UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

FELIPE BARBOSA CAVALCANTE

Invariantes Separadores de Matrizes

Campinas

2021

Felipe Barbosa Cavalcante

Invariantes Separadores de Matrizes

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Orientador: Artem Lopatin

Este trabalho corresponde à versão final da Tese defendida pelo aluno Felipe Barbosa Cavalcante e orientada pelo Prof. Dr. Artem Lopatin.

Campinas

2021

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

C314i

Cavalcante, Felipe Barbosa, 1993-
Invariantes separadores de matrizes / Felipe Barbosa Cavalcante. – Campinas, SP : [s.n.], 2021.

Orientador: Artem Lopatin.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos invariantes. 2. Invariantes de matrizes. 3. Semi-invariantes de matrizes. 4. Invariantes separadores. I. Lopatin, Artem, 1980-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Separating invariants of matrices
Palavras-chave em inglês:
Invariant theory
Invariants of matrices
Semi-invariants of matrices
Separating invariants
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Artem Lopatin [Orientador]
Alexandre Grichkov
Alexey Kuzmin
Dimas José Gonçalves
Elizaveta Vishnyakova
Saeed Tafazolian
Data de defesa: 15-12-2021
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0003-1959-6978
- Currículo Lattes do autor: http://lattes.cnpq.br/4860284383730149

Tese de Doutorado defendida em 15 de dezembro de 2021 e aprovada

pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). Artem Lopatin

Prof(a). Dr(a). Alexandre Grichkov

Prof(a). Dr(a). Alexey Kuzmin

Prof(a). Dr(a). Dimas José Gonçalves

Prof(a). Dr(a). Elizaveta Vishnyakova

Prof(a). Dr(a). Saeed Tafazolian

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Dedico a minha mãe, Josefa Barboza.

Agradecimentos

Agradeço inicialmente a minha família: a minha filha Saphira por servir de constante fonte de inspiração e estímulo; aos meus pais Josefa e Luis pelo suporte durante os estudos e por tantos sacrifícios feitos, e a minha companheira Vitória por sempre me lembrar que embora nem sempre fácil, continuar é possível.

Também gostaria de agradecer a todos os professores e funcionários do Imecc. Em especial, ao professor: Artem Lopatin, por ter me orientado neste trabalho, bem como por todo auxílio prestado durante o curso inteiro.

Finalmente agradeço aos amigos do curso por todo apoio e incentivo dados e também pela companhia em diversas seções de estudos e momentos de descontração regados a café e boas conversa.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Esta tese é dedicada ao estudo de conjuntos de invariantes separadores minimais da álgebra de invariantes de matrizes nilpotentes 3×3, bem como da álgebra de semi-invariantes de matrizes 2×2. Baseados em conjuntos geradores destas álgebras, construímos explicitamente conjuntos separadores minimais para a álgebra de invariantes de matrizes nilpotentes $\mathcal{O}(n,m)$ para o caso $n = m = 3$, como também estabelecemos limitações para o grau máximo de qualquer conjunto separador minimal da álgebra $\mathcal{O}(n,m)$, quando $n = 3$ e $d \geq 3$. Além disso, obtivemos uma descrição de um conjunto separador minimal para a álgebra de semi-invariantes de matrizes $SI_{(2,2)}(m,p,q)$, quaisquer que sejam $m,p,q \in \mathbb{N}$ não todos nulos.

Palavras-chave: teoria dos invariantes, invariantes de matrizes, semi-invariantes de matrizes, invariantes separadores.

Abstract

This thesis is dedicated to the study of minimal separating invariant sets of the nilpotent matrix invariant algebras 3×3, as well as the matrix semi-invariant algebra 2×2. Based on generator sets of these algebras, we explicitly construct minimal separating sets for the invariant algebra of nilpotent matrices $\mathcal{O}(n,m)$ for the case $n = m = 3$, as well as establishing limitations for the degree maximum of any separating minimal set of the algebra $\mathcal{O}(n,m)$, when $n = 3$ and $d \geq 3$. Furthermore, we obtain a description of a minimal separating set for the algebra of semi-invariant matrices $SI_{(2,2)}(m,p,q)$, whatever $m, p, q \in \mathbb{N}$ not all zeros.

Keywords: invariant theory, matrix invariants, semi-invariants, separating invariants.

Sumário

Introducão

A teoria dos invariantes é um ramo da matemática com uma longa tradição, o qual existem registros datados de pelo menos cento e vinte anos atrás, conforme pode ser visto em trabalhos de alguns nomes como Cayley, Gordan, Jacobi e Sylvester. Embora inicialmente o objetivo desta teoria tenha sido estudar expressões algébricas que não variam (ou variam de maneira determinada) após a aplicação de transformações lineares não degeneradas de variáveis, ao longo do tempo a gama de problemas, e técnicas utilizadas nas suas resoluções, referentes à esta teoria vêm se expandindo e atualmente a teoria dos invariantes, de forma mais geral, estuda a ação de grupos algébricos sobre variedades algébricas. Esta expansão ocasionou uma contribuição mútua entra a teoria dos invariantes e outros ramos da matemática como geometria, álgebra comutativa, combinatória, teoria das representações e etc. Além de diversos resultados nas áreas citadas, também é possível encontrar aplicações da teoria dos invariantes em áreas fora da matemática como física, engenharia e teoria dos grafos.

Desde seu início, um dos problemas que norteou o estudo da teoria dos invariantes é estudar álgebras concretas de invariantes, e obter uma descrição explícita de conjuntos geradores destas álgebras, bem como estabelecer relações entre os invariantes pertencentes a esses conjuntos geradores. Uma outra questão interessante sobre essa temática diz respeito a finitude desses conjuntos de geradores. Diversos matemáticos dedicaram-se a esses problemas, e um dos resultados mais gerais nesse sentido deve-se a Hilbert (para uma demonstração mais moderna deste teorema indicamos ver [15]), o qual garante que a álgebra de invariantes de uma variedade afim, sob a ação de um grupo redutivo G, é finitamente gerada. Contudo, vale a pena destacar que este resultado não é válido para o caso geral em que G é um grupo algébrico qualquer, conforme comprova o contraexemplo estabelecido por Nagata em 1959 (vide [34]). Para exemplos de algumas descrições de conjuntos geradores de álgebras invariantes indicamos as referências [6], [25] [4], [31]. Um outro ponto a esse respeito, é que embora possamos obter diversos resultados uma vez conhecido um conjunto gerador de uma álgebra de invariantes, tal conjunto gerador pode ser bastante grande, díficil de descrever explicitamente, ou até mesmo infinito (no caso de grupos não redutivos). Portanto, surge a pergunta natural: um conjunto menor de invariantes pode ser suficiente para atingir as mesmas (ou semelhantes) propriedades?

Em 2002, Derksen e Kemper (vide [15]) introduziram a noção de invariantes separadores como um conceito "mais fraco" que o conceito de geradores de invariantes uma vez que é de fácil observação que todo conjunto gerador é naturalmente um conjunto separador, embora a recíproca nem sempre seja válida. Portanto, temos um interesse especial nos casos quando algum conjunto separador de invariantes não gera a álgebra de invariantes. Além disso, existem vários resultados semelhantes aos obtidos para geradores de invariantes nos quais é suficiente considerar apenas conjuntos separadores, a título de exemplo: mesmo que um grupo G não seja redutivo, se ele age por automorfismos em uma variedade afim, então existe um subconjunto separador finito contido na álgebra de invariantes $\mathbb{F}[\mathcal{H}]$ (veja [15]). Assim, de modo geral, em certas situações podemos encontrar conjuntos de invariantes separadores finitos, mesmo quando não um existe um conjunto gerador finito para a álgebra de invariantes.

Um outro problema oriundo da finitude de certos conjuntos geradores (ou separadores, respectivamente) de uma álgebra de invariantes $\mathbb{F}[\mathcal{H}]^G$ consiste em obter limitações, ou o valor exato quando possível, para o menor inteiro D tal que o conjunto de todos os invariantes homogêneos de $\mathbb{F}[\mathcal{H}]^G$ com grau $\leq D$ é um conjunto gerador (conjunto separador, respectivamente), o qual é denotado por $\beta(\mathbb{F}[\mathcal{H}]^G)$ ($\beta_{\text{sep}}(\mathbb{F}[\mathcal{H}]^G)$, respectivamente). Este problema foi vastamente estudado e existem diversos resultados nessa linha obtidos para álgebras específicas, como exemplos indicamos os resultados apresentados em [10], [19], [21], [22] e [12].

Denotemos por $M^m_{n_1\times n_2}$ ($\mathcal{N}^m_n$, respectivamente), a soma direta de m cópias do espaço das matrizes $n_1 \times n_2$ sobre $\mathbb{F}$ (da variedade afim $\mathcal{N}$ das matrizes nilpotentes $n \times n$, respectivamente). Consideremos agora as seguintes álgebras de invariantes de matrizes, as quais serão de suma importância nesta tese:

- $S(n,m) = \mathbb{F}[M^m_n]^{GL(n)}$ a álgebra de invariantes de matrizes, onde $GL(n)$ age em M^m_n diagonalmente pela conjugação;
- $\mathcal{O}(n,m) = \mathbb{F}[\mathcal{N}^m_n]^{GL(n)}$ a álgebra de invariantes de matrizes nilpotentes, onde $GL(n)$ age em $\mathcal{N}^m_n$ diagonalmente pela conjugação;
- $R(n,m) = \mathbb{F}[M^m_n]^{SL(n)\times SL(n)}$ a álgebra de invariantes de matrizes, com respeito a ação diagonal bilateral de $SL(n) \times SL(n)$ em M^m_n.
- $SI_{(n_1\times n_2)}(m,p,q) = \mathbb{F}[M^m_{n_1\times n_2} \oplus M^p_{n_1} \oplus M^q_{n_2}]^G$, a álgebra de semi-invariantes de matrizes com respeito a ação diagonal do grupo $G = SL(n_1) \times SL(n_2)$.

Nesta tese iremos descrever um conjunto minimal de geradores e obter um conjunto separador minimal para a álgebra de invariantes $\mathcal{O}(3,3)$, bem como iremos mostrar que sendo $m \geq 2$ então $\beta(\mathcal{O}(3,m)) = \beta_{\mathrm{sep}}(\mathcal{O}(3,m)) = 6$, onde $\mathbb{F}$ é um corpo algebricamente fechado de característica zero, o que será o resultado principal do Capítulo 2 (ver Teorema 2.2.15). Além disso, obteremos a descrição de um conjunto separador minimal para a álgebra de semi-invariantes $SI_{(2\times 2)}(m,p,q)$, onde $\mathbb{F}$ é um corpo algebricamente fechado de característica diferente de 2, o que, junto com noções e conceitos preliminares necessários para esta descrição, irá compor o Capítulo 3 (vide Teorema 3.4.17). Os resultados do Capítulo 2 foram publicados na revista Linear Algebra and Its Applications sob o título "Separating invariants of three nilpotent 3×3 matrices"([10]).

1 Preliminares

Neste capítulo apresentaremos os resultados e conceitos básicos que se farão necessários para o desenvolvimento deste estudo. Trabalharemos as noções de variedades afins, grupos algébricos redutivos, e finalizaremos abordando invariantes e invariantes separadores de matrizes. Além disso também estabeleceremos algumas terminologias e notações, as quais utilizaremos nos capítulos seguintes. No intuito de evitar repetições, $\mathbb{F}$ ira sempre denotar um corpo e todos as álgebras, bem como os espaços vetoriais, serão considerados sobre $\mathbb{F}$.

1.1 Variedades afins

Ao longo desta seção iremos considerar $\mathbb{F}$ um corpo algebricamente fechado e denotaremos por $\mathbb{F}^n$ o espaço vetorial n-dimensional e por $\mathbb{F}[x_1, \cdots, x_n]$ o anel dos polinômios nas variáveis comutativas $x_1, \cdots, x_n$.

Definição 1.1.1. Um subconjunto $\mathcal{H} \subseteq \mathbb{F}^n$ é dito uma variedade afim se existe um conjunto de polinômios $S \subseteq \mathbb{F}[x_1, \cdots, x_n]$, tal que

$$\mathcal{H} = \mathcal{V}(S) = \{(v_1, \cdots, v_n) \in \mathbb{F}^n \mid f(v_1, \cdots, v_n) = 0, \ \forall \ f(x_1, \cdots, x_n) \in S\}.$$

Recordemos que sendo $S \subseteq \mathbb{F}[x_1, \cdots, x_n]$ e J o ideal gerado por S em $\mathbb{F}[x_1, \cdots, x_n]$, definimos o ideal radical de J, denotado por $\sqrt{J}$, como sendo

$$\sqrt{J} = \{f \in \mathbb{F}[x_1, \cdots, x_n] \mid f^p \in J, \text{ para algum } p \in \mathbb{N}\}.$$

Nestas condições, é de fácil verificação que se $\mathcal{H}$ é uma variedade afim tal que $\mathcal{H} = \mathcal{V}(S)$, então $\mathcal{H} = \mathcal{V}(\sqrt{J})$.

Definição 1.1.2. Sejam $\mathcal{H} = \mathcal{V}(S)$ uma variedade afim e $I = \sqrt{J}$, o ideal radical de J, onde J denota o ideal gerado por S em $\mathbb{F}[x_1, \cdots, x_n]$. Então, o anel de coordenadas de $\mathcal{H}$ é o anel quociente

$$\mathbb{F}[\mathcal{H}] = \frac{\mathbb{F}[x_1, \cdots, x_n]}{I}.$$

Observemos que, como uma consequência do teorema dos zeros de Hilbert (Hilbert's Nullstellensatz), podemos identificar o anel de coordenadas $\mathbb{F}[\mathcal{H}]$ como um subconjunto do anel das funções de $\mathcal{H}$ em $\mathbb{F}$, o qual denotaremos por $\mathbb{F}^{\mathcal{H}}$. Assim, os elementos de $\mathbb{F}[\mathcal{H}]$ são chamados de funções regulares em $\mathcal{H}$. Fazemos uso deste conceito para estabelecer a noção de morfismos entre variedades afim, conforme pode ser visto na definição a seguir.

Definição 1.1.3. Sejam $\mathcal{H}$ e $\mathcal{V}$ variedades afins. Um mapa $\phi : \mathcal{H} \to \mathcal{V}$ é dito um morfismo se a imagem do mapa induzido $\phi^* : \mathbb{F}[\mathcal{V}] \to \mathbb{F}^{\mathcal{H}}$, dado por $\phi^*(f) = f \circ \phi$, é um subconjunto de $\mathbb{F}[\mathcal{H}]$.

Para finalizarmos esta seção, definiremos uma topologia de Zariski para uma variedade afim $\mathcal{H}$, bem como estabelecer o conceito de uma variedade afim irredutível. Para tal observemos que, conforme pode ser visto em [38], tomando as variedades afins de $\mathbb{F}^n$ como os conjuntos fechados, temos uma topologia de Zariski. Logo, qualquer subconjunto de $\mathbb{F}^n$, em particular qualquer variedade afim, herda a topologia de Zariski definida acima. E assim, temos estabelecida uma topologia de Zariski para qualquer variedade afim $\mathcal{H}$.

Por fim, temos a definição seguir.

Definição 1.1.4. Uma variedade afim não-vazia é chamada irredutível quando não pode ser escrita como a união de dois subconjuntos próprios fechados e não-vazios. Caso contrário, tal variedade é dita redutível.

1.2 Grupos algébricos lineares

Ao longo desta seção iremos considerar $\mathbb{F}$ um corpo algebricamente fechado.

