbb{K}=m$ e $|\mathbb{K}|>m$. Defina as matrizes que queremos da seguinte forma: $A_1=A_2=\ldots=A_{m-1}=PQ$, $A_m=tPQ$ e $A_{m+1}=P\left((1-t)I_n+\sum_{j=1}^{s} e_{j(j+1)}\right)Q$, onde $t\in\mathbb{K}\setminus\{0,1,\ldots,m-1\}$. Devemos analisar a interseção $\{m,m+1\}\cap\{l_1,l_2,,\ldots,l_i\}$ e observar que $A_{l_1}+A_{l_2}+\cdots+A_{l_i}\in GL_n(\mathbb{K})$, para qualquer sequência $1\leq l_1<l_2<\ldots<l_i\leq m+1$.

É imediato que se $\{m,m+1\}\cap\{l_1,l_2,,\ldots,l_i\}$ for vazio, tem-se

$$A_{l_1}+A_{l_2}+\cdots+A_{l_i}=iPQ\in GL_n(\mathbb{K}),$$

pois *char* $\mathbb{K}=m$ e $i\in\{1,\ldots,m-1\}$.

No caso $|\{m,m+1\}\cap\{l_1,l_2,,\ldots,l_i\}|=1$, segue que

$$A_{l_1}+A_{l_2}+\cdots+A_{l_{i-1}}+A_m=(i-1)PQ+tPQ=(t+i-1)PQ$$

ou

$$\begin{aligned}A_{l_1}+A_{l_2}+\cdots+A_{l_{i-1}}+A_{m+1} &= (i-1)PQ+P\left((1-t)I_n+\sum_{j=1}^{s} e_{j(j+1)}\right)Q\\ &= P((i-1)I_n)Q+P\left((1-t)I_n+\sum_{j=1}^{s} e_{j(j+1)}\right)Q\\ &= P\left((i-1)I_n+(1-t)I_n+\sum_{j=1}^{s} e_{j(j+1)}\right)Q\\ &= P\left((i-t)I_n+\sum_{j=1}^{s} e_{j(j+1)}\right)Q,\end{aligned}$$

onde $i\in\{1,\ldots,m\}$. Como $t\in\mathbb{K}\setminus\{0,1,\ldots,m-1\}$, tem-se $1-t\notin\{0,1,\ldots,m-1\}$. Com efeito, se $1-t\in\{0,1,\ldots,m-1\}$, como $t\neq 0,1$, então existiria $k\in\{2,\ldots,m-1\}$ de modo que $(1-t)1+k1=m1=0$, acarretando que $t=1+k\in\{0,1,\ldots,m-1\}$, o que seria uma contradição. Logo, segue que $t+i-1\neq m$, e $(1-t)+(i-1)\neq m$, donde concluímos, respectivamente, que $(t+i-1)PQ\in GL_n(\mathbb{K})$ e $(i-t)I_n+\sum_{j=1}^{s} e_{j(j+1)}\in GL_n(\mathbb{K})$, em outras palavras, que as matrizes $A_{l_1}+A_{l_2}+\cdots+A_{l_{i-1}}+A_m$ e $A_{l_1}+A_{l_2}+\cdots+A_{l_{i-1}}+A_{m+1}$ estão em $GL_n(\mathbb{K})$, para $i\in\{1,2,\ldots,m\}$.

Por fim, caso $\{m, m+1\} \subseteq \{l_1, l_2, , \ldots, l_i\}$, com $i \in \{2, 3, \ldots, m\}$, temos

$$\begin{aligned} A_{l_1} + A_{l_2} + \cdots + A_{l_{i-2}} + A_m + A_{m+1} &= (i-2)PQ + tPQ + P\left((1-t)I_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q \\ &= P\left((i-1)I_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q, \end{aligned}$$

com $i \in \{1, 2, \ldots, m\}$. Sendo $i-1 \neq m$, segue que $P\left((i-1)I_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q \in GL_n(\mathbb{K})$. Além disso, não é difícil ver que

$$A = \sum_{i=1}^{m+1} A_i.$$

Por último, suponha que $|\mathbb{K}| \geq 2^m$. Provaremos, por indução em m, que existem elementos $x_1, x_2, \ldots, x_m$ em $\mathbb{K}^*$ tais que $x_{l_1} + x_{l_2} + \cdots + x_{l_k} \in \mathbb{K}^*$, para cada $k \in \{1, 2, \ldots, m\}$ e para qualquer sequência da forma $1 \leq l_1 < \ldots < l_k \leq m$. Ora, para $m = 2$ tome $x_1 = 1$ e $x_2 \in \mathbb{K} \setminus \{0, -1\}$. Veja que existe um tal elemento x_2, pois $|\mathbb{K}| \geq 2^2 = 4$. Nestas condições, $x_1, x_2, x_1 + x_2 \in \mathbb{K}^*$.

Sendo assim, a hipótese de indução nos permite afirmar que, para todo corpo cuja ordem é maior ou igual a 2^{m-1}, existem elementos não nulos x_1, x_2, $\ldots$, x_{m-1} neste mesmo corpo base de modo que $x_{l_1} + x_{l_2} + \cdots + x_{l_k}$ seja não nulo, para cada $k \in \{1, 2, \ldots, m-1\}$ e para qualquer sequência da forma $1 \leq l_1 < \ldots < l_k \leq m-1$. Em particular, tal afirmação é válida para o corpo $\mathbb{K}$ que estamos supondo, uma vez que $|\mathbb{K}| \geq 2^m > 2^{m-1}$. Agora, considere

$$S = \left\{-(x_{l_1} + x_{l_2} + \cdots + x_{l_k}) \mid 1 \leq k \leq m-1, 1 \leq l_1 < \ldots < l_k \leq m-1\right\} \cup \{0\}.$$

Observe que S contém no máximo 2^{m-1} elementos. Dessa forma, existe $x_m \in \mathbb{K} \setminus S$ tal que $x_m \in \mathbb{K}^*$ e

$$x_{l_1} + x_{l_2} + \cdots + x_{l_k} + x_m \neq 0,$$

ou seja, $x_{l_1} + x_{l_2} + \cdots + x_{l_k} + x_m \in \mathbb{K}^*$ para cada $k \in \{1, 2 \ldots, m-1\}$ e qualquer sequência da forma $1 \leq l_1 < \ldots < l_k \leq m-1$. Em outras palavras, $x_{l_1} + x_{l_2} + \cdots + x_{l_k} \in \mathbb{K}^*$ para cada $k \in \{1, 2 \ldots, m\}$ e qualquer sequência da forma $1 \leq l_1 < \cdots < l_k \leq m$, concluindo o processo indutivo.

Por fim, defina $A_i = x_i PQ$, para $i \in \{1, 2, \ldots, m\}$, e

$$A_{m+1} = P\left(-(x_1 + x_2 + \cdots + x_m)I_n + \sum_{j=1}^{s} e_{j(j+1)}\right)Q.$$

Não é difícil observar nestas condições que

$$A = \sum_{i=1}^{m+1} A_i,$$

o que finaliza a demonstração. ■

De posse de todos os resultados mencionados até aqui, temos todas as peças necessárias para provar o resultado principal deste capítulo. Além do que já foi dito, também dedicaremos a próxima seção a fazer comentários adicionais.