Definição 1.2.1. Um grupo algébrico linear é uma variedade afim G munida de um elemento unidade $e \in G$ e morfismos, chamados de multiplicação e inversão respectivamente, $m : G \times G \to G$ e $i : G \to G$, os quais satisfazem os axiomas de grupo, ou seja,

(a) $m(g, e) = m(e, g) = g$, para todo $g \in G$;

(b) $m(g, i(g)) = m(i(g), g) = e$, para todo $g \in G$;

(c) $m(g, m(g_1, g_2)) = m(m(g, g_1), g_2)$, para todos $g, g_1, g_2 \in G$.

Frequentemente, escreveremos simplesmente gg_1 e g^{-1}, para denotar $m(g, g_1)$ e $i(g)$, respectivamente.

Em outras palavras um grupo algébrico linear é uma variedade afim G que possui uma estrutura de grupo tal que a multiplicação e a inversão de elementos em G são morfismos de variedades afins.

Exemplo 1.2.2. O grupo linear geral GL_n é um grupo algébrico linear. Ademais, qualquer subgrupo $G < GL_n$ que é um fechado na topologia de Zariski de GL_n, é também um grupo algébrico linear. Na verdade, conforme pode ser visto em [15, Exemplo A.1.2], todo grupo algébrico linear é isomorfo a algum subgrupo de GL_n, o qual é fechado na topologia de Zariski. Este fato, justifica a terminologia grupo algébrico linear.

Definição 1.2.3. Seja $\mathcal{H}$ uma variedade afim. Uma ação regular de um grupo algébrico linear G em $\mathcal{H}$ é um morfismo de variedades afins $\mu : G \times \mathcal{H} \to \mathcal{H}$, que satisfaz os axiomas de ação, isto é,

(a) $\mu(e, v) = v$, para todo $v \in \mathcal{H}$;

(b) $\mu(g, \mu(g_1, v)) = \mu(m(g, g_1), v)$, para todos $g, g_1 \in G$ e $v \in \mathcal{H}$.

Quando não houver riscos de confusão, denotaremos $\mu(g, v)$ simplesmente por $g \cdot v$. Além disso, quando G age regularmente em $\mathcal{H}$, diremos simplesmente que $\mathcal{H}$ é uma G-variedade.

Em termos mais práticos, dizemos que um grupo linear algébrico G age regularmente na variedade afim $\mathcal{H}$, quando a ação de G em $\mathcal{H}$ é dada por um morfismo.

Definição 1.2.4. Uma representação de G é um espaço vetorial de dimensão finita $\mathcal{H}$, munido de um morfismo de grupos $\rho : G \to GL(\mathcal{H})$. Além disso, dizemos que uma representação $\mathcal{H}$ é racional, quando G age regularmente em $\mathcal{H}$.

Se $\mathcal{H}$ é uma representação racional de G, dizemos simplesmente que $\mathcal{H}$ é um G-módulo.

Atrelada a definição de representação racional, temos a definição de grupos linearmente redutivos apresentada a seguir.

Definição 1.2.5. Um grupo algébrico linear é chamado de linearmente redutivo se para cada representação racional $\mathcal{H}$ e cada $v \in \mathcal{H}^G/\{0\}$, existe uma função linear invariante $f \in (\mathcal{H}^*)^G$, tal que $f(v) \neq 0$.

Exemplo 1.2.6. Exemplos clássicos de grupos linearmente redutivos são os grupos GL_n, SL_n, grupos finitos e etc.

1.3 Álgebras de Invariantes

Nesta seção apresentaremos a construção da álgebra de invariantes de matrizes e algumas de suas propriedades básicas. Além disso, construiremos a álgebra de invariantes da variedade afim das matrizes nilpotentes.

Inicialmente, definiremos a álgebra de invariantes de forma mais geral. Para tal, consideremos um espaço vetorial de dimensão finita $\mathcal{H}$ e um grupo linear $G < GL(\mathcal{H})$. É um fato conhecido que $\mathcal{H}$ é um G-módulo com respeito a ação dada por: $g \cdot h = g(h)$, para todos $g \in G$ e $h \in \mathcal{H}$. Assim, podemos estender a ação de G sobre $\mathcal{H}$ para a ação de G sobre o anel de coordenadas $\mathbb{F}[\mathcal{H}]$ da seguinte maneira natural: $(g \cdot f)(h) = f(g^{-1}h)$, para todos $g \in G$, $f \in \mathbb{F}[\mathcal{H}]$ e $h \in \mathcal{H}$. Então, temos a seguinte definição.

Definição 1.3.1. Consideremos $\mathcal{H}$ um espaço vetorial de dimensão finita e um grupo linear $G < GL(\mathcal{H})$. A álgebra de invariantes de $\mathcal{H}$, com respeito a ação do grupo G, é o conjunto:

$$\mathbb{F}[\mathcal{H}]^G = \{f \in \mathbb{F}[\mathcal{H}] \,|\, g \cdot f = f, \ \forall\, g \in G\}$$

ou seja,

$$\mathbb{F}[\mathcal{H}]^G = \{f \in \mathbb{F}[\mathcal{H}] \,|\, f(g \cdot h) = f(h), \ \forall\, g \in G, \, h \in \mathcal{H}\}.$$

Vejamos agora exemplos mais concretos desta estrutura.

Exemplo 1.3.2. Sejam $n > 1$, $m \geq 1$ e M_n^m a soma direta de m cópias do espaço das matrizes $n \times n$ sobre $\mathbb{F}$. Considerando a ação diagonal por conjugação do grupo linear geral GL_n dada por:

$$g \cdot \underline{A} = (gA_1g^{-1}, \ldots, gA_mg^{-1}), \text{ para todos } g \in GL_n \text{ e } \underline{A} = (A_1, \ldots, A_m) \in M_n^m,$$

temos que M_n^m é um GL_n-módulo. Assim, podemos considerar a álgebra de invariantes de matrizes $\mathbb{F}[M_n^m]^{GL_n}$, a qual será denotada por $S(n, m)$, definida por:

$$\mathbb{F}[M_n^m]^{GL_n} = S(n, m) = \{f \in \mathbb{F}[M_n^m] \,|\, f(g \cdot \underline{A}) = f(\underline{A}), \ \forall\, g \in GL_n, \, \underline{A} \in M_n^m\}.$$

Buscaremos agora descrever mais concretamente os elementos de $S(n, m)$. Dada uma matriz A, denotaremos por A_{ij} a $(i, j)-$ésima entrada de A. É um fato conhecido que qualquer elemento do anel de coordenadas de M_n^m

$$\mathbb{F}[M_n^m] = \mathbb{F}[x_{ij}(k) \mid 1 \leq i, j \leq n, 1 \leq k \leq m]$$

pode ser considerado como a função polinomial $x_{ij}(k) : M_n^m \to \mathbb{F}$, a qual associa $(A_1, \ldots, A_m)$ ao elemento $(A_k)_{ij}$. Sibirskii em [25] e Procesi em [6], estabeleceram que a álgebra de invariantes $S(n,m)$ é gerada por $\operatorname{tr}(X_{i_1} \cdots X_{i_r})$, onde X_k denota a matriz genérica $(x_{ij}(k))_{1\le i,j\le n}$ de ordem n. Observemos que sobre um corpo infinito de característica positiva um conjuto gerador para $S(n,m)$ foi descrito por Donkin em [37].

Exemplo 1.3.3. Denotemos por $\mathcal{N}_n$ a variedade afim de todas as matrizes nilpotentes $n\times n$, isto é, $A \in M_n$ pertence a $\mathcal{N}_n$ se, e somente se, tivermos $\operatorname{tr}(A) = \operatorname{tr}(A^2) = \cdots = \operatorname{tr}(A^n) = 0$, ou equivalentemente, $A^n = 0$. Sabe-se que $\mathcal{N}_n^m$ é uma variedade irredutível. De forma análoga ao caso das matrizes $n\times n$, o anel de coordenadas $\mathbb{F}[(\mathcal{N}_n^m)]$, de $\mathcal{N}_n^m \subset M_n^m$, é gerado por $y_{ij}(k)$ para $1 \le i,j \le n$ e $1 \le k \le m$, onde $y_{ij}(k) : \mathcal{N}_n^m \to \mathbb{F}$ associa $(A_1, \ldots, A_m)$ ao elemento $(A_k)_{ij}$.

Consideremos agora $J = J_{n,m}$ o ideal de todas as funções polinomiais $f \in \mathbb{F}[M_n^m]$ que são zero em $\mathcal{N}_n^m$. Então, observemos que $\operatorname{tr}(X_k^s) \in J$ para todos $1 \le k, s \le n$, uma vez que $\operatorname{tr}(A) = \operatorname{tr}(A^2) = \cdots = \operatorname{tr}(A^n) = 0$. Logo, temos

$$\mathbb{F}[\mathcal{N}_n^m] = \mathbb{F}[M_n^m]/J \qquad \text{e} \qquad y_{ij}(k) = x_{ij}(k) + J.$$

A álgebra $\mathcal{O}(n,m) = \mathbb{F}[\mathcal{N}_n^m]^{GL_n}$ de invariantes de matrizes nilpotentes é definida da mesma forma que $S(n,m)$. Além disso, considerando $\phi : J \to \mathbb{F}[M_n^m]$ a inclusão e $\Psi : \mathbb{F}[M_n^m] \to \mathbb{F}[\mathcal{N}_n^m]$ a projeção canônica, uma vez que

$$0 \longrightarrow J \xrightarrow{\phi} \mathbb{F}[M_n^m] \xrightarrow{\Psi} \mathbb{F}[\mathcal{N}_n^m] \longrightarrow 0$$

é uma sequência exata curta, então

$$0 \longrightarrow J^{GL_n} \xrightarrow{\hat{\phi}} S(n,m) \xrightarrow{\hat{\Psi}} \mathcal{O}(n,m) \longrightarrow 0$$

é também uma sequência exata curta, pois GL_n é um grupo linearmente redutivo. Portanto, concluímos que a álgebra $\mathcal{O}(n,m)$ é gerada por $\operatorname{tr}(Y_{i_1} \cdots Y_{i_r})$, onde $Y_k = (y_{ij}(k))_{1\le i,j\le n}$ é a matriz nilpotente genérica de ordem n. Obviamente, $\operatorname{tr}(Y_k^s) = 0$ para qualquer $s > 0$ and $Y_k^n = 0$. Observe que no caso $m = 1$, temos $\mathcal{O}(n,1) = \mathbb{F}$.

Exemplo 1.3.4. De modo análogo ao feito no Exemplo 1.3.2, iremos considerar o grupo especial linear SL_n e a ação diagonal bilateral do grupo $SL(n) \times SL(n)$ em M_n^m, isto é, para $g_1, g_2 \in SL(n)$ e $\underline{A} \in M_n^m$, temos

$$(g_1, g_2) \cdot \underline{A} = (g_1 A_1 g_2^{-1}, \ldots, g_1 A_m g_2^{-1}).$$

Portanto, podemos ver M_n^m como um $SL_n \times SL_n$-módulo e consequentemente podemos definir a álgebra de invariantes $\mathbb{F}[M_n^m]^{SL_n \times SL_n}$, a qual denotaremos por $R(n, m)$.

Um conjunto gerador minimal para $R(2, m)$ foi obtido por Domokos e Drensky (vide [27] e [28]) para $\operatorname{char} \mathbb{F} \neq 2$, e por Lopatin (veja [4]) para o caso geral. Um conjunto gerador minimal para $R(3, 3)$ foi descrito por Domokos e Drensky em [26] e [31]. É de conhecimento geral que a álgebra $R(n, 2)$ é polinomial com $n + 1$ geradores algebricamente independentes de mesmo grau n (veja [31] para maiores detalhes).

1.4 Invariantes Separadores

Nesta seção abordaremos o conceito de invariantes separadores. Este conceito foi estabelecido em 2002 por Derksen e Kemper (vide [15]), e como veremos a seguir, de certa maneira este conceito é "mais fraco"que o conceito de conjuntos geradores da álgebra de invariantes. Iniciaremos com as seguintes definições:

Definição 1.4.1. Dado um subconjunto S de $\mathbb{F}[\mathcal{H}]^G$, dizemos que elementos u, v de $\mathcal{H}$ são separados por S se existe um invariante $f \in S$ com $f(u) \neq f(v)$. Além disso, se $u, v \in \mathcal{H}$ são separados por $\mathbb{F}[\mathcal{H}]^G$, então simplesmente dizemos que eles são separados.

Definição 1.4.2. Um subconjunto $S \subset \mathbb{F}[\mathcal{H}]^G$ do anel de invariantes é chamado separador se para cada par de elementos separados u, v de $\mathcal{H}$, tivermos que u, v são separados por S.

Observemos que é de verificação imediata que qualquer conjunto gerador da álgebra de invariantes $\mathbb{F}[\mathcal{H}]^G$ é também um conjunto separador, por isso o conceito de conjunto separadores de invariantes é considerado "mais fraco" que o conceito de geradores da álgebra de invariantes. Contudo, vale destacar que nem sempre a recíproca é válida, assim temos interesse especial nos casos em que esses conjuntos são distintos.

Um outro ponto de interesse no estudo de invariantes separadores consiste em determinar conjuntos separadores minimais, com respeito a relação de ordem dada pela inclusão, os quais chamaremos simplesmente de conjuntos separadores minimais. Exemplos de conjuntos separadores minimais, para álgebras de invariantes particulares, foram contruidos em [23, 32, 11, 5, 14, 35, 10].

Notemos agora que uma vez conhecido um conjunto gerador de uma álgebra de invariantes, teoricamente podemos reduzir de forma conveniente este conjunto até obter um conjunto separador minimal desta álgebra. Contudo, na prática esta redução pode ser bastante árdua, uma vez que sendo S um conjunto gerador da álgebra de invariantes $\mathbb{F}[\mathcal{H}]^G$, para mostrarmos que um elemento $f_0 \in S$ pertence a um conjunto separador minimal, obtido a partir de S, é necessário encontrar elementos $u, v \in \mathcal{H}$ tais que $f_0(u) \neq f_0(v)$, mas $f(u) = f(v)$ para todo $f \in S \backslash \{f_0\}$. Portanto, ao aplicar esta técnica, um fator de extrema importância é a cardinalidade do conjunto gerador S. Entretanto, existem resultados que permitem limitar essa cardinalidade. Para conjuntos geradores temos o clássico teorema devido a Hilbert:

Teorema 1.4.3. *Sejam $\mathcal{H}$ uma variedade afim e G um grupo redutivo. Então, a álgebra de invariantes $\mathbb{F}[\mathcal{H}]^G$ é finitamente gerada.*

Para um conjunto separador de invariantes, temos um resultado ainda mais geral, o qual pode ser encontrado em [15, Teorema 2.4.8].

Teorema 1.4.4. *Sejam $\mathcal{H}$ uma variedade afim e G um grupo agindo em $\mathbb{F}[\mathcal{H}]$ por automorfismos, isto é, $G \subseteq Aut(\mathcal{H})$. Então, existe um conjunto separador finito $S \subseteq \mathbb{F}[\mathcal{H}]^G$.*

Observemos que uma vez que os grupos GL_n e $SL_n \times SL_n$ são redutivos, então as álgebras de invariantes $S(n, m)$, $\mathcal{O}(n, m)$ e $R(n, m)$ apresentadas nos Exemplos 1.3.2, 1.3.3 e 1.3.4, respectivamente, possuem conjuntos geradores (e consequentemente separadores) finitos.

Uma vez, sob determinadas circunstâncias, garantida a existência de conjuntos geradores (ou separadores) finitos para uma álgebra de invariantes $\mathbb{F}[\mathcal{H}]^G$ podemos nos indagar a respeito de uma limitação para o grau dos elementos desse conjunto. Neste sentido, consideremos a definição a seguir.

Definição 1.4.5. Denotemos por $\beta(\mathbb{F}[\mathcal{H}]^G)$ ($\beta_{\text{sep}}(\mathbb{F}[\mathcal{H}]^G)$, respectivamente) o menor inteiro D tal que o conjunto de todos os invariantes homogêneos de $\mathbb{F}[\mathcal{H}]^G$ com grau $\leq D$ é um conjunto gerador (conjunto separador, respectivamente).