4.2 Resultado Principal e Comentários Adicionais

Abriremos a seção com o enunciado e a prova do resultado principal deste capítulo.

Teorema 4.6. *Sejam m e n números naturais ≥ 1. Considere $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ uma aplicação m-aditiva tal que $G(x,x,\ldots,x) = 0$, para todo $x \in GL_n(\mathbb{K})$. Então, $G(x,x,\ldots,x) = 0$, para todo $x \in M_n(\mathbb{K})$, se vale alguma das condições:*

i. char $\mathbb{K} = 0$;

ii. char $\mathbb{K} > m$;

iii. char $\mathbb{K} = m$ e $|\mathbb{K}| > m$;

iv. $|\mathbb{K}| \geq 2^m$.

Demonstração. Para obtermos o resultado desejado é suficiente provarmos que $\delta_1(A) = 0_n$, para qualquer matriz singular $A \in M_n(\mathbb{K})$. Com efeito, o Lema 4.5 implica que dada A uma matriz singular em $M_n(K)$, existem $A_1, A_2, \ldots, A_{m+1} \in M_n(\mathbb{K})$ tais que $A_{l_1} + A_{l_2} + \cdots + A_{l_i} \in GL_n(\mathbb{K})$, para cada $i \in \{1,2,\ldots,m\}$ e qualquer sequência $1 \leq l_1 < l_2 < \cdots < l_i \leq m+1$, e $A = \sum_{i=1}^{m+1} A_i$. Deste modo, segue do Lema 4.4 que $\delta_i(A_{l_1} + A_{l_2} + \cdots + A_{l_i}) = 0$, para cada $i \in \{1,2,\ldots,m\}$ e qualquer sequência $1 \leq l_1 < l_2 < \cdots < l_i \leq m+1$. Pela definição de δ_k e pelo Corolário 4.3, tem-se que

$$\delta_1(A) = \delta_1\left(\sum_{i=1}^{m+1} A_i\right) = \sum_{i=1}^{m} \sum_{1 \leq l_1 < \cdots < l_i \leq m+1} \delta_i(A_{l_1}, A_{l_2}, \ldots, A_{l_i}) = 0.$$

Com isso, concluímos que $G(e_{ij}, \ldots, e_{ij}) = 0$, para quaisquer $i, j \in \{1, \ldots, n\}$. Por conseguinte, obtemos que $G(A, \ldots, A) = 0$ para toda matriz $A \in M_n(\mathbb{K})$. ■

Observe que a hipótese de que *char* $\mathbb{K} \neq 0$ livre das restrições a m e a quantidade de elementos de $\mathbb{K}$ não vale em geral. Vejamos os exemplos abaixo.

Exemplo 4.7. *Considere p um número primo e o corpo de p elementos $\mathbb{Z}_p$. Considere também $M_2(\mathbb{Z}_p)$ e $G : M_2(\mathbb{Z}_p)^{2(p-1)} \to M_2(\mathbb{Z}_p)$ dada por*

$$G(x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1}) = \prod_{i=1}^{p-1} (e_{11}x_ie_{11} + ie_{12}x_ie_{21})(e_{11}y_ie_{21} + ie_{12}y_ie_{11}).$$

Vamos provar neste exemplo que G *é uma aplicação multiaditiva tal que* $G(x,x,\ldots,x)=0$, *para todo* $x\in GL_2(\mathbb{Z}_p)$, *mas* $G(x_0,x_0,\ldots,x_0)\neq 0$ *para* $x_0=e_{11}+e_{12}$.

De fato, não é difícil ver que G *é multiaditiva. Agora, considere*

$$x=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2(\mathbb{Z}_p).$$

Outra forma de visualizar a matriz x *é escrevê-la na forma* $x=ae_{11}+be_{12}+ce_{21}+de_{22}$. *Observe que*

$$G(x,\ldots,x)=\prod_{i=1}^{p-1}(e_{11}xe_{11}+ie_{12}xe_{21})(e_{11}xe_{21}+ie_{12}xe_{11}),$$

e como

- $e_{11}(ae_{11}+be_{12}+ce_{21}+de_{22})e_{11}=ae_{11}$;
- $ie_{12}(ae_{11}+be_{12}+ce_{21}+de_{22})e_{21}=ide_{11}$;
- $e_{11}(ae_{11}+be_{12}+ce_{21}+de_{22})e_{21}=be_{11}$;
- $ie_{12}(ae_{11}+be_{12}+ce_{21}+de_{22})e_{11}=ice_{11}$,

obtemos

$$\begin{aligned} G(x,\ldots,x) &= \prod_{i=1}^{p-1}(ae_{11}+ide_{11})(be_{11}+ice_{11}) \\ &= \prod_{i=1}^{p-1}(a+id)(b+ic)e_{11}. \end{aligned}$$

Se $x\in GL_2(\mathbb{Z}_p)$, *então* $ad\neq 0$ *ou* $bc\neq 0$. *Sem perda de generalidade podemos supor que* $ad\neq 0$, *donde segue que* a *e* d *são não nulos. Dessa forma, existe um* $i\in\{1,2,\ldots,p-1\}$ *tal que* $a+id=0$, *haja visto que qualquer* $x\in\mathbb{Z}_p$, *não nulo, é gerador do grupo aditivo* $\mathbb{Z}_p$, *isto é,* $\mathbb{Z}_p=\{nx\mid n\in\{0,1,2,\ldots,p-1\}\}$. *Em particular, dados elementos* a *e* d *em* $\mathbb{Z}_p^*$, *existe um tal* i *(também em* $\mathbb{Z}_p^*$*) satisfazendo* $id=-a$. *Deste modo, segue que* $G(x,\ldots,x)=0$ *para toda* $x\in GL_2(\mathbb{Z}_p)$. *No entanto,* $G(x,\ldots,x)=0$ *não vale para toda matriz de* $M_2(\mathbb{Z}_p)$, *basta ver que* $G(x_0,x_0,\ldots,x_0)=e_{11}$, *para* $x_0=e_{11}+e_{12}$.

Exemplo 4.8. *Neste segundo exemplo, considere a aplicação* $G\colon M_2(\mathbb{K})^2\to M_2(\mathbb{K})$ *dada por*

$$G(x_1,x_2)=(e_{11}x_1e_{11})(e_{12}x_2e_{21})-(e_{11}x_1e_{21})(e_{12}x_2e_{11}).$$

Notemos que G *é uma aplicação 2-aditiva. Além disso, observamos que dada uma matriz* $x=ae_{11}+be_{12}+ce_{21}+de_{22}$, *temos:*

$$G(x,x)=(e_{11}xe_{11})(e_{12}xe_{21})-(e_{11}xe_{21})(e_{12}xe_{11})$$

em que

- $e_{11}xe_{11} = e_{11}(ae_{11} + be_{12} + ce_{21} + de_{22})e_{11} = ae_{11}$;
- $e_{12}xe_{21} = e_{12}(ae_{11} + be_{12} + ce_{21} + de_{22})e_{21} = de_{11}$;
- $e_{11}xe_{21} = e_{11}(ae_{11} + be_{12} + ce_{21} + de_{22})e_{21} = be_{11}$;
- $e_{12}xe_{11} = e_{12}(ae_{11} + be_{12} + ce_{21} + de_{22})e_{11} = ce_{11}$,

isto é,

$$G(x,x) = (ae_{11})(de_{11}) - (be_{11})(ce_{11}) = (ad)e_{11} - (bc)e_{11} = (ad - bc)e_{11} = \det(x)e_{11},$$

onde $\det(x)$ *denota o determinante da matriz* x.