Notemos que $\beta(\mathbb{F}[\mathcal{H}]^G)$ é o grau máximo dos elementos de qualquer conjunto gerador minimal de $\mathbb{F}[\mathcal{H}]^G$.

Para a álgebra $S(n, m)$ Derksen e Makam em [19] estabeleceram as limitações $\beta(S(n, m)) \leq (m + 1)n^4$ e $\beta_{\text{sep}}(S(n, m)) \leq n^6$ onde $\mathbb{F}$ é um corpo algebricamente fechado arbitrário. A segunda limitação foi melhorada em [22], onde obtiveram $\beta_{\text{sep}}(S(n, m)) \leq 4n^2 \log_2(n) + 12n^2 - 4n$. Ademais, foi mostrado em [22] que $\beta_{\text{sep}}(S(n, m)) \leq 4n \log_2(n) + 12n - 4$ para um corpo algebricamente fechado de característica zero.

Para a álgebra $R(n,m)$ várias limitações foram obtidas para $\beta(R(n,m))$ e $\beta_{\text{sep}}(R(n,m))$, a título de exemplos listamos as seguintes:

- $\beta(R(3,m)) \leq 309$ quando $\operatorname{char}\mathbb{F} = 0$ (veja Proposição 1.13 em [17]);
- $\beta(R(n,m)) \geq n^2$ onde $m \geq n^2$ e $\mathbb{F} = \mathbb{C}$ (vide Teorema 1.15 de [17]);
- $\beta(R(n,m)) \leq mn^3(n-1)$ no caso em que $n \geq 2$ (veja Teorema 1.5 em [21]);
- $\beta(R(n,m)) \leq n^6$ para $\operatorname{char}\mathbb{F} = 0$ ou $\operatorname{char}\mathbb{F} > 2n^6 + n^2$ (vide Teoremas 1.5 e 1.6 de [21]);
- $\beta(R(n,m)) \leq n^7$ quando $\operatorname{char}\mathbb{F} > n^6$ (veja Proposição 1.8 de [21]);
- $\beta_{\text{sep}}(R(n,m)) \leq n^6$ (vide Corolário 1.12 em [19]);
- $\beta_{\text{sep}}(R(n,m)) \leq 4n^4\log_2(n) + 14n^4 - 4n^3$ (pelo Corolário 1.19 de [22]);
- $\beta_{\text{sep}}(R,n,m)) \leq 4n^3\log_2(n) + 14n^3 - 4n^2$, onde $\operatorname{char}\mathbb{F} = 0$ (vide Corolário 1.19 em [22]).

2 Invariantes separadores de matrizes nilpotentes 3×3.

No decorrer deste capítulo todos os espaços vetoriais, álgebras, e módulos serão considerados sobre um corpo algebricamente fechado $\mathbb{F}$ de característica zero a menos que especifiquemos o contrário. Além disso, por uma álgebra sempre nos referimos a uma álgebra associativa com unidade. Teremos como objetivo principal deste capítulo obter um conjunto separador minimal para a álgebra $\mathcal{O}(3,3)$ (veja Teorema 2.2.15), resultado este que foi publicado na revista Linear Álgebra and Its Applications (vide [10]). Contudo, iniciaremos considerando alguns casos particulares, bem como alguns resultados auxiliares que irão nos ajudar nesse objetivo.

2.1 As álgebras $\mathcal{O}(2,m)$ e $\mathcal{O}(3,2)$

Nesta seção iremos apresentar a descrição de um conjunto minimal de geradores que também é um conjunto separador minimal para as álgebras $\mathcal{O}(2,m)$ e $\mathcal{O}(3,2)$ (vide Proposições 2.1.4 e 2.1.5). Contudo, antes de passar a essa descrição fixemos algumas notações que serão adotadas ao longo desta tese.

Iremos denotar a matriz identidade por E, e por E_{ij} denotaremos a matriz tal que a (i,j)-entrada é igual a um e o resto das entradas são iguais a zero. Além disso, iremos adotar as seguintes notações para matrizes nilpotentes 3×3 : $J_1 = E_{12}$ e $J_2 = E_{12} + E_{23}$.

Seja $\mathbb{F}$ um corpo infinito de característica arbitrária. Kaygorodov, Lopatin e Popov em [23] descreveram o seguinte conjunto separador minimal de $S(2,m)$:

$$\mathrm{tr}(X_i^2),\ 1 \leq i \leq m;\ \mathrm{tr}(X_{i_1} \cdots X_{i_k}),\ k \in \{1,2,3\},\ 1 \leq i_1 < \cdots < i_k \leq m. \tag{2.1}$$

Além disso, conforme é possível observar em [7, 29], o conjunto dado em (2.1) gera a álgebra $S(2,m)$ se, e somente se, a característica de $\mathbb{F}$ é diferente de 2 ou $m \leq 3$. Portanto, uma vez fixado que *char* $\mathbb{F} = 0$, temos que o conjunto dado em (2.1) é um conjunto gerador minimal para a álgebra $S(2,m)$.

Consideremos agora o conjunto $S_{2,m} \subseteq \mathcal{O}(2,m)$ dado por:

$$S_{2,m} = \{\mathrm{tr}(Y_iY_j),\ 1 \leq i < j \leq m;\ \ \mathrm{tr}(Y_iY_jY_k),\ 1 \leq i < j < k \leq m\}$$

e as observações a seguir.

Lema 2.1.1. *O conjunto $S_{2,m}$ é um conjunto gerador, e consequentemente separador, da álgebra $\mathcal{O}(2,m)$.*

Demonstração. De fato, uma vez que o conjunto dado em (2.1) é um conjunto gerador minimal para a álgebra $S(2,m)$, e o homomorfismo $\hat{\Psi}$ descrito no Exemplo 1.3.3 é sobrejetivo, temos que a imagem do conjunto (2.1) será um conjundo gerador para $\mathcal{O}(2,m)$. Assim, a afirmação segue do fato que $S_{2,m}$ coincide com a imagem de (2.1) por $\hat{\Psi}$. □

Lema 2.1.2. *Supondo $m = 2$, temos que $S_{2,2} \backslash \{tr(Y_1Y_2)\}$ não é um conjunto separador de $\mathcal{O}(2,2)$.*

Demonstração. Basta considerar $\underline{A} = (E_{12}, E_{12})$ $\underline{B} = (E_{12}, E_{21})$ elementos de $\mathcal{N}_2^2$, e notar que $\mathrm{tr}(A_1A_2) \neq \mathrm{tr}(B_1B_2)$. □

Lema 2.1.3. *Seja $m = 3$. Então, $S_{2,3} \backslash \{\mathrm{tr}(Y_1Y_2Y_3)\}$ não é um conjunto separador de $\mathcal{O}(2,3)$.*

Demonstração. Com efeito, considerando $\underline{A} = (E_{12}, -E_{21}, C)$ e $\underline{B} = (E_{12}, C, -E_{21})$ elementos de $\mathcal{N}_2^3$, onde $C = E_{11} + E_{12} - E_{21} - E_{22}$, segue que, $\mathrm{tr}(A_iA_j) = \mathrm{tr}(B_iB_j)$ para todos $1 \leq i < j \leq 3$, mas $\mathrm{tr}(A_1A_2A_3) \neq \mathrm{tr}(B_1B_2B_3)$. □

Observemos agora que unindo os lemas anteriores, podemos concluir a seguinte proposição.

Proposição 2.1.4. *O conjunto*

$$S_{2,m} = \{\mathrm{tr}(Y_iY_j),\ 1 \leq i < j \leq m;\ \ \mathrm{tr}(Y_iY_jY_k),\ 1 \leq i < j < k \leq m\}$$

é um conjuto gerador minimal, bem como um conjunto separador minimal para a álgebra de invariantes $\mathcal{O}(2,m)$.

Consideremos agora o caso da álgebra $\mathcal{O}(3,2)$. De forma semelhante a Proposição 2.1.4, temos o seguinte resultado.

Proposição 2.1.5. *O conjunto*

$$S_{3,2} = \{\mathrm{tr}(Y_1Y_2),\ \mathrm{tr}(Y_1^2Y_2),\ \mathrm{tr}(Y_1Y_2^2),\ \mathrm{tr}(Y_1^2Y_2^2),\ \mathrm{tr}(Y_1^2Y_2^2Y_1Y_2)\}$$

é um conjunto gerador minimal, bem como um conjunto separador minimal, para a álgebra de invariantes $\mathcal{O}(3,2)$.

Demonstração. De fato, para concluirmos que $S_{3,2}$ é um conjunto gerador de $\mathcal{O}(3,2)$, basta observar que $S_{3,2}$ coincide com a imagem, via o homomorfismo sobrejetivo $\hat{\Psi}$, do conjunto gerador minimal de $S(3,2)$ descrito por Lopatin (veja Teorema 1 de [2]). Segue daí, que $S_{3,2}$ é um conjunto separador.

Afim de finalizarmos a demonstração, é suficiente mostrar que $S_{3,2}$ é um conjunto separador minimal, ou seja, para qualquer $f \in S_{3,2}$ devemos mostrar que $S_{3,2} \backslash \{f\}$ não é separador. Para tal, devemos construir $\underline{A} = (A_1, A_2)$ e $\underline{B} = (B_1, B_2)$ de $\mathcal{N}_3^2$ tais que para qualquer $h \in S_{3,2} \backslash \{f\}$ teremos $h(\underline{A}) = h(\underline{B})$, mas $f(\underline{A}) \neq f(\underline{B})$.

Sendo $f = \mathrm{tr}(Y_1Y_2)$, tomemos $A_1 = B_1 = J_2$, $A_2 = E_{32}$, e $B_2 = E_{12}$.

Para $f = \mathrm{tr}(Y_1^2Y_2)$, o qual por semelhança nos permite obter um exemplo para $f = \mathrm{tr}(Y_1Y_2^2)$, basta considerar $A_1 = B_1 = J_2$,

$$A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \ \text{e} \ B_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ -1 & 1 & 0 \end{pmatrix}.$$

Quando $f = \mathrm{tr}(Y_1^2Y_2^2)$, tomemos $A_1 = B_1 = J_2$,

$$A_2 = \begin{pmatrix} 0 & -2 & 1 \\ 2 & 0 & 1 \\ 2 & 2 & 0 \end{pmatrix}, \ \text{e} \ B_2 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & -1 \\ 2 & 4 & 0 \end{pmatrix}.$$

Por fim, para $f = \mathrm{tr}(Y_1^2Y_2^2Y_1Y_2)$, consideramos $A_1 = B_1 = J_2$,

$$A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \ \text{e} \ B_2 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

□

Antes de apresentarmos o corolário que irá encerrar esta seção, destacamos que a sobrejetividade do homomorfismo $\hat{\Psi}$ nos permite concluir as seguintes desigualdades

$$\beta(\mathcal{O}(n,m)) \leq \beta(S(n,m)) \quad \text{e} \quad \beta_{\mathrm{sep}}(\mathcal{O}(n,m)) \leq \beta_{\mathrm{sep}}(S(n,m)).$$

Assim, da Proposição 2.1.5, temos o resultado a seguir.

Corolário 2.1.6. *Assuma que* $m \geq 2$. *Então,* *(a)* $\beta_{\text{sep}}(S(3, m)) = 6$*, onde o corpo* $\mathbb{F}$ *não necessariamente é algebricamente fechado;*

(b) $\beta(\mathcal{O}(3, n)) = \beta_{\text{sep}}(\mathcal{O}(3, n)) = 6$.

Demonstração. Conforme pode ser visto em [1, Teorema 2], sobre um corpo arbitrário de característica zero a álgebra $S(3, m)$ é gerada por invariantes homogêneos de grau menor ou igual a 6. Logo, $\beta_{\text{sep}}(S(3, m)) \leq 6$ e $\beta_{\text{sep}}(\mathcal{O}(3, m)) \leq \beta(\mathcal{O}(3, m)) \leq 6$. Portanto, a conclusão da demonstração segue da Proposição 2.1.5. □

Observemos que uma das conclusões do corolário anterior nos diz que vale $\beta_{\text{sep}}(S(3, m)) = 6$. Este fato nos garante que embora as limitações para $\beta_{\text{sep}}(S(n, m))$ sejam bastante gerais, para casos particulares, como no caso de $S(3, m)$, elas não são limitações ideais, o que sugere que talvez seja possível obter limitações mais precisas, além de destacar a importância de obter essas limitações exatas para álgebras de invariantes fixadas.

2.2 A álgebra $\mathcal{O}(3, 3)$

Nesta seção iremos apresentar um dos principais resultados obtidos nesta tese, o qual consiste em descrever explicitamente um conjunto minimal de geradores, bem como um conjunto separador minimal, para a álgebra $\mathcal{O}(3, 3)$ (ver Teorema 2.2.15).

Iniciaremos definindo alguns conjuntos que serão necessários para as formulações que seguirão nesta seção. Denotaremos por $S_{3,3}$ o seguinte subconjunto da álgebra $\mathcal{O}(3, 3)$:

$$\text{tr}(Y_iY_j),\ \text{tr}(Y_i^2Y_j),\ \text{tr}(Y_iY_j^2),\ \text{tr}(Y_i^2Y_j^2),\ \text{tr}(Y_i^2Y_j^2Y_iY_j) \text{ com } 1 \leq i < j \leq 3,$$

$$\text{tr}(Y_1Y_2Y_3),\ \text{tr}(Y_1Y_3Y_2)$$

$$\text{tr}(Y_i^2Y_jY_k) \text{ com } \{i, j, k\} = \{1, 2, 3\},$$

$$\text{tr}(Y_1^2Y_2Y_1Y_3),\ \text{tr}(Y_2^2Y_1Y_2Y_3),\ \text{tr}(Y_3^2Y_1Y_3Y_2).$$

Ademais, definiremos $P_{3,3} = S_{3,3} \sqcup P'_{3,3}$, onde $P'_{3,3} \subset \mathcal{O}(3, 3)$ é o conjunto a seguir:

$$\text{tr}(Y_i^2Y_j^2Y_k),\ \text{tr}(Y_i^2Y_j^2Y_iY_k) \text{ com } \{i, j, k\} = \{1, 2, 3\},\ \text{tr}(Y_1^2Y_2^2Y_3^2).$$

Observemos que $|S_{3,3}| = 26$ e $|P_{3,3}| = 39$.

A respeito desses conjuntos temos a seguinte observação.

Observação 2.2.1. Aplicando o homomorfismo sobrejetivo, dado no Exemplo 1.3.3, $\hat{\Psi}$ ao conjunto gerador minimal de $S(3, 3)$, descrito do Teorema 1 de [2], podemos concluir que $P_{3,3}$ é um conjunto gerador para a álgebra $\mathcal{O}(3, 3)$.

No intuito de mostrar que o conjunto $P_{3,3}$ é um conjunto gerador minimal para a álgebra $\mathcal{O}(3,3)$, recordemos os fatos a seguir.

Assumamos que $\mathcal{A}$ é $S(n,m)$ ou $\mathcal{O}(n,m)$. Para um monômio $f \in \mathcal{A}$ denotemos por $\deg f$ seu grau e por $\operatorname{mdeg} f$ seu multigrau, isto é, $\operatorname{mdeg} f = (t_1, \ldots, t_m)$, onde t_k é o grau total do monômio f in $x_{ij}(k)$, $1 \le i, j \le n$, e $\deg f = t_1 + \cdots + t_m$. Então as álgebras $S(n,m)$ e $\mathcal{O}(n,m)$ possuem uma $\mathbb{N}$-graduação pelo grau e uma $\mathbb{N}^d$-graduação pelo multigrau, onde $\mathbb{N}$ denota o conjunto de inteiros não negativos. Ademais, dizemos que um multigrau $(t_1, \ldots, t_m)$ é menor que o multigrau $(r_1, \ldots, r_m)$ se $t_i \le r_i$ para todos i e $t_j < r_j$ para algum j. Além disso, dizemos que um invariante $\mathbb{N}$-homogêneo $f \in \mathcal{A}$ é decomponível e escrevemos $f \equiv 0$ se f é um polinômio nos invariantes $\mathbb{N}$-homogêneos de $\mathcal{A}$ de grau estritamente menor. Se f não é decomponível, então dizemos que f é indecomponível, e escrevemos $f \not\equiv 0$. No caso em que $f - h \equiv 0$ escrevemos $f \equiv h$. Obviamente, se $f \equiv 0$ para $f \in S(n,m)$, então $\hat{\Psi}(f) \equiv 0$ em $\mathcal{O}(n,m)$.

Acerca destes conceitos temos os seguintes lemas:

Lema 2.2.2. *Para qualquer $f \in S_{3,3}$ o conjunto $P_{3,3} \backslash \{f\}$ não é separador para $\mathcal{O}(3,3)$. Em particular, qualquer subconjunto próprio de $S_{3,3}$ não é um conjunto separador para $\mathcal{O}(3,3)$.*

Demonstração. Inicialmente, notemos que se f depende das entradas de apenas duas matrizes da lista Y_1, Y_2, Y_3, então o lema segue do fato que $S_{3,2}$ é um conjunto separador minimal para $\mathcal{O}(3,2)$ (veja a Proposição 2.1.5).

Construiremos $\underline{A} = (A_1, A_2, A_3)$ e $\underline{B} = (B_1, B_2, B_3)$ de $\mathcal{N}_3^3$ tais que para qualquer $h \in P_{3,3} \backslash \{f\}$ teremos $h(\underline{A}) = h(\underline{B})$, mas $f(\underline{A}) \neq f(\underline{B})$.

Para $f = \operatorname{tr}(Y_1 Y_2 Y_3)$, consideramos $\underline{A} = (E_{31}, E_{12} + E_{32}, E_{23})$ e $\underline{B} = (0, E_{12}, E_{21})$.

Para $f = \operatorname{tr}(Y_1^2 Y_2 Y_3)$ tomemos $\underline{A} = (E_{21} + E_{32}, E_{12}, E_{23})$ e $\underline{B} = (E_{13} + E_{21}, E_{12}, J_2)$.

Por fim, sendo $f = \operatorname{tr}(Y_1^2 Y_2 Y_1 Y_3)$ basta tomarmos $\underline{A} = (E_{21} + E_{32}, E_{13}, E_{23})$ e $\underline{B} = (E_{23} + E_{31}, E_{12}, E_{13})$.

Obviamente, dada a simetria entre os elementos de $S_{3,3}$ de mesmo multigrau, temos que os casos considerados de $f \in S_{3,3}$, implicam todos os casos possíveis. $\square$

Lema 2.2.3. *Os elementos a seguir são indecomponíveis em $\mathcal{O}(3,3)$:*

(a) $\alpha_1 \operatorname{tr}(Y_1^2 Y_2^2 Y_3) + \alpha_2 \operatorname{tr}(Y_2^2 Y_1^2 Y_3)$ *para quaisquer $\alpha_1, \alpha_2 \in \mathbb{F}$, onde α_1 ou α_2 é não nulo;*

(b) $\mathrm{tr}(Y_1^2Y_2^2Y_1Y_3)$;

(c) $\mathrm{tr}(Y_1^2Y_2^2Y_3^2)$.

Demonstração. Por simplicidade de notação, denotaremos

$$C = \begin{pmatrix} 0 & -1 & -1 \\ 0 & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \quad \text{e} \quad D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & -1 \end{pmatrix}.$$

(a) Assumamos que o item (a) não é válido. Visto que a álgebra $\mathcal{O}(3,3)$ admite uma $\mathbb{N}^3$-graduação dada pelo multigrau e é gerada por $P_{3,3}$ (veja a Observação 2.2.1), sem perda de generalidade podemos assumir que existem $\alpha_1 \neq 0, \alpha_2, \beta_1, \ldots, \beta_4$ de $\mathbb{F}$ tais que

$$\begin{aligned} \alpha_1 \,\mathrm{tr}(A_1^2A_2^2A_3) + \alpha_2 \,\mathrm{tr}(A_2^2A_1^2A_3) = {} & \beta_1 \,\mathrm{tr}(A_1A_2A_3)\,\mathrm{tr}(A_1A_2) + \beta_2 \,\mathrm{tr}(A_1A_3A_2)\,\mathrm{tr}(A_1A_2) \\ & + \beta_3 \,\mathrm{tr}(A_1^2A_2)\,\mathrm{tr}(A_2A_3) + \beta_4 \,\mathrm{tr}(A_2^2A_1)\,\mathrm{tr}(A_1A_3) \end{aligned}$$

para todas A_1, A_2, A_3 de $\mathcal{N}_3$. Consequentemente, considerando as ternas $(J_2, E_{23}+E_{31}, E_{13})$ e (J_2, C, E_{21}) obtemos respectivamente $\beta_3 = 0$ e $\alpha_1 = 0$, o que é uma contradicão.

(b) Suponhamos que o item (b) seja falso. Como no item (a), existem elementos $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3, \gamma \in \mathbb{F}$ tais que

$$\begin{aligned} \mathrm{tr}(A_1^2A_2^2A_1A_3) = {} & \alpha_1\mathrm{tr}(A_1^2A_2^2)\mathrm{tr}(A_1A_3) + \alpha_2\mathrm{tr}(A_1^2A_2A_3)\mathrm{tr}(A_1A_2) + \alpha_3\mathrm{tr}(A_1^2A_3A_2)\mathrm{tr}(A_1A_2) \\ & + \beta_1\mathrm{tr}(A_1^2A_2)\mathrm{tr}(A_1A_2A_3) + \beta_2\mathrm{tr}(A_1^2A_2)\mathrm{tr}(A_1A_3A_2) + \beta_3\mathrm{tr}(A_2^2A_1)\mathrm{tr}(A_1^2A_3) \\ & + \gamma \,\mathrm{tr}(A_1A_2)^2 \,\mathrm{tr}(A_1A_3) \end{aligned}$$

para todas ternas $(A_1, A_2, A_3) \in \mathcal{N}_3^3$. Consequentemente, considerando respectivamente as ternas $(J_2, E_{31} + E_{32}, E_{21} - E_{32})$, $(J_2, E_{31} + E_{32}, E_{32})$, (J_2, C, E_{32}), $(J_2, C, E_{31} + E_{32})$ e $(J_2, C, E_{21} - E_{32})$, obtemos $\alpha_2 = 0$, $\gamma = 0$, $\beta_2 = \alpha_1 + \beta_1$, $\alpha_1 = 1$, $\beta_1 = 0$, respectivamente. Então, tomando

$$A_1 = \begin{pmatrix} 1 & 1 & 0 \\ -1 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \; A_2 = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

e $A_3 = E_{12}$, iremos concluir que $0 = -1$, um absurdo.

(c) Supondo o item (c) falso, como em (a), existem $\alpha_1, \ldots, \alpha_6, \beta_1, \ldots, \beta_6, \gamma \in \mathbb{F}$ tais que

$$\begin{aligned} \mathrm{tr}(A_1^2A_2^2A_3^2) = {} & \alpha_1\mathrm{tr}(A_1^2A_2A_3)\mathrm{tr}(A_2A_3) + \alpha_2\mathrm{tr}(A_1^2A_3A_2)\mathrm{tr}(A_2A_3) + \alpha_3\mathrm{tr}(A_2^2A_1A_3)\mathrm{tr}(A_1A_3) \\ & + \alpha_4\mathrm{tr}(A_2^2A_3A_1)\mathrm{tr}(A_1A_3) + \alpha_5\mathrm{tr}(A_3^2A_1A_2)\mathrm{tr}(A_1A_2) + \alpha_6\mathrm{tr}(A_3^2A_2A_1)\mathrm{tr}(A_1A_2) \\ & + \beta_1\mathrm{tr}(A_1A_2A_3)^2 + \beta_2\mathrm{tr}(A_1A_2A_3)\,\mathrm{tr}(A_1A_3A_2) + \beta_3\mathrm{tr}(A_1A_3A_2)^2 \\ & + \beta_4\mathrm{tr}(A_1^2A_2)\,\mathrm{tr}(A_3^2A_2) + \beta_5\mathrm{tr}(A_1^2A_3)\,\mathrm{tr}(A_2^2A_3) + \beta_6\mathrm{tr}(A_2^2A_1)\,\mathrm{tr}(A_3^2A_1) \\ & + \gamma\mathrm{tr}(A_1A_2)\,\mathrm{tr}(A_1A_3)\,\mathrm{tr}(A_2A_3) \end{aligned}$$

para todas as ternas $(A_1, A_2, A_3) \in \mathcal{N}_3^3$. Assim, avaliando a igualdade anterior nas ternas $(J_2, E_{23} + E_{31}, E_{31})$, $(J_2, E_{31}, E_{23} + E_{31})$, e $(J_2, D, E_{31} + E_{32})$ obteremos $\beta_1 = 0$, $\beta_3 = 0$, e $\beta_2 = -\gamma$, respectivamente. Considerando agora, todas as permutações de entradas na terna $(J_2, D + E_{31}, E_{32})$ podemos concluir $\alpha_1 = \cdots = \alpha_6 = -\gamma$. Analogamente, tomando todas as permutações de entradas na terna $(J_2, J_2, E_{23} + E_{31})$ teremos $\beta_4 = \beta_5 = \beta_6 = \gamma$. Considerando agora a terna $(J_2, C, E_{21} + E_{32})$ obteremos $\gamma = 0$. Por fim, tomando $A_2 = J_2$, $A_3 = E_{21} + E_{32}$, e

$$A_1 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

deveriamos ter $0 = -1$, o que é uma contradicão. $\square$

Lema 2.2.4. *Seja $\mathcal{A}$ uma das álgebras $S(n, m)$ ou $\mathcal{O}(n, m)$. Assumamos que $P = P_1 \cup P_2$ gera a álgebra $\mathcal{A}$ e que $P_1, P_2 \subset \mathcal{A}$ satisfazem as seguintes condições:*

(a) $P \backslash \{f\}$ não é um conjunto separador para $\mathcal{A}$ qualquer que seja $f \in P_1$;

(b) Qualquer combinação linear não trivial de elementos $f_1, \ldots, f_m \in P_2$ de mesmo multigrau é indecomponível em $\mathcal{A}$.

Então, P é um conjunto gerador minimal para $\mathcal{A}$.

Demonstração. Se P não é um conjunto gerador minimal para $\mathcal{A}$, então existe $f \in P$ tal que $P \backslash \{f\}$ é ainda um conjunto gerador para $\mathcal{A}$. Mas a condição (a) implica que f não pertence a P_1 e a condição (b) assegura que f não pertence a P_2, o que é uma contradição. $\square$

Fazendo uso dos lemas anteriores temos o seguinte teorema.

Teorema 2.2.5. *O conjunto $P_{3,3}$ é um conjunto gerador minimal para a álgebra de invariantes $\mathcal{O}(3, 3)$.*

Demonstração. Basta observar que a Observação 2.2.1 e os Lemas 2.2.2 e 2.2.3 implicam que $P_{3,3} = S_{3,3} \sqcup P'_{3,3}$ satisfaz as condições (a) e (b) do Lema 2.2.4, para $P_1 = S_{3,3}$ e $P_2 = P'_{3,3}$, as quais implicam que $P_{3,3}$ é um conjunto gerador minimal para $\mathcal{O}(3, 3)$. $\square$

Nossos esforços agora irão se concentrar em mostrar que o conjunto $S_{3,3}$ é um conjunto separador minimal para a álgebra $\mathcal{O}(3, 3)$. Vale salientar que a minimalidade segue imediatamente do Lema 2.2.2, então para obtermos este resultado resta mostrar que $S_{3,3}$ é um conjunto separador, e teremos então o teorema.

Teorema 2.2.6. *O conjunto $S_{3,3}$ é um conjunto separador minimal para a álgebra de invariantes $\mathcal{O}(3,3)$.*

Conforme comentado acima, para demonstrar o Teorema 2.2.6 é suficiente provar o lema a seguir.

Lema 2.2.7. *Sejam $\underline{A} = (A_1, A_2, A_3)$ e $\underline{B} = (B_1, B_2, B_3)$ pertencentes a $\mathcal{N}_3^3$ os quais não são separados por $S_{3,3}$. Então, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3}$.*

Demonstração. Pela Proposição 2.1.5 podemos supor que

$$A_i \neq 0 \text{ ou } B_i \neq 0 \text{ para todos } 1 \leq i \leq 3. \tag{2.2}$$

Como $\mathbb{F}$ é algebricamente fechado aplicando a ação de GL_3 no par $(\underline{A}, \underline{B})$, considerando as notações comentadas no início da Seção 2.1, podemos assumir que ocorre um dos seguintes casos:

(1) $A_1 = J_2$ e $B_1 = J_2$;

(2) $A_1 = J_2$ e $B_1 = J_1$;

(3) $A_1 = J_2$ e $B_1 = 0$;

(4) $A_1 = J_1$ e $B_1 = J_2$;

(5) $A_1 = J_1$ e $B_1 = J_1$;

(6) $A_1 = J_1$ e $B_1 = 0$;

(7) $A_1 = 0$ e $B_1 = J_2$;

(8) $A_1 = 0$ e $B_1 = J_1$.

Ademais, renomeando $\underline{A}$ e $\underline{B}$ se necessário, podemos diminuir o número de casos, para os casos seguintes:

(a) $A_1 = J_2$ e $B_1 = J_2$;

(b) $A_1 = J_2$ e $B_1 = J_1$;

(c) $A_1 = J_2$ e $B_1 = 0$;

(d) $A_1 = J_1$ e $B_1 = J_1$;

(e) $A_1 = J_1$ e $B_1 = 0$.

Portanto, os Lemas 2.2.10, 2.2.11, 2.2.12, 2.2.13 e 2.2.14, a seguir, finalizam a demonstração. $\square$

Antes de passarmos as demonstrações dos Lemas 2.2.10, 2.2.11, 2.2.12, 2.2.13 e 2.2.14, iremos apresentar dois lemas que descrevem formas canônicas para simplificar as possibilidades para os elementos $\underline{A}$ e $\underline{B}$ de $\mathcal{N}_3^3$.

Lema 2.2.8. *Consideremos $A_1 = J_2$ e $A_2 \in \mathcal{N}_3$. Então, existe $g \in GL_3$ tal que $gA_1g^{-1} = A_1$ e gA_2g^{-1} é uma das seguintes matrizes:*

(1) $W_{\mathrm{I}} = \begin{pmatrix} 0 & a_2 & a_3 \\ 0 & 0 & a_6 \\ 0 & 0 & 0 \end{pmatrix}$;

(2) $W_{\mathrm{II}} = \begin{pmatrix} 0 & 0 & a_3 \\ 0 & 0 & 0 \\ 0 & a_8 & 0 \end{pmatrix}$ *com* $a_8 \neq 0$;

(3) $W_{\mathrm{III}} = \begin{pmatrix} 0 & 0 & a_3 \\ a_4 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ *com* $a_4 \neq 0$;

(4) $W_{\mathrm{IV}} = \begin{pmatrix} 0 & 0 & 0 \\ a_4 & a_5 & a_6 \\ 0 & a_8 & -a_5 \end{pmatrix}$ *com* $a_4, a_8 \neq 0$;

(5) $W_{\mathrm{V}} = \begin{pmatrix} 0 & a_2 & a_3 \\ 0 & a_5 & a_6 \\ a_7 & a_8 & -a_5 \end{pmatrix}$ *com* $a_7 \neq 0$.