Nestas condições, segue que $G(x,x) = 0$ *para qualquer matriz singular* $x \in M_2(\mathbb{K})$. *Entretanto,* $G(x,x) \neq 0$, *para qualquer matriz* $x \in GL_2(\mathbb{K})$, *uma vez que* $\det(x) \neq 0$ *e* e_{11} *é uma matriz não nula.*

Em resumo, os exemplos anteriores mostram que, se nenhuma das condições descritas no Teorema 4.7 ocorrer, então o resultado é falso. Isso demonstra como o resultado possui uma caracterização completa sobre a descrição de matrizes invertíveis. Em outras palavras, o Exemplo 4.7 é um contraexemplo para o Teorema 4.6 quando char $\mathbb{K} \leq m$ ou $|\mathbb{K}| < 2^m$. Escolhendo $p = 2$, o Exemplo 4.7 torna-se um contraexemplo para o Teorema 4.6 quando char $\mathbb{K} = m$ e $|\mathbb{K}| = m$. Já o Exemplo 4.8 nos mostra que o traço de uma aplicação multiaditiva que se anula no conjunto de matrizes singulares nem sempre é uma aplicação nula.

Para concluir esta seção, apresentaremos uma demonstração alternativa do resultado exposto no Teorema 3.14, utilizando o Teorema 4.6 como base. Para deixar o texto o mais completo possível, enunciaremos o resultado novamente e, em seguida, procederemos com a nova prova.

Teorema 4.9 (Enunciado do Teorema 3.14)**.** *Sejam* $\mathbb{K}$ *um corpo e* n *e* m *inteiros satisfazendo* $n > m > 1$. *Tome uma aplicação m-aditiva* $G\colon M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ *tal que*

$$[G(x,x,\ldots,x),x] = 0,\ \forall x \in GL_n(\mathbb{K}).$$

Além disso, assuma que char $\mathbb{K} = 0$ *ou char* $\mathbb{K} \geq m+1$, *e que* $|\mathbb{K}| \geq m^2 + 2m + 3$. *Então, existem* $\mu_0 \in \mathcal{Z}$ *e* $\mu_i : M_n(\mathbb{K}) \to \mathcal{Z}$, *tais que cada* μ_i *é o traço de uma aplicação i-aditiva para* $i \in \{1,\ldots,m\}$ *e*

$$G(x,\ldots,x) = \mu_0 x^m + \mu_1(x)x^{m-1} + \cdots + \mu_{m-1}(x)x + \mu_m(x),\ \forall x \in M_n(\mathbb{K}).$$

Aqui $\mathcal{Z}$ *denota o centro* $\mathbb{K} \cdot I_n$ *de* $M_n(\mathbb{K})$, *onde* I_n *é a matriz identidade de ordem* n.

Demonstração. Defina $M(x_1,\ldots,x_m,x_{m+1}) = [G(x_1,\ldots,x_m),x_{m+1}]$. Dado o bom comportamento do comutador com relação à adição da álgebra de matrizes $M_n(\mathbb{K})$, segue que M é uma aplicação $(m+1)$-aditiva. Desde que, por hipótese do Teorema 3.14, temos $[G(x,\ldots,x),x] = 0$, para toda $x \in GL_n(\mathbb{K})$, segue-se da definição de M que $M(x,x,\ldots,x) = 0$, para toda matriz $x \in GL_n(\mathbb{K})$. Além disso, temos também nas hipóteses que vale uma das seguintes condições

- *char* $\mathbb{K} = 0$ ou *char* $\mathbb{K} > m+1$;
- *char* $\mathbb{K} = m+1$ e $|\mathbb{K}| > m+1$.

O último item pode ser válido, já que $|\mathbb{K}| \geq (m+1)^2 + 2 > (m+1)$. Aplicando o Teorema 4.6, $M(x,x,\ldots,x) = 0$ para toda matriz $x \in M_n(\mathbb{K})$, ou seja, G é uma aplicação comutante. Como $M_n(\mathbb{K})$ não é algébrica de grau menor do que ou igual m, pois $n > m > 1$, segue do Teorema 3.10 o resultado desejado. ■

APÊNDICE $\mathcal{A}$

Apêndice

A.1 Provas de Resultados via Indução

Nesta seção, achamos por bem realizar algumas demonstrações para identidades que envolvem aplicações $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ que são m-aditivas e simétricas, por meio do processo de indução finita. Vamos a elas:

Proposição A.1. *Sejam $n > m > 1$ naturais e $\mathbb{K}$ um corpo, com char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$. Considere s o menor número par tal que $s \geq m$, isto é, ou $s = m$, se m é par, ou $s = m+1$, se m é ímpar. Seja $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ uma aplicação m-aditiva e simétrica. Para cada $a \in \{1, \ldots, \frac{s}{2}\}$ defina $y_a = az + u \in M_n(\mathbb{K})$, com $z, u \in M_n(\mathbb{K})$. Então, vale:*

$$G(y_a, \ldots, y_a) = \sum_{\zeta=0}^{m} a^{m-\zeta} \binom{m}{\zeta} G(\underbrace{z, \ldots, z}_{m-\zeta}, \underbrace{u, \ldots, u}_{\zeta}).$$

Demonstração. Provaremos por indução em m que a igualdade é válida. De fato, para $m = 1$ tem-se

$$\begin{aligned} G(y_a) = G(az+u) = G(az) + G(u) &= aG(z) + G(u) \\ &= a^{1-0}\binom{1}{0}G(z) + a^{1-1}\binom{1}{1}G(u). \end{aligned}$$

Para $m = 2$ tem-se:

$$\begin{aligned}G(y_a, y_a) = G(az+u, az+u) &= G(az, az+u) + G(u, az+u)\\ &= G(az, az) + G(az, u) + G(u, az) + G(u, u)\\ &= a^2 G(z, z) + aG(z, u) + aG(u, z) + G(u, u).\end{aligned}$$

Sendo G simétrica, vale $G(z, u) = G(u, z)$, donde

$$\begin{aligned}G(y_a, y_a) &= a^2 G(z, z) + 2aG(z, u) + G(u, u)\\ &= a^{2-0}\binom{2}{0}G(z, z) + a^{2-1}\binom{2}{1}G(z, u) + a^{2-2}\binom{2}{2}G(u, u).\end{aligned}$$

Então, suponhamos que tal igualdade seja válida para aplicações $(m-1)$-aditivas, isto é,

$$G(\underbrace{y_a, \ldots, y_a}_{m-1}) = \sum_{\zeta=0}^{m-1} a^{(m-1)-\zeta}\binom{m-1}{\zeta} G(\underbrace{z, \ldots, z}_{m-1-\zeta}, \underbrace{u, \ldots, u}_{\zeta}).$$