Demonstração. **(1)** Suponhamos que A_2 é uma matriz triangular superior. Como $A_2 \in \mathcal{N}_3$, os elementos da diagonal principal são zeros. Assim, tomando $g = E$ concluímos a demonstração de (1).

No resto da demonstração iremos considerar a seguinte $g \in GL_3$ com $gA_1g^{-1} = A_1$, onde $g_1 \neq 0$:

$$g = \begin{pmatrix} g_1 & g_2 & g_3 \\ 0 & g_1 & g_2 \\ 0 & 0 & g_1 \end{pmatrix} \text{ e } A_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}.$$

(2) Suponhamos que $a_4 = a_7 = 0$ e $a_8 \neq 0$. Tomando $g_2 = \dfrac{-g_1a_5}{a_8}$ e $g_3 = -(a_2 + \dfrac{a_1a_5 - a_5^2}{a_8})\dfrac{g_1}{a_8}$ obtemos

$$gA_2g^{-1} = \begin{pmatrix} * & 0 & * \\ 0 & 0 & * \\ 0 & a_8 & * \end{pmatrix}.$$

A condição $A_2 \in \mathcal{N}_3$ assegura a afirmação (2).

(3) Suponhamos agora $a_7 = a_8 = 0$ e $a_4 \neq 0$. Escolhendo $g_2 = \dfrac{-g_1a_1}{a_4}$ e $g_3 = \dfrac{g_1}{a_4^2}(a_1^2 + a_4a_6 + a_1(a_5 - a_9))$ teremos

$$gA_2g^{-1} = \begin{pmatrix} 0 & * & * \\ a_4 & * & 0 \\ 0 & 0 & * \end{pmatrix}.$$

Logo, segue de $A_2 \in \mathcal{N}_3$ a parte (3).

(4) Assumamos que $a_7 = 0$ e $a_4, a_8 \neq 0$. Considerando $g_2 = \dfrac{-g_1a_1}{a_4}$ e $g_3 = (\dfrac{a_1a_5}{a_4} - a_2)\dfrac{g_1}{a_8}$ iremos obter

$$gA_2g^{-1} = \begin{pmatrix} 0 & 0 & * \\ a_4 & * & * \\ 0 & a_8 & * \end{pmatrix}.$$

A afirmação (4) segue de $A_2 \in \mathcal{N}_3$.

(5) Por fim, supondo $a_7 \neq 0$ e tomando $g_2 = \dfrac{-g_1a_4}{a_7}$ e $g_3 = (\dfrac{a_4^2}{a_7} - a_1)\dfrac{g_1}{a_7}$, teremos

$$gA_2g^{-1} = \begin{pmatrix} 0 & * & * \\ 0 & * & * \\ a_7 & * & * \end{pmatrix}.$$

Assim, uma vez que $A_2 \in \mathcal{N}_3$, temos (5). □

Lema 2.2.9. *Sejam $A_1 = J_1$ e $A_2 \in \mathcal{N}_3$. Então, existe $g \in GL_3$ tal que $gA_1g^{-1} = A_1$ e gA_2g^{-1} é uma das matrizes a seguir:*

(1) $V_{\mathrm{I}} = \begin{pmatrix} 0 & a_2 & a_3 \\ 0 & 0 & a_6 \\ 0 & 0 & 0 \end{pmatrix}$;

(2) $V_{\mathrm{II}} = \begin{pmatrix} 0 & 0 & a_3 \\ 0 & a_5 & -a_5^2 \\ 0 & 1 & -a_5 \end{pmatrix}$;

(3) $V_{\mathrm{III}} = \begin{pmatrix} a_1 & a_2 & -a_1^2 \\ 0 & -a_1 & a_6 \\ 1 & 0 & 0 \end{pmatrix}$;

(4) $V_{\mathrm{IV}} = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & 0 & 0 \\ a_7 & a_8 & -a_1 \end{pmatrix}$ *com* $a_4 \neq 0$.

Demonstração. **(1)** Suponhamos que A_2 é uma matriz triangular superior. A condição $A_2 \in \mathcal{N}_3$ conclui a demonstração da parte (1).

No resto da demonstração iremos considerar a seguinte $g \in GL_3$ com $gA_1g^{-1} = A_1$, onde $g_1, g_9 \neq 0$:

$$g = \begin{pmatrix} g_1 & g_2 & g_3 \\ 0 & g_1 & 0 \\ 0 & 0 & g_9 \end{pmatrix} \text{ e } A_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}.$$

(2) Suponhamos que $a_4 = a_7 = 0$ e $a_8 \neq 0$. Tomando $g_1 = 1$, $g_3 = \dfrac{1}{a_8}((a_1 - a_5)g_2 - a_2)$ e $g_9 = \dfrac{1}{a_8}$ obtemos

$$gA_2g^{-1} = \begin{pmatrix} * & 0 & * \\ 0 & * & * \\ 0 & 1 & * \end{pmatrix}.$$

Assim, a afirmação da parte (2) segue da condição $A_2 \in \mathcal{N}_3$.

(3) Suponhamos agora $a_4 = 0$ e $a_7 \neq 0$. Tomando $g_2 = \dfrac{g_1 a_8}{a_7}$, $g_3 = \dfrac{g_1 a_9}{a_7}$ e $g_9 = \dfrac{g_1}{a_7}$, teremos

$$gA_2g^{-1} = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 1 & 0 & 0 \end{pmatrix}.$$

A condição $A_2 \in \mathcal{N}_3$ conclui a afirmação (3).

(4) Por fim suponhamos $a_4 \neq 0$. Considerando $g_2 = \dfrac{g_1 a_5}{a_4}$ e $g_3 = \dfrac{a_6 g_1}{a_4}$ obtemos

$$gA_2g^{-1} = \begin{pmatrix} * & * & * \\ a_4 & 0 & 0 \\ * & * & * \end{pmatrix}.$$

A conclusão da demonstração segue da condição $A_2 \in \mathcal{N}_3$. □

Nos Lemas 2.2.10, 2.2.11, 2.2.12, 2.2.13, 2.2.14, a seguir, iremos considerar $\underline{A} = (A_1, A_2, A_3)$ e $\underline{B} = (B_1, B_2, B_3)$ de $\mathcal{N}_3^3$ com certas matrizes A_1 e B_1. Além disso, consideraremos as matrizes A_i, B_i, onde $i = 2, 3$, como segue:

$$A_i = \begin{pmatrix} a_{i1} & a_{i2} & a_{i3} \\ a_{i4} & a_{i5} & a_{i6} \\ a_{i7} & a_{i8} & a_{i9} \end{pmatrix} \quad \text{e} \quad B_i = \begin{pmatrix} b_{i1} & b_{i2} & b_{i3} \\ b_{i4} & b_{i5} & b_{i6} \\ b_{i7} & b_{i8} & b_{i9} \end{pmatrix}.$$

Por simplicidade, denotaremos por $T_{i_1,\ldots,i_k}$ a igualdade $f(\underline{A}) = f(\underline{B})$ para $f = \mathrm{tr}(Y_{i_1} \cdots Y_{i_k})$ e por $\sigma_l(X)$ o l-ésimo coeficiente do polinômio característico de uma matriz X . Diremos que podemos expressar a variável $c \in \{a_{ij}, b_{ij} \mid i = 2, 3,\ 1 \leq j \leq 9\}$ de $T_{i_1,\ldots,i_k}$, se $T_{i_1,\ldots,i_k}$ puder ser reescrito como $cf = h$, onde f, h são polinômios em variáveis comutativas $\{a_{ij}, b_{ij}\}$, as quais não contêm c, e $f \neq 0$.

Diremos que a matriz $A \in \mathcal{N}_3$ tem tipo $V_{\mathrm{I}}, \ldots, V_{\mathrm{IV}}, W_{\mathrm{I}}, \ldots, W_{\mathrm{V}}$, respectivamente, se A é igual a matriz correspondente do Lema 2.2.9 ou Lema 2.2.8. Nas demonstrações dos Lemas 2.2.10, 2.2.11, 2.2.12, a seguir, diremos que o tipo do par (A_2, B_2) é (K, R) para alguns símbolos K, R pertencentes ao conjunto de símbolos $\{V_{\mathrm{I}}, \ldots, V_{\mathrm{IV}}, W_{\mathrm{I}}, \ldots, W_{\mathrm{V}}\}$ se

- o tipo de A_2 é K e os elementos de A_2 são o resultado das substituições $a_i \to a_{2i}$, onde $1 \leq i \leq 9$, na matriz correspondente do Lema 2.2.9 ou Lema 2.2.8.
- o tipo de B_2 é L e os elementos de B_2 são o resultado das substituições $a_i \to b_{2i}$, onde $1 \leq i \leq 9$, na matriz correspondente do Lema 2.2.9 ou Lema 2.2.8.

Passemos agora as formulações e demonstrações dos Lemas 2.2.10, 2.2.11, 2.2.12, 2.2.13 e 2.2.14.

Lema 2.2.10. *Consideremos* $\underline{A} = (J_2, A_2, A_3)$ *e* $\underline{B} = (J_2, B_2, B_3)$ *de* $\mathcal{N}_3^3$ *os quais não são separados por* $S_{3,3}$. *Então,* $\underline{A}$ *e* $\underline{B}$ *não são separados por* $P_{3,3}$.

Demonstração. Pelo Lema 2.2.8, podemos assumir que A_2 e B_2 têm um dos seguintes tipos: $W_{\rm I}, \ldots, W_{\rm V}$. A igualdade T_{112} implica $b_{27} = a_{27}$.

Suponhamos $a_{27} \neq 0$. Então, o par (A_2, B_2) tem tipo $(W_{\rm V}, W_{\rm V})$. Consequentemente, considerando T_{12} e T_{113} obtemos $b_{28} = a_{28}$ e $b_{37} = a_{37}$, respectivamente. Assim, como $a_{27} \neq 0$, pelas igualdades T_{1122}, T_{112212}, T_{1132} e T_{11213} teremos $b_{25} = a_{25}$, $b_{22} = a_{22}$, $b_{39} = a_{39}$ and $b_{34} = a_{34}$, respectivamente. Além disso fazendo uso das igualdades T_{13}, T_{221}, T_{1123}, $\mathrm{tr}(A_3) - \mathrm{tr}(B_3) = 0$, $\sigma_2(A_2) - \sigma_2(B_2) = 0$, T_{123}, T_{132} e T_{23}, podemos concluir que $b_{38} = a_{38}$, $b_{26} = a_{26}$, $b_{31} = a_{31}$, $b_{35} = a_{35}$, $b_{23} = a_{23}$, $b_{32} = a_{32}$, $b_{36} = a_{36}$ e $b_{33} = a_{33}$, respectivamente. Portanto, $\underline{A} = \underline{B}$, e o resultado é imediato.

Suponhamos agora $a_{27} = 0$. Então, a igualdade T_{12} implica $b_{28} = a_{24} + a_{28} - b_{24}$. Logo, de T_{1122} devemos ter $a_{24} - b_{24} = 0$ or $a_{28} - b_{24} = 0$. Dividiremos a demonstração em dois casos.

1. Seja $b_{24} \neq a_{24}$. Então, devemos ter $b_{24} = a_{28}$ e $b_{28} = a_{24}$. Essas restrições mostram que as únicas possibilidades para o tipo do par (A_2, B_2) são $(W_{\rm II}, W_{\rm III})$, $(W_{\rm III}, W_{\rm II})$ e $(W_{\rm IV}, W_{\rm IV})$. Obviamente, é suficiente considerar apenas a primeira e última possibilidades.

1.1. Assumamos que o tipo de (A_2, B_2) seja $(W_{\rm II}, W_{\rm III})$. Uma vez que $a_{28} \neq 0$, considerando T_{113}, T_{1123}, T_{1132}, T_{13} e T_{11213} obtemos $b_{37} = a_{37}$, $a_{34} = 0$, $b_{38} = 0$, $b_{34} = a_{38}$ e $a_{37} = 0$, respectivamente. Portanto, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$ e temos o resultado para este caso.

1.2. Assumamos agora que o tipo de (A_2, B_2) é $(W_{\rm IV}, W_{\rm IV})$. Daí, teremos $a_{24} \neq 0$ e $a_{28} \neq 0$. As igualdades T_{113} e T_{112212} implicam que $b_{37} = a_{37}$ e $a_{24}a_{28}(a_{24} - a_{28}) = 0$, o que é uma contradição.

2. Seja $b_{24} = a_{24}$. Logo, devemos ter $b_{28} = a_{28}$. É fácil ver que nessas condições existem apenas 4 possibilidades para o tipo do par (A_2, B_2), a saber $(W_{\rm I}, W_{\rm I})$, $(W_{\rm II}, W_{\rm II})$, $(W_{\rm III}, W_{\rm III})$ e $(W_{\rm IV}, W_{\rm IV})$.

2.1. Assumamos que o tipo de (A_2, B_2) é $(W_{\rm I}, W_{\rm I})$. Consequentemente, considerando as igualdades $\mathrm{tr}(A_3) = 0$, $\mathrm{tr}(B_3) = 0$, T_{13} e T_{113} obtemos $a_{39} = -a_{31} - a_{35}$, $b_{39} = -b_{31} - b_{35}$, $b_{38} = a_{34} + a_{38} - b_{34}$, e $b_{37} = a_{37}$, respectivamente.

Supondo $a_{37} \neq 0$ a partir das igualdades T_{123}, T_{132}, T_{1133}, T_{23}, podemos concluir que $b_{26} = a_{26}$, $b_{22} = a_{22}$, $a_{35} = ((a_{34} - b_{34})(a_{38} - b_{34}) + a_{37}b_{35})/a_{37}$, $b_{23} = ((a_{22} - a_{26})(a_{34} -$

$b_{34}) + a_{23}a_{37})/a_{37}$, respectivamente. Além disso, de T_{113313}, T_{331} podemos expressar b_{32} e b_{36}, respectivamente. Logo, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$ e temos o resultado.

Consideremos $a_{37} = 0$. Supondo $a_{34} - b_{34} \neq 0$ a igualdade T_{1133} implica $b_{34} = a_{38}$. Se $a_{34} = 0$, é imediato que $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Por outro lado, se $a_{34} \neq 0$, então T_{113313} implica $a_{38} = 0$ e também teremos $\underline{A}$, $\underline{B}$ não separados por $P_{3,3} \backslash S_{3,3}$.

Finalmente, sejam $a_{37} = 0$ e $a_{34} - b_{34} = 0$. Se $a_{34} = 0$ ou $a_{38} = 0$, o resultado é imediato. Por outro lado, se a_{34} e a_{38} são diferentes de zero, então considerando T_{3312} e T_{3321} obtemos $b_{26} = a_{26}$ e $b_{22} = a_{22}$, respectivamente. Donde $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

2.2. Assumamos que o tipo de (A_2, B_2) é $(W_{\mathrm{II}}, W_{\mathrm{II}})$. Uma vez que $a_{28} \neq 0$, considerando as igualdades T_{113}, T_{123}, T_{132}, $\mathrm{tr}(A_3) - \mathrm{tr}(B_3) = 0$, T_{1123} e T_{13} obtemos $b_{37} = a_{37}$, $b_{35} = a_{35}$, $b_{39} = a_{39}$, $b_{31} = a_{31}$, $b_{34} = a_{34}$, $b_{38} = a_{38}$, respectivamente.

Supondo $a_{37} \neq 0$ e aplicando T_{113313}, T_{331} e T_{23} podemos ver que $b_{32} = a_{32}$, $b_{36} = a_{36}$ e $b_{23} = a_{23}$, respectivamente. Logo, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

Agora suponhamos $a_{37} = 0$. Segue de T_{23} que $b_{36} = a_{36}$. Se $a_{34} = 0$, então $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$. Por outro lado se $a_{34} \neq 0$, então segue das igualdades $\sigma_2(A_3) - \sigma_2(B_3) = 0$ e T_{223} que $b_{32} = a_{32}$ e $b_{23} = a_{23}$, respectivamente. Portanto, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$.