Provaremos que a igualdade vale para $G(\underbrace{y_a, \ldots, y_a}_{m})$, uma aplicação m-aditiva. De fato, note que para $y \in M_n(\mathbb{K})$ fixo, a m-aditiva $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ induz uma aplicação $(m-1)$-aditiva $\overline{G} : M_n(\mathbb{K})^{m-1} \to M_n(\mathbb{K})$ dada por $\overline{G}(x_1, \ldots, x_{m-1}) = G(y, x_1, \ldots, x_{m-1})$. Desta forma, considerando as $(m-1)$-aditivas

$$G_1(x_1, \ldots, x_{m-1}) = G(az, x_1, \ldots, x_{m-1}) \quad \text{e} \quad G_2(x_1, \ldots, x_{m-1}) = G(u, x_1, \ldots, x_{m-1})$$

observe que

$$\begin{aligned}G(\underbrace{y_a, \ldots, y_a}_{m}) &= G(az, \underbrace{y_a, \ldots, y_a}_{m-1}) + G(u, \underbrace{y_a, \ldots, y_a}_{m-1})\\ &= G_1(\underbrace{y_a, \ldots, y_a}_{m-1}) + G_2(\underbrace{y_a, \ldots, y_a}_{m-1})\\ &= \sum_{\zeta=0}^{m-1} a^{(m-1)-\zeta}\binom{m-1}{\zeta} G(az, \underbrace{z, \ldots, z}_{m-1-\zeta}), \underbrace{u, \ldots, u}_{\zeta}\\ &+ \sum_{\zeta=0}^{m-1} a^{(m-1)-\zeta}\binom{m-1}{\zeta} G(u, \underbrace{z, \ldots, z}_{m-1-\zeta}, \underbrace{u, \ldots, u}_{\zeta})\end{aligned}$$

uma vez que G_1 e G_2 são $m-1$-aditivas e podemos utilizar a hipótese de indução. Daí,

$$\begin{aligned}
G(y_a,\ldots,y_a) = {} & a^{m-1}\binom{m-1}{0}G(az,z,\ldots,z)+a^{m-2}\binom{m-1}{1}G(az,z,\ldots,z,u)\\
&+a^{m-3}\binom{m-1}{2}G(az,z,\ldots,z,u,u)+\cdots+a\binom{m-1}{m-2}G(az,z,u,\ldots,u)\\
&+a^{0}\binom{m-1}{m-1}G(az,u,\ldots,u)+a^{m-1}\binom{m-1}{0}G(u,z,\ldots,z)\\
&+a^{m-2}\binom{m-1}{1}G(u,z,\ldots,z,u)+\cdots+a^{2}\binom{m-1}{m-3}G(u,z,z,u,\ldots,u)\\
&+a^{1}\binom{m-1}{m-2}G(u,z,u,\ldots,u)+a^{0}\binom{m-1}{m-1}G(u,u,\ldots,u).
\end{aligned}$$

Agora, reordenando a soma de maneira conveniente, tem-se

$$\begin{aligned}
G(y_a,\ldots,y_a) = {} & a^{m-1}\binom{m-1}{0}G(az,z,\ldots,z)\\
&+\left[a^{m-2}\binom{m-1}{1}G(az,z,\ldots,z,u)+a^{m-1}\binom{m-1}{0}G(u,z,\ldots,z)\right]\\
&+\left[a^{m-3}\binom{m-1}{2}G(az,z,\ldots,z,u,u)+a^{m-2}\binom{m-1}{1}G(u,z,\ldots,z,u)\right]+\cdots\\
&+\left[a\binom{m-1}{m-2}G(az,z,u,\ldots,u)+a^{2}\binom{m-1}{m-3}G(u,z,z,u,\ldots,u)\right]\\
&+\left[a^{0}\binom{m-1}{m-1}G(az,u,\ldots,u)+a^{1}\binom{m-1}{m-2}G(u,z,u,\ldots,u)\right]\\
&+a^{0}\binom{m-1}{m-1}G(u,u,\ldots,u).
\end{aligned}$$

Sendo assim, utilizando o fato de G ser simétrica e m-aditiva, obtemos

$$\begin{aligned}
G(y_a,\ldots,y_a) = {} & (a^{m-1}\cdot a)G(z,z,\ldots,z)\\
&+\left[(m-1)(a^{m-2}\cdot a)G(z,z,\ldots,z,u)+a^{m-1}G(z,\ldots,z,u)\right]\\
&+\left[\frac{(m-1)(m-2)}{2}(a^{m-3}\cdot a)G(z,z,\ldots,z,u,u)+(m-1)a^{m-2}G(z,\ldots,z,u,u)\right]\\
&+\cdots+\left[(m-1)(a\cdot a)G(z,z,u,\ldots,u)+\frac{(m-1)(m-2)}{2}a^{2}G(z,z,u,u,\ldots,u)\right]\\
&+\left[aG(z,u,\ldots,u)+(m-1)aG(z,u,\ldots,u)\right]+G(u,u,\ldots,u)
\end{aligned}$$

ou seja,

$$\begin{aligned}
G(y_a,\ldots,y_a) &= a^m G(z,z,\ldots,z) + \left[(m-1)a^{m-1}G(z,z,\ldots,z,u) + a^{m-1}G(z,\ldots,z,u)\right] \\
&+ \left[\frac{(m-1)(m-2)}{2}a^{m-2}G(z,z,\ldots,z,u,u) + (m-1)a^{m-2}G(z,\ldots,z,u,u)\right] + \cdots \\
&+ \left[(m-1)a^2G(z,z,u,\ldots,u) + \frac{(m-1)(m-2)}{2}a^2G(z,z,u,u,\ldots,u)\right] \\
&+ m\cdot aG(z,u,\ldots,u) + G(u,u,\ldots,u) \\
&= a^m G(z,z,\ldots,z) + ma^{m-1}G(z,z,\ldots,z,u) + \frac{m(m-1)}{2}\cdot a^{m-2}G(z,z,\ldots,z,u,u) + \\
&\cdots + \frac{m(m-1)}{2}\cdot a^2G(z,z,u,u,\ldots,u) + m\cdot aG(z,u,\ldots,u) + G(u,u,\ldots,u) \\
&= a^m\binom{m}{0}G(z,z,\ldots,z) + a^{m-1}\binom{m}{1}G(z,z,\ldots,z,u) \\
&+ a^{m-2}\binom{m}{2}G(z,z,\ldots,z,u,u) + \cdots + a^2\binom{m}{m-2}G(z,z,u,u,\ldots,u) \\
&+ a\binom{m}{m-1}G(z,u,\ldots,u) + \binom{m}{m}G(u,u,\ldots,u) \\
&= \sum_{\zeta=0}^{m} a^{m-\zeta}\binom{m}{\zeta}G(\underbrace{z,\ldots,z}_{m-\zeta},\underbrace{u,\ldots,u}_{\zeta}),
\end{aligned}$$

como queríamos demonstrar. ■

A próxima proposição pode ser obtida como consequência da Proposição A.1 tomando $y_{-a} = -az + u = a(-z) + u$, mas por cortesia, faremos a demonstração similar ao que foi feito anteriormente.