2.3. Suponhamos que o tipo de (A_2, B_2) é $(W_{\mathrm{III}}, W_{\mathrm{III}})$. Daí, uma vez que $a_{24} \neq 0$, considerando as igualdades T_{113}, T_{123}, T_{132}, $\mathrm{tr}(A_3) - \mathrm{tr}(B_3) = 0$, T_{1132} e T_{13} obtemos $b_{37} = a_{37}$, $b_{31} = a_{31}$, $b_{35} = a_{35}$, $b_{39} = a_{39}$, $b_{38} = a_{38}$ e $b_{34} = a_{34}$, respectivamente.

Assumindo $a_{37} \neq 0$ e aplicando as igualdades T_{113313}, T_{23}, T_{331} e $\sigma_2(A_3) - \sigma_2(B_3) = 0$ podemos ver que $b_{32} = a_{32}$, $b_{23} = a_{23}$, $b_{36} = a_{36}$ e $b_{33} = a_{33}$, respectivamente. Logo, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$.

Agora assumamos que $a_{37} = 0$. Segue de T_{23} que $b_{32} = a_{32}$. Se $a_{38} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3}$. Por outro lado, se $a_{38} \neq 0$, então considerando as igualdades $\sigma_2(A_3) - \sigma_2(B_3) = 0$ e T_{223} obteremos $b_{36} = a_{36}$ e $b_{23} = a_{23}$, respectivamente. Decorre daí que $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

2.4. Assumamos que o tipo de (A_2, B_2) é $(W_{\mathrm{IV}}, W_{\mathrm{IV}})$. Como $a_{24} \neq 0$ e $a_{28} \neq 0$, segue das igualdades T_{113}, T_{13}, $\mathrm{tr}(A_3) = 0$, $\mathrm{tr}(B_3) = 0$, T_{221}, $\sigma_2(A_2) - \sigma_2(B_2) = 0$, T_{1123}, $\sigma_2(A_2) = 0$, T_{2213}, T_{2231}, T_{123} e T_{223} que $b_{37} = a_{37}$, $b_{38} = a_{34} + a_{38} - b_{34}$, $a_{39} = -a_{31} - a_{35}$, $b_{39} = -b_{31} - b_{35}$, $b_{25} = a_{25}$, $b_{26} = a_{26}$, $b_{34} = a_{34}$, $a_{26} = -a_{25}^2/a_{28}$, $b_{36} = a_{36} + a_{25}(a_{35} - b_{35})/a_{28}$, $b_{32} =$

$a_{32}+a_{25}(a_{31}-b_{31})/a_{28}$, $b_{35} = a_{35}+a_{24}(a_{31}-b_{31})/a_{28}$ e $b_{33} = a_{33}+a_{24}a_{25}^2(b_{31}-a_{31})/(a_{24}a_{28}^2)$, respectivamente.

Se $b_{31} = a_{31}$ teremos $\underline{A} = \underline{B}$ e o resultado torna-se óbvio. Assim, podemos supor $b_{31} \neq a_{31}$. Das igualdades T_{1133} e T_{331}, podemos concluir que $a_{37} = 0$ e $a_{38} = a_{34}-a_{24}a_{34}/a_{28}$, respectivamente.

Se $a_{28} = a_{24}$, então T_{132} implica que $a_{24}(a_{31} - b_{31}) = 0$, o que é um absurdo. Assim considerando $a_{28} \neq a_{24}$ e as igualdades T_{22123} e T_{2233} teremos $a_{25} = 0$ e $a_{33} = 0$, respectivamente. Segue de

$$T_{332} - a_{32}T_{132} = a_{28}(a_{32} - a_{36})(a_{31} - b_{31}) = 0$$

que $a_{36} = a_{32}$. Consequentemente, aplicando as igualdades T_{3312} e $\sigma_2(A_3) - \sigma_2(B_3) = 0$ podemos ver que $a_{35} = \frac{1}{2}(a_{31} + b_{31} + a_{24}(b_{31} - a_{31})/a_{28})$ e $a_{31}^2 = b_{31}^2$. Portanto, $b_{31} = -a_{31} \neq 0$ e a igualdade $\det(A_3) = 0$ implica $a_{24}a_{31}(a_{24} - a_{28}) = 0$, uma contradição. □

Lema 2.2.11. *Consideremos $\underline{A} = (J_2, A_2, A_3)$ e $\underline{B} = (J_1, B_2, B_3)$ em $\mathcal{N}_3^3$ os quais não são separados por $S_{3,3}$. Então, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$.*

Demonstração. Pelos Lemas 2.2.8 e 2.2.9, podemos assumir que A_2 e B_2 têm um dos seguintes tipos: $W_{\mathrm{I}}, \ldots, W_{\mathrm{V}}$ and $V_{\mathrm{I}}, \ldots, V_{\mathrm{IV}}$, respectivamente. Igualdades T_{112} e T_{113} implicam que $a_{27} = a_{37} = 0$.

1. Suponhamos $a_{28} \neq 0$. Então, as igualdades T_{1122} e T_{12} implicam que $a_{24} = 0$ e $b_{24} = a_{28}$, respectivamente. Portanto, o tipo de (A_2, B_2) é $(W_{\mathrm{II}}, V_{\mathrm{IV}})$. Consequentemente, considerando as igualdades T_{1123}, T_{13}, T_{221}, T_{123}, $\sigma_2(A_2) - \sigma_2(B_2) = 0$, $\mathrm{tr}(A_3) = 0$, $\mathrm{tr}(B_3) = 0$, T_{132} e T_{23} obtemos $a_{34} = 0$, $b_{34} = a_{38}$, $b_{21} = 0$, $b_{31} = a_{35}$, $b_{22} = -b_{23}b_{27}/a_{28}$, $a_{39} = -a_{31} - a_{35}$, $b_{39} = -a_{35}-b_{35}$, $b_{35} = -a_{31}-a_{35}-b_{27}b_{36}/a_{28}$ e $b_{32} = (a_{28}a_{36}-b_{27}b_{33}-b_{28}b_{36}-b_{23}b_{37})/a_{28}+a_{38}b_{23}b_{27}/a_{28}^2$, respectivamente.

Se $b_{28} \neq 0$ aplicando as igualdades $\det(B_2) = 0$, T_{223} e T_{2213} concluímos que $b_{23} = b_{33} = b_{36} = 0$. Logo, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$.

Seja $b_{28} = 0$. Observemos que se $b_{23} = 0$, então $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3.3}$. Assim, podemos assumir que $b_{23} \neq 0$. Daí, a partir de T_{2231} e T_{223} obtemos $b_{37} = a_{38}b_{27}/a_{28}$ e $b_{38} = (a_{35}b_{27} + 2b_{27}b_{35})/a_{28} + b_{27}^2b_{36}/a_{28}^2$, respectivamente. Portanto, $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$.

2. Agora suponhamos $a_{28} = 0$. A igualdade T_{12} implica que $b_{24} = a_{24}$. Essas restrições mostram que as únicas possibilidades para o tipo do par (A_2, B_2) são $(W_{\mathrm{I}}, V_{\mathrm{I}})$, $(W_{\mathrm{I}}, V_{\mathrm{II}})$, $(W_{\mathrm{I}}, V_{\mathrm{III}})$ e $(W_{\mathrm{III}}, V_{\mathrm{IV}})$.

2.1. Assumamos que o tipo de (A_2, B_2) é $(W_{\mathrm{I}}, V_{\mathrm{I}})$. Considerando as igualdades T_{13}, $\mathrm{tr}(A_3) = 0$ e $\mathrm{tr}(B_3) = 0$ obtemos $b_{34} = a_{34} + a_{38}$, $a_{39} = -a_{31} - a_{35}$ e $b_{39} = -b_{31} - b_{35}$, respectivamente. Se $a_{34} = 0$, a igualdade T_{123} implica que $b_{26}b_{37} = 0$. Por outro lado, se $a_{34} \neq 0$, aplicando T_{1133} e T_{123} obtemos $a_{38} = 0$ e $b_{26}b_{37} = 0$, respectivamente. Logo, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$ em ambos os casos.

2.2. Suponhamos que o tipo de (A_2, B_2) é $(W_{\mathrm{I}}, V_{\mathrm{II}})$. Consequentemente, considerando as igualdades T_{13}, $\mathrm{tr}(A_3) = 0$ e $\mathrm{tr}(B_3) = 0$ teremos $b_{34} = a_{34} + a_{38}$, $a_{39} = -a_{31} - a_{35}$ e $b_{39} = -b_{31} - b_{35}$, respectivamente.

Seja $a_{34} \neq 0$. Segue de T_{1133} e T_{331} que $a_{38} = 0$ e $b_{35} = a_{31} + a_{35} - b_{31} - b_{36}b_{37}/a_{34}$, respectivamente. Assim, supondo $b_{25} \neq 0$, a igualdade T_{123} implica que $a_{34} = b_{25}b_{37}$. Por outro lado, se $b_{25} = 0$, a igualdade T_{223} implica que $b_{23} = 0$. Portanto, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$ em ambos os casos.

Seja $a_{34} = 0$. Se $b_{25} \neq 0$, segue de T_{123} que $a_{38} = b_{25}b_{37}$. Por outro lado, supondo $b_{25} = 0$, a igualdade T_{223} implica que $a_{38}b_{23} = 0$. Em ambos os caso temos $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

2.3. Assumamos que o tipo de (A_2, B_2) é $(W_{\mathrm{I}}, V_{\mathrm{III}})$. Considerando as igualdades T_{221}, $\det(B_2) = 0$, T_{132}, T_{1133} e T_{3321} obtemos que b_{26}, b_{21}, b_{36}, $a_{34}a_{38}$, $b_{33}b_{34}$ são iguais a zero. Logo, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

2.4. Suponhamos que o tipo de (A_2, B_2) é $(W_{\mathrm{III}}, V_{\mathrm{IV}})$. Uma vez que $a_{24} \neq 0$, considerando as igualdades T_{221}, T_{1132}, T_{13}, T_{123}, $\sigma_2(A_2) - \sigma_2(B_2) = 0$, $\mathrm{tr}(A_3) = 0$, e $\mathrm{tr}(B_3) = 0$ temos $b_{21} = 0$, $a_{38} = 0$, $b_{34} = a_{34}$, $b_{31} = a_{31}$, $b_{22} = -b_{23}b_{27}/a_{24}$, $a_{39} = -a_{31} - a_{35}$, e $b_{39} = -a_{31} - b_{35}$, respectivamente.

Se $b_{28} \neq 0$, então segue das igualdades $\det(B_2) = 0$, T_{223} e T_{2213} que $b_{23} = b_{33} = b_{36} = 0$, donde $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Assim, podemos assumir que $b_{28} = 0$. Se $b_{23} = 0$ é imediato que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3.3}$. Por outro lado, se $b_{23} \neq 0$ as igualdades T_{2231}, T_{132}, T_{223} implicam que $b_{37} = a_{34}b_{27}/a_{24}$, $b_{35} = a_{35} - b_{27}b_{36}/a_{24}$ e $b_{38} = (a_{31}b_{27} + 2a_{35}b_{27})/a_{24} - b_{27}^2 b_{36}/a_{24}^2$, respectivamente. Portanto, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. $\square$

Lema 2.2.12. *Sejam* $\underline{A} = (J_2, A_2, A_3)$ *e* $\underline{B} = (0, B_2, B_3)$ *em* $\mathcal{N}_3^3$ *os quais não são separados por* $S_{3,3}$*. Então,* $\underline{A}$ e $\underline{B}$ *não são separados por* $P_{3,3}$*.*

Demonstração. Pelo Lema 2.2.8, podemos assumir que A_2 tem um dos tipos a seguir: $W_{\mathrm{I}}, \ldots, W_{\mathrm{V}}$. Considerando as igualdades T_{112}, T_{12} e T_{1122} temos que $a_{27} = 0$, $a_{28} = -a_{24}$ e $a_{24} = 0$, respectivamente. Daí, o tipo de A_2 é W_{I}. Consequentemtente, aplicando as igualdades T_{13}, T_{113} e T_{1133} teremos $a_{38} = -a_{34}$, $a_{37} = 0$, $a_{34} = 0$, respectivamente. Donde segue que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. □

Lema 2.2.13. *Consideremos* $\underline{A} = (J_1, A_2, A_3)$ *e* $\underline{B} = (J_1, B_2, B_3)$ *em* $\mathcal{N}_3^3$*, os quais não são separados por* $S_{3,3}$*. Então,* $\underline{A}$ e $\underline{B}$ *não são separados por* $P_{3,3}$*.*

Demonstração. Pelo Lema 2.2.9, podemos assumir que A_2 e B_2 têm um dos seguintes tipos: $V_{\mathrm{I}}, \ldots, V_{\mathrm{IV}}$. A igualdade T_{12} implica que $b_{24} = a_{24}$, portanto podemos ver que as únicas possibilidades para o tipo de (A_2, B_2) são $(V_{\mathrm{I}}, V_{\mathrm{I}})$, $(V_{\mathrm{I}}, V_{\mathrm{II}})$, $(V_{\mathrm{I}}, V_{\mathrm{III}})$, $(V_{\mathrm{II}}, V_{\mathrm{II}})$, $(V_{\mathrm{II}}, V_{\mathrm{III}})$, $(V_{\mathrm{III}}, V_{\mathrm{III}})$ e $(V_{\mathrm{IV}}, V_{\mathrm{IV}})$. Ademais, considerando as igualdades T_{13}, $\mathrm{tr}(A_3) = 0$, e $\mathrm{tr}(B_3) = 0$ obtemos que $b_{34} = a_{34}$, $a_{39} = -a_{31} - a_{35}$, e $b_{39} = -b_{31} - b_{35}$.

1. Assumamos que o tipo de (A_2, B_2) é $(V_{\mathrm{I}}, V_{\mathrm{I}})$. Notemos que se $b_{26} = 0$, a igualdade T_{123} implica que $a_{26} = 0$ ou $a_{37} = 0$ e em ambos os casos teremos $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Por outro lado, se $b_{26} \neq 0$ considerando as igualdades T_{23} e T_{123} obtemos $b_{38} = (a_{22}a_{34} + a_{23}a_{37} + a_{26}a_{38} - a_{34}b_{22} - b_{23}b_{37})/b_{26}$ e $b_{37} = a_{26}a_{37}/b_{26}$, respectivamente. Além disso, se $a_{26} = 0$ ou $a_{37} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Logo, podemos assumir que $a_{26}, a_{37} \neq 0$. Daí, segue das igualdades T_{223} e T_{331}, que $b_{22} = a_{22}$ e $a_{36} = a_{34}(-a_{31} - a_{35} + b_{31} + b_{35})/a_{37} + a_{26}a_{36}/b_{26}$. Portanto, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

2. Suponhamos que o tipo de (A_2, B_2) é $(V_{\mathrm{I}}, V_{\mathrm{II}})$. Inicialmente, iremos assumir $a_{37} \neq 0$. Então, considerando as igualdades T_{331} e T_{123} teremos $a_{36} = (a_{34}(-a_{31} - a_{35} + b_{31} + b_{35}) + b_{36}b_{37})/a_{37}$, $a_{26} = b_{25}(a_{34} - b_{25}b_{37})/a_{37}$, respectivamente. Daí, a igualdade T_{223} implica que $b_{23} - a_{22}b_{25} = 0$ ou $a_{34} - b_{25}b_{37} = 0$, e portanto $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

Por outro lado, seja $a_{37} = 0$. Se $b_{23} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Além disso, se $b_{23} \neq 0$, então a igualdade T_{223} implica $a_{34} = b_{25}b_{37}$ e também teremos que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

3. Assumamos que o tipo de (A_2, B_2) é $(V_{\mathrm{I}}, V_{\mathrm{III}})$. Considerando as igualdades T_{221}, $\det(B_2) = 0$, e T_{132}, obtemos $b_{26} = b_{21} = b_{36} = 0$. Assim, segue de T_{123} e T_{3321} que

$a_{26}a_{37} = 0$ e $a_{34}b_{33} = 0$, respectivamente. Logo, concluímos que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

4. Suponhamos agora que o tipo de (A_2, B_2) é $(V_{\text{II}}, V_{\text{II}})$. Segue da igualdade T_{23} que $b_{36} = a_{36} + a_{25}(a_{31} + 2a_{35}) - a_{25}^2 a_{38} + a_{23}a_{37} - b_{25}(b_{31} + 2b_{35}) \; - b_{23}b_{37} + b_{25}^2 b_{38}$.