Proposição A.2. *Sejam $n > m > 1$ naturais e $\mathbb{K}$ um corpo, com char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$. Considere s o menor número par tal que $s \geq m$, isto é, ou $s = m$, se m é par, ou $s = m+1$, se m é ímpar. Seja $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ uma aplicação m-aditiva e simétrica. Para cada $a \in \{1,\ldots,\frac{s}{2}\}$ defina $y_{-a} = -az + u \in M_n(\mathbb{K})$, com $z,u \in M_n(\mathbb{K})$. Então, vale:*

$$G(y_{-a},\ldots,y_{-a}) = \sum_{\zeta=0}^{m}(-1)^{m-\zeta}a^{m-\zeta}\binom{m}{\zeta}G(\underbrace{z,\ldots,z}_{m-\zeta},\underbrace{u,\ldots,u}_{\zeta}).$$

Demonstração. Para verificar que a igualdade é válida aplicaremos indução em m. De fato, para $m = 1$ tem-se

$$\begin{aligned}
G(y_{-a}) = G(-az+u) = G(-az) + G(u) &= -aG(z) + G(u) \\
&= (-1)^{1-0}a^{1-0}\binom{1}{0}G(z) + (-1)^{1-1}a^{1-1}\binom{1}{1}G(u).
\end{aligned}$$

Para $m = 2$ temos

$$\begin{aligned} G(y_{-a}, y_{-a}) = G(-az+u, -az+u) &= G(-az, -az+u) + G(u, -az+u) \\ &= G(-az, -az) + G(-az, u) + G(u, -az) + G(u, u) \\ &= (-a)^2 G(z,z) + -aG(z,u) + -aG(u,z) + G(u,u). \end{aligned}$$

Sendo G simétrica, vale $G(z,u) = G(u,z)$, donde

$$\begin{aligned} G(y_{-a}, y_{-a}) &= a^2 G(z,z) + 2(-a)G(z,u) + G(u,u) \\ &= (-1)^{2-0} a^{2-0} \binom{2}{0} G(z,z) + (-1)^{2-1} a^{2-1} \binom{2}{1} G(z,u) + (-1)^{2-2} a^{2-2} \binom{2}{2} G(u,u). \end{aligned}$$

Suponhamos que tal igualdade seja válida para aplicações $(m-1)$-aditivas, isto é,

$$G(\underbrace{y_{-a}, \ldots, y_{-a}}_{m-1}) = \sum_{\zeta=0}^{m-1} (-1)^{(m-1)-\zeta} a^{(m-1)-\zeta} \binom{m-1}{\zeta} G(\underbrace{z, \ldots, z}_{m-1-\zeta}, \underbrace{u, \ldots, u}_{\zeta}).$$

Provaremos que a igualdade vale para $G(\underbrace{y_{-a}, \ldots, y_{-a}}_{m})$, uma aplicação m-aditiva. De fato, note que para $y \in M_n(\mathbb{K})$ fixo, a m-aditiva $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ induz uma aplicação $\overline{G} : M_n(\mathbb{K})^{m-1} \to M_n(\mathbb{K})$ que é $(m-1)$-aditiva dada por $\overline{G}(x_1, \ldots, x_{m-1}) = G(y, x_1, \ldots, x_{m-1})$. Desta forma, considerando as $(m-1)$-aditivas

$$G_1(x_1, \ldots, x_{m-1}) = G(-az, x_1, \ldots, x_{m-1}) \quad \text{e} \quad G_2(x_1, \ldots, x_{m-1}) = G(u, x_1, \ldots, x_{m-1})$$

observe que

$$\begin{aligned} G(\underbrace{y_{-a}, \ldots, y_{-a}}_{m}) &= G(-az, \underbrace{y_{-a}, \ldots, y_{-a}}_{m-1}) + G(u, \underbrace{y_{-a}, \ldots, y_{-a}}_{m-1}) \\ &= G_1(\underbrace{y_{-a}, \ldots, y_{-a}}_{m-1}) + G_2(\underbrace{y_{-a}, \ldots, y_{-a}}_{m-1}) \\ &= \sum_{\zeta=0}^{m-1} (-1)^{(m-1)-\zeta} a^{(m-1)-\zeta} \binom{m-1}{\zeta} G(-az, \underbrace{z, \ldots, z}_{m-1-\zeta}, \underbrace{u, \ldots, u}_{\zeta}) \\ &+ \sum_{\zeta=0}^{m-1} (-1)^{(m-1)-\zeta} a^{(m-1)-\zeta} \binom{m-1}{\zeta} G(u, \underbrace{z, \ldots, z}_{m-1-\zeta}, \underbrace{u, \ldots, u}_{\zeta}), \end{aligned}$$

uma vez que G_1 e G_2 são $(m-1)$-aditivas, as quais podemos utilizar a hipótese de indução.

Logo,

$$\begin{aligned}
G(y_{-a},\dots,y_{-a}) &= (-1)^{m-1}a^{m-1}\binom{m-1}{0}G(-az,z,\dots,z)\\
&+(-1)^{m-2}a^{m-2}\binom{m-1}{1}G(-az,z,\dots,z,u)\\
&+(-1)^{m-3}a^{m-3}\binom{m-1}{2}G(-az,z,\dots,z,u,u)\\
&+\cdots+(-1)a\binom{m-1}{m-2}G(-az,z,u,\dots,u)\\
&+(-1)^{0}a^{0}\binom{m-1}{m-1}G(-az,u,\dots,u)+(-1)^{m-1}a^{m-1}\binom{m-1}{0}G(u,z,\dots,z)\\
&+(-1)^{m-2}a^{m-2}\binom{m-1}{1}G(u,z,\dots,z,u)\\
&+\cdots+(-1)^{2}a^{2}\binom{m-1}{m-3}G(u,z,z,u,\dots,u)\\
&+(-1)^{1}a^{1}\binom{m-1}{m-2}G(u,z,u,\dots,u)+(-1)^{0}a^{0}\binom{m-1}{m-1}G(u,u,\dots,u).
\end{aligned}$$

Agora, reordenando a soma de maneira conveniente, tem-se

$$\begin{aligned}
G(y_{-a},\dots,y_{-a}) &= (-1)^{m-1}a^{m-1}\binom{m-1}{0}G(-az,z,\dots,z)\\
&+\Bigg[(-1)^{m-2}a^{m-2}\binom{m-1}{1}G(-az,z,\dots,z,u)\\
&+(-1)^{m-1}a^{m-1}\binom{m-1}{0}G(u,z,\dots,z)\Bigg]\\
&+\Bigg[(-1)^{m-3}a^{m-3}\binom{m-1}{2}G(-az,z,\dots,z,u,u)\\
&+(-1)^{m-2}a^{m-2}\binom{m-1}{1}G(u,z,\dots,z,u)\Bigg]\\
&+\cdots+\Bigg[(-1)a\binom{m-1}{m-2}G(-az,z,u,\dots,u)\\
&+(-1)^{2}a^{2}\binom{m-1}{m-3}G(u,z,z,u,\dots,u)\Bigg]\\
&+\Bigg[(-1)^{0}a^{0}\binom{m-1}{m-1}G(-az,u,\dots,u)+(-1)^{1}a^{1}\binom{m-1}{m-2}G(u,z,u,\dots,u)\Bigg]\\
&+(-1)^{0}a^{0}\binom{m-1}{m-1}G(u,u,\dots,u).
\end{aligned}$$