Assumindo que $a_{25} \neq 0$, a igualdade T_{123} implica que $a_{37} = (a_{25}a_{34} + b_{25}(-a_{34} + b_{25}b_{37}))/a_{25}^2$, e T_{223} acarreta $a_{25}b_{23} - a_{23}b_{25} = 0$ ou $-a_{34} + b_{25}b_{37} = 0$. Além disso, se $-a_{34} + b_{25}b_{37} = 0$, então, podemos assumir $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.Por outro lado, se $-a_{34} + b_{25}b_{37} \neq 0$, então $b_{23} = a_{23}b_{25}/a_{25}$ e podemos expressar a_{38} pela igualdade T_{3312}. Assim, uma vez que $T_{332231} = (a_{23}b_{25}(a_{34} - b_{25}b_{37})/a_{25})T_{331}$, podemos concluir que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

Agora assumamos que $a_{25} = 0$. Se $a_{34} = b_{25} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Em contrapartida, se $a_{34} \neq 0$ e $b_{25} = 0$, então segue de T_{223} e T_{331} que $b_{23} = a_{23}$ e $a_{31} = (a_{34}(-a_{35} + b_{31} + b_{35}) + (a_{37} - b_{37})(-a_{36} + a_{23}b_{37}))/a_{34}$. Logo, também concluíremos que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Finalmente, se $b_{25} \neq 0$, então T_{123} assegura que $a_{34} = b_{25}b_{37}$ e T_{223} implica $a_{23} = 0$ ou $b_{37} = 0$. Daí, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

5. Suponhamos que o tipo de (A_2, B_2) is $(V_{\text{II}}, V_{\text{III}})$. Considerando as igualdades T_{221}, $\det(B_2) = 0$, e T_{132} obtemos $b_{26} = b_{21} = b_{36} = 0$. Assim, $T_{332231} = (a_{31}a_{34} + a_{34}a_{35} + a_{36}a_{37})T_{223} + a_{34}b_{22}T_{3321}$. Logo, as igualdades T_{223} e T_{3321} implicam que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

6. Assumamos que o tipo de (A_2, B_2) é $(V_{\text{III}}, V_{\text{III}})$. Segue das igualdades T_{221} e T_{132} que $b_{26} = a_{26}$ e $b_{36} = a_{21}a_{34} + a_{36} - a_{34}b_{21}$, respectivamente.

Consideremos $a_{26} = 0$. Então, aplicando as igualdades $\det(A_2) = 0$, $\det(B_2) = 0$, e T_{23} teremos $a_{21} = b_{21} = 0$ e $b_{33} = a_{33} + a_{22}a_{34} - a_{34}b_{22}$. Daí, se $a_{34} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Em contrapartida, se $a_{34} \neq 0$, as igualdades T_{331} e T_{3321} asseguram que $b_{35} = (a_{31}a_{34} + a_{34}(a_{35} - b_{31}) + a_{36}(a_{37} - b_{37}))/a_{34}$ e $a_{22} = (-a_{31}a_{36} + a_{34}^2 b_{22} + a_{36}b_{31})/a_{34}^2$, respectivamente. Por fim, T_{223} implica que $a_{36} = 0$ ou $a_{31} - b_{31} = 0$. Em ambos os casos temos que $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

Agora suponhamos que $a_{26} \neq 0$. Aplicando as igualdades $\det(A_2) = \det(B_2) = 0$, T_{123}, T_{2213}, T_{2231}, e T_{23} obtemos $a_{22} = a_{21}^3/a_{26}$, $b_{22} = b_{21}^3/a_{26}$, $b_{37} = (-a_{21}a_{34} + a_{34}b_{21} + a_{26}a_{37})/a_{26}$, $b_{35} = ((a_{21} - b_{21})(a_{36} - a_{34}b_{21}) + a_{26}a_{35})/a_{26}$, $b_{31} = (a_{21}a_{34}(a_{21} - b_{21}) + a_{26}(a_{31} - a_{21}a_{37} + a_{37}b_{21}))/a_{26}$ e $b_{38} = (a_{21}^3 a_{34} + a_{21}b_{21}(a_{36} - a_{34}b_{21}) + b_{21}^2(-a_{36} + a_{34}b_{21}) - a_{21}^2(a_{26}a_{37} +$

$a_{34}b_{21}) + a_{21}a_{26}(a_{31} - a_{35} + a_{37}b_{21}) + a_{26}(a_{33} - a_{31}b_{21} + a_{35}b_{21} - b_{33}) + a_{26}^2 a_{38})/a_{26}^2$, respectivamente. Se $a_{34} \neq 0$, então pelas igualdades T_{3312} e T_{223} podemos expressar b_{33} e b_{32}. Portanto, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3}$. Logo, podemos assumir que $a_{34} = 0$. Das igualdades T_{22123} e T_{223} podemos expressar b_{33} e b_{32}. Consequentemente, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3}$.

7. Por fim, suponhamos que o tipo de (A_2, B_2) é $(V_{\mathrm{IV}}, V_{\mathrm{IV}})$. Uma vez que $a_{24} \neq 0$, analisando as igualdades T_{221}, T_{123}, $\sigma_2(A_2) = 0$, $\sigma_2(B_2) = 0$, T_{132}, e T_{23} podemos concluir que $b_{21} = a_{21}$, $b_{31} = a_{31}$, $a_{22} = (-a_{21}^2 - a_{23}a_{27})/a_{24}$, $b_{22} = (-a_{21}^2 - b_{23}b_{27})/a_{24}$, $b_{35} = (a_{27}a_{36} + a_{24}a_{35} - b_{27}b_{36})/a_{24}$ e $b_{32} = (-a_{23}a_{27}a_{34} - a_{21}a_{27}a_{36} + a_{34}b_{23}b_{27} + a_{24}^2 a_{32} + a_{21}b_{27}b_{36} + a_{24}(a_{27}a_{33} + a_{28}a_{36} + a_{23}a_{37} - b_{27}b_{33} - b_{28}b_{36} - b_{23}b_{37}))/a_{24}^2$, respectivamente.

7.1. Consideremos $a_{23} \neq 0$. Pelas igualdades $\det(A_2) = 0$ e T_{2231} teremos que $a_{28} = (a_{21}^3 + a_{21}a_{23}a_{27})/(a_{23}a_{24})$ e $a_{37} = (a_{23}a_{27}a_{34} - a_{34}b_{23}b_{27} + a_{24}b_{23}b_{37})/(a_{23}a_{24})$.

Suponhamos $b_{23} = 0$. Assim, a igualdade $\det(B_2) = 0$ implica que $a_{21} = 0$, e podemos expressar a_{38} da igualdade T_{223}. Se $b_{28} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Por outro lado, se $b_{28} \neq 0$, então as igualdades T_{2213} e T_{22123} nos permitem concluir que $b_{36} = b_{33} = 0$, e portanto $\underline{A}$, $\underline{B}$ não são separados por $P_{3,3}$.

Supondo agora $b_{23} \neq 0$. Pela igualdade $\det(B_2) = 0$ teremos $b_{28} = (a_{21}^3 + a_{21}b_{23}b_{27})/(a_{24}b_{23})$. Se $a_{21} = 0$ podemos expressar b_{38} pela igualdade T_{223} e veremos $T_{332231} = (-a_{24}a_{27}(a_{31} + 2a_{35}) - a_{27}^2 a_{36} + a_{24}^2 a_{38})(a_{23}/a_{24})T_{331}$. Logo, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Por outro lado, se $a_{21} \neq 0$, então as igualdades T_{2213}, T_{22123} implicam que $b_{36} = a_{36}b_{23}/a_{23}$, $b_{33} = a_{33}b_{23}/a_{23}$ e que podemos expressar b_{38} por T_{223}. Portanto, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3}$.

7.2. Por fim, seja $a_{23} = 0$. A igualdade $\det(A_2) = 0$ implica que $a_{21} = 0$.

Seja $b_{23} \neq 0$. Uma vez que $a_{24} \neq 0$, considerando as igualdades $\det(B_2) = 0$, T_{2231} obteremos que $b_{28} = 0$, $b_{37} = a_{34}b_{27}/a_{24}$, e daí podemos expressar b_{38} por T_{223}. Se $a_{28} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Assim, podemos assumir que $a_{28} \neq 0$. Segue de T_{2213} e T_{22123} que $a_{36} = a_{33} = 0$, e portanto $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3}$.

Por outro lado, seja $b_{23} = 0$. Se $b_{28} \neq 0$, então segue das igualdades T_{223} e T_{2213} que $b_{33} = a_{28}a_{33}/b_{28}$ e $b_{36} = a_{28}a_{36}/b_{28}$, respectivamente. Logo, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Assim, podemos assumir que $b_{28} = 0$. É fácil ver que se $a_{28} = 0$, então $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. Sendo $a_{28} \neq 0$, então as igualdades T_{223} e T_{2213} implicam que $a_{33} = a_{36} = 0$, e portanto $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. $\square$

Lema 2.2.14. *Consideremos* $\underline{A} = (J_1, A_2, A_3)$ *e* $\underline{B} = (0, B_2, B_3)$ *em* $\mathcal{N}_3^3$ *os quais não são separados por* $S_{3,3}$. *Então,* $\underline{A}$ *e* $\underline{B}$ *não são separados por* $P_{3,3}$.

Demonstração. Pelo Lema 2.2.9, podemos assumir que A_2 tem um dos seguintes tipo: $V_{\mathrm{I}}, \dots, V_{\mathrm{IV}}$. As igualdades T_{12} e T_{13} implicam que $a_{24} = a_{34} = 0$. Então, segue da igualdade T_{221} que $a_{26} = 0$ ou $a_{27} = 0$.

Suponhamos $a_{26} = 0$ e $a_{27} \neq 0$. Logo, o tipo de A_2 é V_{III}. A igualdade T_{132} nos mostra que $a_{36} = 0$. Assim, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$.

Consideremos $a_{27} = 0$. Logo, o tipo de A_2 é V_{I} ou V_{II}. Em ambos os casos da igualdade temos $a_{36}a_{37} = 0$. Portanto, $\underline{A}$ e $\underline{B}$ não são separados por $P_{3,3} \backslash S_{3,3}$. $\square$

Os resultados obtidos nesta seção foram publicados na revista Linear Algebra and Its Applications sob o título "Separating invariants of three nilpotent 3×3 matrices" (vide [10]), cujo principal resultado pode ser sintetizado, como a junção dos Teoremas 2.2.5 e 2.2.6, no teorema a seguir.

Teorema 2.2.15. *Suponhamos que* $n = d = 3$ *e que* $\mathbb{F}$ *é um corpo algebricamente fechado de característica zero. Então,*

(a) $P_{3,3}$ *é um conjunto gerador minimal para a álgebra de invariantes* $\mathcal{O}(3, 3)$.

(b) $S_{3,3}$ *é um conjunto separador minimal para a álgebra de invariantes* $\mathcal{O}(3, 3)$;

3 Semi-invariantes separadores de matrizes 2×2

Todos os espaços vetoriais serão considerados sobre um corpo infinito $\mathbb{F}$ de característica $\operatorname{char}\mathbb{F} \geq 0$, a menos que especifiquemos o contrário. Este capítulo será dedicado a aprensentar a construção da álgebra de semi-invariantes $SI(m,p,q)$, a qual será definida a seguir (veja Exemplo 3.1.1), bem como a obtenção de um conjunto separador minimal da mesma (vide Teorema 3.4.17). Iniciaremos, apresentando esta construção, bem como uma série de definições e resultados auxiliares.

3.1 Semi-invariantes de Matrizes

Nesta seção iremos apresentar a construção da álgebra de semi-invariantes de matrizes e algumas de suas propriedades básicas. Destacaremos que esta álgebra generaliza as álgebras $S(n,m)$ e $R(n,m)$ apresentadas nos Exemplos 1.3.2 e 1.3.4, respectivamente.

Exemplo 3.1.1. Sejam $p,q,m \geq 0$ não todos nulos. O grupo $G = SL(n_1) \times SL(n_2)$ age diagonalmente em

$$\mathcal{H} = \mathcal{H}_{\underline{n}}(m,p,q) = (M_{n_1 \times n_2})^m \oplus (M_{n_1})^p \oplus (M_{n_2})^q$$

como segue:

$$(g_1,g_2) \cdot \underline{A} = (g_1A_1g_2^{-1},\ldots,g_1A_mg_2^{-1}; g_1A'_1g_1^{-1},\ldots,g_1A'_pg_1^{-1}; g_2A''_1g_2^{-1},\ldots,g_2A''_qg_2^{-1})$$

para $g_1 \in SL(n_1)$, $g_2 \in SL(n_2)$, e $\underline{A} = (A_1,\ldots A_m; A'_1,\ldots,A'_p; A''_1,\ldots,A''_q)$ de $\mathcal{H}$.

Então, para $\underline{n} = (n_1,n_2)$, a álgebra de semi-invariantes de matrizes é a álgebra de invariantes dada por:

$$SI_{\underline{n}}(m,p,q) = \mathbb{F}[\mathcal{H}]^G$$

É de fácil verificação que $R(n,m) = SI_{(n,n)}(m,0,0)$. Além disso, da Observação 3.1.2 a seguir, podemos concluir que $S(n,m) = SI_{(n,n)}(0,m,0) \simeq SI_{(n,n)}(0,0,m)$. Assim, de fato a álgebra de semi-invariantes de matrizes generaliza as álgebras $S(n,m)$ e $R(n,m)$. Além disso, uma vez que $SL(n_1) \times SL(n_2)$ é um grupo redutivo, temos que a álgebra $SI_{\underline{n}}(m,p,q)$ possui um conjunto gerador, e consequentemente separador, finito.

Antes dos próximmos resultado, fixemos a seguinte notação. Dada A uma matriz 2×2 sobre um anel comutativo, definimos

$$A^* = -JA^TJ, \quad \text{onde} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Notemos que $AA^* = \det(A)E$, onde E representa a matriz identidade 2×2.

Observação 3.1.2. O mapa linear $\iota : \mathcal{H}(m,p,q) \to \mathcal{H}(m,q,p)$ definido por

$$(A_1, A_2, \ldots, A_m; A'_1, \ldots, A'_p; A''_1, \ldots, A''_q) \to (A^*_m, \ldots, A^*_2, A^*_1; A''_1, \ldots, A''_q; A'_1, \ldots, A'_p)$$

induz o isomorfismo de álgebras de invariantes $\iota^* : SI(m,q,p) \to SI(m,p,q)$, uma vez que $\iota((g_1,g_2) \cdot \underline{A}) = (g_2,g_1) \cdot \iota(\underline{A})$ para todo par $(g_1,g_2) \in G$.