Deste modo, utilizando o fato de G ser simétrica e m-aditiva, obtemos

$$\begin{aligned}
G(y_{-a},\ldots,y_{-a}) &= (-1)^m(a^m)G(z,z,\ldots,z)\\
&+\left[(m-1)(-1)^{m-1}a^{m-1}G(z,\ldots,z,u)+(-1)^m a^{m-1}G(z,\ldots,z,u)\right]\\
&+\left[\frac{(m-1)(m-2)}{2}(-1)^{m-2}a^{m-2}G(z,\ldots,z,u,u)\right.\\
&\left.+(m-1)(-1)^{m-2}a^{m-2}G(z,\ldots,z,u,u)\right]\\
&+\left[(m-1)(-1)^2a^2G(z,z,u,\ldots,u)\right.\\
&\left.+\frac{(m-1)(m-2)}{2}(-1)^2a^2G(z,z,u,u,\ldots,u)\right]\\
&+\cdots+\left[(-1)aG(z,u,\ldots,u)+(m-1)(-1)aG(z,u,\ldots,u)\right]+G(u,u,\ldots,u)
\end{aligned}$$

ou seja,

$$\begin{aligned}
G(y_{-a},\ldots,y_{-a}) &= (-1)^m a^m G(z,z,\ldots,z)+m(-1)^{m-1}a^{m-1}G(z,z,\ldots,z,u)\\
&+\frac{m(m-1)}{2}(-1)^{m-2}a^{m-2}G(z,z,\ldots,z,u,u)+\cdots\\
&+\frac{m(m-1)}{2}(-1)^2a^2G(z,z,u,u,\ldots,u)+m\cdot(-1)aG(z,u,\ldots,u)+G(u,u,\ldots,u)\\
&= (-1)^m a^m G(z,z,\ldots,z)+m(-1)^{m-1}a^{m-1}G(z,z,\ldots,z,u)\\
&+\frac{m(m-1)}{2}\cdot(-1)^{m-2}a^{m-2}G(z,z,\ldots,z,u,u)+\cdots\\
&+\frac{m(m-1)}{2}\cdot(-1)^2a^2G(z,z,u,u,\ldots,u)+m\cdot(-1)aG(z,u,\ldots,u)+G(u,u,\ldots,u)\\
&= (-1)^m a^m\binom{m}{0}G(z,z,\ldots,z)+(-1)^{m-1}a^{m-1}\binom{m}{1}G(z,z,\ldots,z,u)\\
&+(-1)^{m-2}a^{m-2}\binom{m}{2}G(z,z,\ldots,z,u,u)+\cdots\\
&+(-1)^2a^2\binom{m}{m-2}G(z,z,u,u,\ldots,u)+(-1)a\binom{m}{m-1}G(z,u,\ldots,u)\\
&+\binom{m}{m}G(u,u,\ldots,u)\\
&= \sum_{\zeta=0}^{m}(-1)^{(m-1)-\zeta}a^{m-\zeta}\binom{m}{\zeta}G(\underbrace{z,\ldots,z}_{m-\zeta},\underbrace{u,\ldots,u}_{\zeta}),
\end{aligned}$$

como queríamos demonstrar. ■

As proposições seguintes são consequências imediatas da Proposição A.1.

Proposição A.3. *Sejam $n > m > 1$ naturais e $\mathbb{K}$ um corpo, com char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$. Considere s o menor número par tal que $s \geq m$, isto é, ou $s = m$, se m é par, ou $s = m+1$, se m é ímpar. Seja $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ uma aplicação m-aditiva e simétrica. Para cada*

$a \in \{1, \dots, \frac{s}{2}\}$ defina $y_a = akI + b \in M_n(\mathbb{K})$, com $kI, b \in M_n(\mathbb{K})$ e $k \in \mathbb{K} \setminus \{0\}$. Então, vale:

$$G(y_a, \dots, y_a) = \sum_{r=0}^{m} a^r \binom{m}{r} G(\underbrace{kI, \dots, kI}_{r}, b, \dots, b).$$

Proposição A.4. *Sejam $n > m > 1$ naturais e $\mathbb{K}$ um corpo, com char $\mathbb{K} = 0$ ou char $\mathbb{K} \geq m+1$. Considere s o menor número par tal que $s \geq m$, isto é, ou $s = m$, se m é par, ou $s = m+1$, se m é ímpar. Seja $G : M_n(\mathbb{K})^m \to M_n(\mathbb{K})$ uma aplicação m-aditiva e simétrica. Para cada $a \in \{1, \dots, \frac{s}{2}\}$ defina $y_{-a} = -akI + b \in M_n(\mathbb{K})$, com $kI, b \in M_n(\mathbb{K})$ e $k \in \mathbb{K} \setminus \{0\}$. Então, vale:*

$$G(y_{-a}, \dots, y_{-a}) = \sum_{r=0}^{m} (-1)^r a^r \binom{m}{r} G(\underbrace{kI, \dots, kI}_{r}, b, \dots, b).$$

A.2 O Determinante de uma Matriz

A teoria de determinantes é bastante conhecida na Matemática e pode ser desenvolvida por meio de algumas formas distintas que nos levam ao mesmo objeto matemático de interesse. Pode-se encontrar em bons livros que tratam de Álgebra Linear com riquíssimos detalhes. Aqui traremos apenas como um extra para nortearmos nosso trabalho no uso das propriedades envolvendo o determinante de uma matriz. Os detalhes podem ser encontrados no livro *Tópicos de Álgebra*[1], que é uma tradução brasileira de *Topics in Algebra* escrito por I.N. Hernstein.

A seguir, definiremos o determinante de uma matriz e apresentaremos alguns resultados sobre determinantes que fornecem um suporte à linguagem matemática básica em nosso trabalho. Por exemplo, podemos definir matrizes inversíveis e singulares a partir do determinante.

Definição A.5. *Seja $X = (x_{ij})_n \in M_n(\mathbb{K})$. Definimos o determinante de X, denotando por* $\det X$, *como sendo o elemento de $\mathbb{K}$ dado por:*

$$\sum_{\sigma \in S_n} sign(\sigma)(x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{n\sigma(n)})$$

onde $sign(\sigma)$ denota o sinal da permutação $\sigma \in S_n$.

Sendo assim, temos $sign(\sigma) = 1$, se σ for par, ou $sign(\sigma) = -1$, se σ for ímpar. Em resumo, $sign(\sigma) \in \{1, -1\}$. Nestas condições, seja $X \in M_2(\mathbb{K})$ uma matriz da forma

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}.$$

No grupo de permutações S_2, temos as permutações identidade, a qual denotaremos por Id, e a permutação $(1\ 2)$. Sendo Id par, temos $sign(Id) = 1$, e $(1\ 2)$ ímpar, temos $sign(1\ 2) = -1$. Daí,

[1] Veja [13, pág. 337]

temos
$$\det X = x_{11}x_{22} - x_{12}x_{21}.$$

Agora, considere $X \in M_3(\mathbb{K})$ uma matriz da forma
$$X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}.$$

No grupo de permutações S_3, temos as seguintes permutações
$$\{Id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Daí,
$$\begin{aligned} \det X &= x_{11}x_{22}x_{33} - x_{12}x_{21}x_{33} - x_{13}x_{22}x_{31} \\ &\quad - x_{11}x_{23}x_{32} + x_{12}x_{23}x_{31} + x_{13}x_{21}x_{32}, \end{aligned}$$

pois $1 = sign(Id) = sign(1\ 2\ 3) = sign(1\ 3\ 2)$ e $-1 = sign(1\ 2) = sign(1\ 3) = sign(2\ 3)$. Reordenando o segundo membro da igualdade, temos
$$\det X = [(x_{11}x_{22}x_{33}) - (x_{11}x_{23}x_{32})] + [(x_{12}x_{23}x_{31}) - (x_{12}x_{21}x_{33})] + [(x_{13}x_{21}x_{32}) - (x_{13}x_{22}x_{31})],$$

isto é, $\det X = [x_{11}(x_{22}x_{33} - x_{23}x_{32})] + [x_{12}(x_{23}x_{31} - x_{21}x_{33})] + [x_{13}(x_{21}x_{32} - x_{22}x_{31})]$, donde obtemos
$$\det X = \left[x_{11} \det \begin{pmatrix} x_{22} & x_{23} \\ x_{32} & x_{33} \end{pmatrix} \right] + \left[x_{12}(-1) \det \begin{pmatrix} x_{21} & x_{23} \\ x_{31} & x_{33} \end{pmatrix} \right] + \left[x_{13} \det \begin{pmatrix} x_{21} & x_{22} \\ x_{31} & x_{32} \end{pmatrix} \right].$$

Veja que o determinante da matriz X, de ordem 3, foi obtido a partir de subdeterminantes de matrizes de ordem 2 definidas a partir da escolha de um elemento da linha 1. Fazendo uma reordenação de forma conveniente, podemos realizar o mesmo procedimento escolhendo uma outra linha da matriz, ou mesmo uma coluna. Nestas condições, perceba que o determinante não se altera. Convencionando
$$\begin{pmatrix} x_{22} & x_{23} \\ x_{32} & x_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad \begin{pmatrix} x_{21} & x_{23} \\ x_{31} & x_{33} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad \begin{pmatrix} x_{21} & x_{22} \\ x_{31} & x_{32} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

e denotando
$$\Delta_{11} = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad \Delta_{12} = \det \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad \Delta_{13} = \det \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

temos

$$\det X = x_{11}(-1)^{1+1}\Delta_{11} + x_{12}(-1)^{1+2}\Delta_{12} + x_{13}(-1)^{1+3}\Delta_{13}.$$

Essa ideia se repete por meio de uma recorrência para o cálculo do determinante de matrizes de ordem n e é chamada de *Desenvolvimento de Laplace*. De maneira geral, temos para uma matriz $X = (x_{ij})_{n\times n}$, com $1 \leq i, j \leq n$, que vale

$$\det X = \sum_{j=1}^{n} x_{i_0 j}(-1)^{i_0+j}\Delta_{i_0 j}, \tag{A.1}$$

para $i_0 \in \{1,\dots,n\}$ fixado e $\Delta_{i_0 j}$ sendo o determinante da matriz de ordem $n-1$, obtida excluindo-se a linha i_0 e a coluna j da matriz $X = (x_{ij})_{n\times n}$. A mesma ideia segue fazendo a escolha de $j_0 \in \{1,\dots,n\}$ fixo e fazendo i variar em $\{1,\dots,n\}$.

Lema A.6. *O determinante de uma matriz triangular é o produto dos elementos de sua diagonal principal.*

Teorema A.7. *Sejam $X, Y \in M_n(\mathbb{K})$. Então,* $\det(XY) = (\det X)(\det Y)$.

Corolário A.8. *Se $X \in GL_n(\mathbb{K})$, então* $\det X \neq 0$ *e* $\det X^{-1} = (\det X)^{-1}$.

Lema A.9. *Seja A^t a matriz transposta de A. Então,* $\det A^t = \det A$.

Definição A.10. *Dizemos que uma matriz $X \in M_n(\mathbb{K})$ é invertível se existe $Y \in M_n(\mathbb{K})$ tal que $XY = YX = I_n$, onde I_n denota a matriz identidade de ordem n. Neste caso, denotamos $Y = X^{-1}$.*

Definição A.11. *Diremos que uma matriz $X \in M_n(\mathbb{K})$ é uma matriz singular se não for invertível.*

Pelas propriedades para determinantes, temos a seguinte caracterização para matrizes invertíveis:

Teorema A.12. *Uma matriz A é inversível se, e somente se,* $\det A \neq 0$.

Dessa forma, dizer que X é uma matriz singular é equivalente a dizer que $\det X = 0$. Das conversas de Álgebra Linear básica, temos a seguinte definição de nulidade e posto de uma aplicação linear.

Definição A.13. *Sendo $T : V \to W$ uma transformação linear, definimos:*

(a) a nulidade de T como sendo $\dim \ker T$.

(b) o posto de T como sendo $\dim\ Im\ T$.

Essa definição pode ser entendida para matrizes. Diremos que *o posto de uma matriz A* em $M_n(\mathbb{K})$ é o número de linhas não nulas da matriz na forma escada que é linha equivalente à matriz A.

A.3 O Determinante de uma Matriz de Vandermonde

Utilizamos as noções de determinante para uma matriz de Vandermonde no Capítulo 3 na Proposição 3.12 e no Teorema 3.14. Por isso, achamos interessante trazer o estudo sobre o determinante de uma matriz de Vandermonde.

Definição A.14. *Dizemos que uma matriz quadrada X, de ordem n, é uma matriz de Vandermonde se tem a forma*

$$X = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-2} & x_{n-1}^{n-1} \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} & x_n^{n-1} \end{pmatrix}.$$

Teorema A.15. *Se X é uma matriz de Vandermonde, então*

$$\det X = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Demonstração. Faremos a demonstração por indução em n, a ordem da matriz X. Ora, não há o que fazer se $n = 1$. Veja que se $n = 2$, tem-se

$$X = \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \end{pmatrix},$$

donde $\det(X) = x_2 - x_1$. Suponhamos que, para toda matriz de Vandermonde X, de ordem $n-1$, tenha-se

$$\det X = \prod_{1 \leq i < j \leq n-1} (x_j - x_i).$$

Nestas condições, tome X uma matriz de Vandermonde de ordem n dada por

$$X = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}.$$

Aplicando as noções de operações elementares com linhas e o desenvolvimento de Laplace, veja que

$$\det(X) = \det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$
$$= \det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 0 & x_2-x_1 & x_2^2-x_1^2 & \cdots & x_2^{n-1}-x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & x_{n-1}-x_1 & x_{n-1}^2-x_1^2 & \cdots & x_{n-1}^{n-1}-x_1^{n-1} \\ 0 & x_n-x_1 & x_n^2-x_1^2 & \cdots & x_n^{n-1}-x_1^{n-1} \end{pmatrix}$$
$$= \det\begin{pmatrix} x_2-x_1 & x_2^2-x_1^2 & \cdots & x_2^{n-1}-x_1^{n-1} \\ x_3-x_1 & x_3^2-x_1^2 & \cdots & x_3^{n-1}-x_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_n-x_1 & x_n^2-x_1^2 & \cdots & x_n^{n-1}-x_1^{n-1} \end{pmatrix}.$$

Sendo assim, das propriedades de determinantes da seção A.2 e utilizando produtos notáveis temos:

$$\det(X) = \det\begin{pmatrix} x_2-x_1 & (x_2-x_1)(x_2+x_1) & \cdots & (x_2-x_1)\left(\sum_{i=0}^{n-2} x_2^{n-2-i}x_1^i\right) \\ x_3-x_1 & (x_3-x_1)(x_3+x_1) & \cdots & (x_3-x_1)\left(\sum_{i=0}^{n-2} x_3^{n-2-i}x_1^i\right) \\ \vdots & \vdots & \ddots & \vdots \\ x_n-x_1 & (x_n-x_1)(x_n+x_1) & \cdots & (x_n-x_1)\left(\sum_{i=0}^{n-2} x_n^{n-2-i}x_1^i\right) \end{pmatrix}$$
$$= \det\left[\begin{pmatrix} x_2-x_1 & 0 & \cdots & 0 \\ 0 & x_3-x_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (x_n-x_1) \end{pmatrix}\begin{pmatrix} 1 & (x_2+x_1) & \cdots & \sum_{i=0}^{n-2} x_2^{n-2-i}x_1^i \\ 1 & (x_3+x_1) & \cdots & \sum_{i=0}^{n-2} x_3^{n-2-i}x_1^i \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (x_n+x_1) & \cdots & \sum_{i=0}^{n-2} x_n^{n-2-i}x_1^i \end{pmatrix}\right],$$

ou seja,

$$
\begin{aligned}
\det(X) &= \left[\prod_{j=2}^{n}(x_j - x_1)\right] \det \begin{pmatrix}
1 & (x_2 + x_1) & \cdots & \sum_{i=0}^{n-2} x_2^{n-2-i} x_1^i \\
1 & (x_3 + x_1) & \cdots & \sum_{i=0}^{n-2} x_3^{n-2-i} x_1^i \\
\vdots & \vdots & \ddots & \vdots \\
1 & (x_n + x_1) & \cdots & \sum_{i=0}^{n-2} x_n^{n-2-i} x_1^i
\end{pmatrix} \\
&= \left[\prod_{j=2}^{n}(x_j - x_1)\right] \det \left[\begin{pmatrix}
1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\
1 & x_3 & x_3^2 & \cdots & x_3^{n-2} \\
\vdots & \vdots & \vdots & & \vdots \\
1 & x_n & x_n^2 & \cdots & x_n^{n-2}
\end{pmatrix} \begin{pmatrix}
1 & x_1 & x_1^2 & \cdots & x_1^{n-2} \\
0 & 1 & x_1 & \cdots & x_1^{n-3} \\
\vdots & \vdots & \vdots & & \vdots \\
0 & 0 & 0 & \cdots & 1
\end{pmatrix} \right] \\
&= \left[\prod_{j=2}^{n}(x_j - x_1)\right] \det \begin{pmatrix}
1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\
1 & x_3 & x_3^2 & \cdots & x_3^{n-2} \\
\vdots & \vdots & \vdots & & \vdots \\
1 & x_n & x_n^2 & \cdots & x_n^{n-2}
\end{pmatrix}.
\end{aligned}
$$

Pela hipótese de indução, segue que

$$
\det \begin{pmatrix}
1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\
1 & x_3 & x_3^2 & \cdots & x_3^{n-2} \\
\vdots & \vdots & \vdots & & \vdots \\
1 & x_n & x_n^2 & \cdots & x_n^{n-2}
\end{pmatrix} = \prod_{2 \le i < j \le n} (x_j - x_i),
$$

donde obtemos que

$$
\begin{aligned}
\det(X) &= \left[\prod_{j=2}^{n}(x_j - x_1)\right] \left[\prod_{2 \le i < j \le n} (x_j - x_i)\right] \\
&= \prod_{1 \le i < j \le n} (x_j - x_i),
\end{aligned}
$$

como queríamos demonstrar. ■

Referências Bibliográficas

[1] M. Brešar. Centralizing mappings and derivations in prime rings. *J. algebra*, 156(2): 385–394, 1993.

[2] M. Brešar. Commuting traces of biadditive mappings, commutativity-preserving mappings and lie mappings. *Transactions of the American Mathematical Society*, 335(2): 525–546, 1993.

[3] M. Brešar. Commuting maps: a survey. *Taiwanese Journal of Mathematics*, 8(3):361–397, 2004.

[4] M. Brešar. *Introduction to noncommutative algebra*. Springer, 2014.

[5] M. Brešar, M. A. Chebotar, and W. S. Martindale. *Functional identities*. Springer Science & Business Media, 2007.

[6] C. Cao and X. Zhang. Additive operators preserving idempotent matrices over fields and applications. *Linear algebra and its applications*, 248:327–338, 1996.

[7] V. Drensky and E. Formanek. *Polynomial identity rings*. Birkhäuser, 2012.

[8] W. Franca. Commuting maps on some subsets of matrices that are not closed under addition. *Linear algebra and its applications*, 437(1):388–391, 2012.

[9] W. Franca. Commuting traces of multiadditive maps on invertible and singular matrices. *Linear and Multilinear Algebra*, 61(11):1528–1535, 2013.

[10] G. Frobenius. *Über die Darstellung der endlichen Gruppen durch lineare Substitutionen. II.:...* Reimer, 1899.

[11] A. Garcia and Y. Lequain. *Elementos de álgebra*. IMPA, Rio de Janeiro, 2001.

[12] A. Giambruno and M. Zaicev. *Polynomial identities and asymptotic methods*. Number 122. American Mathematical Soc., 2005.

[13] I. N. Hernstein, A. P. Bergamasco, and L. J. Monteiro. *Tópicos de álgebra*. 1970.

[14] K. Hoffman, R. Kunze, H. E. Finsterbusch, et al. *Álgebra lineal*. Prentice-Hall Hispanoamericana, 1973.

[15] J. Lambek. *Lectures on rings and modules*, volume 283. American Mathematical Soc., 2009.

[16] S. Lang. *Algebra*, volume 211. Springer Science & Business Media, 2012.

[17] S. Lang. *Introduction to linear algebra*. Springer Science & Business Media, 2012.

[18] P.-H. Lee, T.-L. Wong, J.-S. Lin, and R.-J. Wang. Commuting traces of multiadditive mappings. *Journal of Algebra*, 193(2):709–723, 1997.

[19] C.-K. Li and S. Pierce. Linear preserver problems. *The American Mathematical Monthly*, 108(7):591–605, 2001.

[20] C.-K. Li and N.-K. Tsing. Linear preserver problems: A brief introduction and some special techniques. *Linear algebra and its applications*, 162:217–235, 1992.

[21] S. Pierce, M. Lim, R. Loewy, C.-K. Li, N. Tsing, B. McDonald, and L. Beasley. A survey of linear preserver problems. *Linear and Multilinear Algebra*, 33(1-2):1–129, 1992.

[22] E. C. Posner. Derivations in prime rings. *Proceedings of the American Mathematical Society*, 8(6):1093–1100, 1957.

[23] X. Xu and J. Zhu. Central traces of multiadditive maps on invertible matrices. *Linear and Multilinear Algebra*, 66(7):1442–1448, 2018.