O anel de coordenadas $\mathbb{F}[\mathcal{H}]$ da variedade afim $\mathcal{H}$ é o anel polinomial livremente gerado por

$$x^k_{ij} \ (i \in [n_1],\ j \in [n_2],\ k \in [m]), \quad y^k_{ij} \ (i,j \in [n_1],\ k \in [p]), \quad z^k_{ij} \ (i,j \in [n_2],\ k \in [q]),$$

onde para todo $s \in \mathbb{N}$, temos $[s] = \{1, 2, \cdots, s\}$. Assim, os elementos de $\mathbb{F}[\mathcal{H}]$ podem ser interpretados como funções polinomiais de $\mathcal{H}$ em $\mathbb{F}$ da seguinte maneira:

$$x^k_{ij}(\underline{A}) = (A_k)_{ij}, \quad y^k_{ij}(\underline{A}) = (A'_k)_{ij}, \quad z^k_{ij}(\underline{A}) = (A''_k)_{ij},$$

onde $(A)_{ij}$ denota a (i,j)-ésima entrada da matriz A.

Denotaremos por

$$X_k = (x^k_{ij})_{i \in [n_1],\, j \in [n_2]}, \quad Y_k = (y^k_{ij})_{i,j \in [n_1]}, \quad \text{e} \quad Z_k = (z^k_{ij})_{i,j \in [n_2]}$$

as matrizes genéricas $n_1 \times n_2$, $n_1 \times n_1$ e $n_2 \times n_2$, respectivamente.

Para um monômio $c \in \mathbb{F}[\mathcal{H}]$ denotamos por $\operatorname{mdeg} c$ seu multigrau, isto é, $\operatorname{mdeg} c = \underline{d} = (d_1, \ldots, d_m; d'_1, \ldots, d'_p; d''_1, \ldots, d''_q)$, onde d_k (d'_k e d''_k, respectivamente) é o grau total do monômio c em x^k_{ij} (y^k_{ij} e z^k_{ij}, respectivamente) para todos i, j. Obviamente, a álgebra $SI_{\underline{n}}(m,p,q)$ possui uma $\mathbb{N}^{m+p+q}$-graduação dada pelos multigraus.

Em particular, para $n_1 = n_2 = 2$ escreveremos $SI(m,p,q)$ para a álgebra $SI_{(2,2)}(m,p,q)$ e denotaremos por $\mathcal{H}(m,p,q)$ a variedade afim $\mathcal{H}_{(2,2)}(m,p,q)$.

Uma vez apresentada a álgebra $SI(m,p,q)$, concentraremos nossos esforços em determinar um conjunto separador minimal para esta álgebra. Contudo, antes de passarmos a este estudo, iremos estabelecer alguns conceitos e resultados que irão nos auxiliar na obtenção de tal conjunto.

3.2 Equivalências

Ao longo desta seção iremos assumir que $\mathbb{F}$ é um corpo arbitrário (possivelmente finito) e G um grupo arbitrário. Nosso objetivo aqui será estabelecer o conceito de polarização de um invariante, bem como estabelecer algumas relações de equivalências. Iniciaremos este estudo com o caso de um espaço vetorial, e em seguida iremos generalizar estes conceitos para o caso de múltiplos espaços.

3.2.1 O caso de um único espaço

Sejam $\mathcal{V}$ e $\mathcal{W}$ G-módulos de dimensão finita sobre $\mathbb{F}$, com bases fixadas e denotemos $\dim \mathcal{V} = n_1$, $\dim \mathcal{W} = n_2$. Dado $v \in \mathcal{V}$, escrevemos $(v)_i$ para a i-ésima coordenada de v com respeito a base fixada de $\mathcal{V}$, e analogamente definimos $(w)_j$ para $w \in \mathcal{W}$. Para $m \geq 1$, a ação diagonal de G no $\mathcal{H} = \mathcal{W} \oplus \mathcal{V}^m$ é definida por $g \cdot \underline{v} = (g \cdot v_0, g \cdot v_1, \ldots, g \cdot v_m)$ para todos $g \in G$, $\underline{v} = (v_0, v_1, \ldots, v_m) \in \mathcal{H}$ com $v_0 \in \mathcal{W}$ e $v_1, \ldots, v_m \in \mathcal{V}$.

O anel de coordenadas $\mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]$ é o anel polinomial livremente gerado por $x_{k,i}$ ($k \in [m]$, $i \in [n_1]$) e y_j ($j \in [n_2]$) de $(\mathcal{W} \oplus \mathcal{V}^m)^*$, onde $x_{k,i}(\underline{v}) = (v_k)_i$ e $y_j(\underline{v}) = (v_0)_j$ para cada $\underline{v} \in \mathcal{W} \oplus \mathcal{V}^m$. Para um monômio $c \in \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]$ denotemos por $\operatorname{mdeg} c$ seu multigrau, isto é, $\operatorname{mdeg} c = (d_0, d_1, \ldots, d_m)$, onde para $k \in [m]$ temos que d_k é o grau total do monômio c em $x_{k,i}$ ($i \in [n_1]$), e d_0 é o grau total de c em y_j, ($j \in [n_2]$). Obviamente, a álgebra $\mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]^G$ admite uma $\mathbb{N}$-graduação pelo grau e uma $\mathbb{N}^{m+1}$-graduação pelo multigrau.

Consideremos a noção clássica de polarização de um invariante, dada em [24].

Definição 3.2.1 (Polarização Pol_m^l)**.** Sejam $l \geq 1$ e $a_{k,r}$ indeterminadas comutativas para todos $k \in [m]$ e $r \in [l]$. Consideremos o homomorfismo de $\mathbb{F}$-álgebras $\Phi : \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m] \to \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^l][a_{1,1}, \ldots, a_{m,l}]$ dado por:

$$\begin{aligned} \Phi(x_{k,i}) &= \sum_{r=1}^{l} a_{k,r} x_{r,i} \quad (k \in [m],\ i \in [n_1]), \\ \Phi(y_j) &= y_j \qquad\qquad\quad (j \in [n_2]). \end{aligned}$$

Então, para $f \in \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]$ existe um subconjunto $P = \mathrm{Pol}_m^l(f) \subset \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^l]$ de elementos não nulos, tais que

$$\Phi(f) = \sum_{h \in P} \underline{a}^{\Delta(h)} h,$$

onde $\{\underline{a}^{\Delta(h)}\}$ são monômios, dois a dois diferentes, em $\{a_{k,r}\}$. Em outras palavras, $\mathrm{Pol}_m^l(f)$ é o conjunto de todos os coeficiente não nulos de $\Phi(f)$, considerados como polinômios nas indeterminadas $\{a_{k,r}\}$.

A próxima observação encontra-se provada na Seção 1 de [24].

Observação 3.2.2. Suponhamos que as condições da Definição 3.2.1 são satisfeitas. Então,

(a) Dado $\alpha_{k,r}$ para todos $k \in [m]$ e $r \in [l]$, consideremos o homomorfismo de $\mathbb{F}$-álgebras $\mu : \mathbb{F}[a_{1,1}, \ldots, a_{m,l}] \to \mathbb{F}$, dado por $\mu(a_{k,r}) = \alpha_{k,r}$. A composição $\widehat{\Phi} = \mu \circ \Phi$ é o homomorfismo $\widehat{\Phi} : \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m] \to \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^l]$. Então, para cada $\underline{v} \in \mathcal{W} \oplus \mathcal{V}^l$, temos

$$\widehat{\Phi}(f)(\underline{v}) = f\left(v_0, \sum_{r=1}^{l} \alpha_{1,r} v_r, \ldots, \sum_{r=1}^{l} \alpha_{m,r} v_r\right) = \sum \underline{\alpha}^{\Delta(h)} h(\underline{v}), \tag{3.1}$$

onde o último somatório é tomado sobre todos $h \in \mathrm{Pol}_m^l(f)$ e $\underline{\alpha}^{\Delta(h)}$ significa $\mu(\underline{a}^{\Delta(h)})$.

(b) Se f é $\mathbb{N}$-homogêneo, então cada $h \in \mathrm{Pol}_m^l(f)$ é também $\mathbb{N}$-homogêneo com $\deg(f) = \deg(h)$. Além disso, se f e $\mathbb{N}^{m+1}$-homogêneo, então cada $h \in \mathrm{Pol}_m^l(f)$ e $\mathbb{N}^{l+1}$-homogêneo.

(c) Se $f \in \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]^G$, então $\mathrm{Pol}_m^l(f) \subset \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^l]^G$.

No exemplo a seguir iremos usar a Definição 3.2.1 para construir a polarização no caso de $\mathbb{F}$ ser infinito ou finito.

Exemplo 3.2.3. Consideremos a álgebra de invariantes $S(n,l) = \mathbb{F}[(M_n)^l]^{GL(n)}$, isto é, $\mathcal{W} = 0$, $\mathcal{V} = M_n$, e $G = GL(n)$. Para $\mathbb{F}[(M_n)^l] = \mathbb{F}[x_{ij}^k \,|\, i,j \in [n],\ k \in [l]]$, seja $X_k = (x_{ij}^k)_{i \in [n],\, j \in [n]}$ a matriz genérica $n \times n$. Denotemos os coeficientes do polinômio característico de uma matriz X de ordem n por $\sigma_i(X)$, onde $i \in [n]$, ou seja, $\det(X + \lambda E) = \sum_{i=0}^{n} \lambda^{n-i} \sigma_i(X)$. Assim, $\sigma_0(X) = 1$, $\sigma_1(X) = \mathrm{tr}(X)$, e $\sigma_n(X) = \det(X)$. Então,

1. $\mathrm{Pol}_1^l(\mathrm{tr}(X_1)) = \{\mathrm{tr}(X_1), \ldots, \mathrm{tr}(X_l)\}$, uma vez que para $m = 1$, temos

$$\Phi(\mathrm{tr}(X_1)) = \mathrm{tr}(a_{11}X_1 + \cdots + a_{1l}X_l) = a_{11}\,\mathrm{tr}(X_1) + \cdots + a_{1l}\,\mathrm{tr}(X_l).$$

2. $\mathrm{Pol}_1^l(\sigma_2(X_1)) = \{\sigma_2(X_1), \ldots, \sigma_2(X_l), \mathrm{tr}(X_i)\,\mathrm{tr}(X_j) - \mathrm{tr}(X_iX_j) \,|\, 1 \le i < j \le l\}$, visto que se $m = 1$, teremos

$$\Phi(\sigma_2(X_1)) = \sigma_2(a_{11}X_1 + \cdots + a_{1l}X_l) =$$
$$a_{11}^2\sigma_2(X_1) + \cdots + a_{1l}^2\sigma_2(X_l) + \sum_{1 \le i < j \le l} a_{1i}a_{1j}\left(\mathrm{tr}(X_i)\,\mathrm{tr}(X_j) - \mathrm{tr}(X_iX_j)\right).$$

3. $\mathrm{Pol}_1^l(\mathrm{tr}(X_1^2)) = \{\mathrm{tr}(X_1), \ldots, \mathrm{tr}(X_l), 2\,\mathrm{tr}(X_iX_j) \,|\, 1 \leq i < j \leq l\}$, pois caso $m = 1$, obtemos
$$\Phi(\mathrm{tr}(X_1^2)) = \mathrm{tr}((a_{11}X_1 + \cdots + a_{1l}X_l)^2) =$$
$$a_{11}^2\,\mathrm{tr}(X_1^2) + \cdots + a_{1l}^2\,\mathrm{tr}(X_l^2) + \sum_{1\leq i<j\leq l} a_{1i}a_{1j}2\,\mathrm{tr}(X_iX_j).$$
Em particular, se $\mathrm{char}\,\mathbb{F} = 2$, então $\mathrm{tr}(X_1X_2)$ não pertence a $\mathrm{Pol}_1^l(\mathrm{tr}(X_1^2))$.

4. $\mathrm{Pol}_2^l(\mathrm{tr}(X_1^2X_2))$ consiste em $\mathrm{tr}(X_i^3)$, $\mathrm{tr}(X_i^2X_j)$ com $i \neq j$, $\mathrm{tr}((X_iX_j + X_jX_i)X_k)$ com $i < j < k$, onde $i, j, k \in [l]$, uma vez que para $m = 2$, temos
$$\Phi(\mathrm{tr}(X_1^2X_2)) = \mathrm{tr}((a_{11}X_1 + \cdots + a_{1l}X_l)^2(a_{21}X_1 + \cdots + a_{2l}X_l)).$$

5. $\mathrm{Pol}_3^l(\mathrm{tr}(X_1X_2) + \mathrm{tr}(X_2X_3)) = \{\mathrm{tr}(X_iX_j) + \mathrm{tr}(X_jX_k) \,|\, i, j, k \in [l]\}$.

Suponhamos que $I \in \mathcal{V}$ é um vetor G-invariante, ou seja, $g \cdot I = I$ para todo $g \in G$. Definindo o mapa linear
$$\Psi_I : \mathcal{W} \oplus \mathcal{V}^m \to \mathcal{W} \oplus \mathcal{V}^{m+1} \quad \text{por} \quad \Psi_I(\underline{v}) = (v_0, v_1, \ldots, v_m, I).$$
Então, obtemos o homomorfismo de álgebras
$$\Psi_I^* : \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^{m+1}]^G \to \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]^G \ \text{, onde} \quad \Psi_I^*(f)(\underline{v}) = f(\Psi_I(\underline{v})).$$

Definição 3.2.4. Sejam $\mathcal{A}$ uma $\mathbb{F}$-álgebra, $S \subset \mathcal{A}$ e $F : \mathcal{A} \to 2^{\mathcal{A}}$ um mapa de $\mathcal{A}$ na família de todos os subconjuntos de $\mathcal{A}$. Dizemos que S é fechado a geradores com respeito a $\mathbb{F}$, se
$$F(S) = \bigcup_{s\in S} F(s)$$
está contido na $\mathbb{F}$-álgebra com unidade, $\mathrm{alg}_{\mathbb{F}}\{S\}$, gerada por S.

Introduzamos as equivalências a seguir, no conjunto de pares de elementos de $(\mathcal{W} \oplus \mathcal{V}^m)^2$.

Definição 3.2.5 (Equivalências)**.** Sejam $(\underline{v}, \underline{v}')$, $(\underline{u}, \underline{u}')$ pertencentes ao espaço $(\mathcal{W} \oplus \mathcal{V}^m)^2$ e $I \in \mathcal{V}$ um vetor G-invariante. Então,

- $(\underline{v}, \underline{v}') \overset{\mathrm{lin}}{\approx} (\underline{u}, \underline{u}')$ se, e somente se, $v_0 = u_0$, $v_0' = u_0'$, e
$$\mathrm{span}_{\mathbb{F}}(v_1 \oplus v_1', \ldots, v_m \oplus v_m') = \mathrm{span}_{\mathbb{F}}(u_1 \oplus u_1', \ldots, u_m \oplus u_m') \quad \text{em} \quad \mathcal{V}^2;$$

- $(\underline{v}, \underline{v}') \overset{G}{\approx} (\underline{u}, \underline{u}')$ se, e só se, existem $g_1, g_2 \in G$ tais que $g_1 \cdot \underline{v} = \underline{u}$;
- $(\underline{v}, \underline{v}') \overset{I}{\approx} (\underline{u}, \underline{u}')$ se, e só se, para todo $k \in [m]$ existe $\alpha_k \in \mathbb{F}$ tal que
$$u_k \oplus u'_k = v_k \oplus v'_k + \alpha_k(I \oplus I);$$
- $(\underline{v}, \underline{v}') \approx (\underline{u}, \underline{u}')$ se, e somente se, o par $(\underline{u}, \underline{u}')$ pode ser obtido a partir de $(\underline{v}, \underline{v}')$, como o resultado de aplicações das equivalências definidas acima.

É fácil ver que todas as relações em $(\mathcal{W} \oplus \mathcal{V}^m)^2$ dadas na Definição 3.2.1 são realmente relações de equivalência. O caso parcial no qual $I = 0$ e $S = \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]^G$, abordado no teorema a seguir, foi obtido por Domokos em [30, Lemma 2.1].

Teorema 3.2.6. *Sejam $I \in \mathcal{V}$ um vetor G-invariante e $S \subset \mathbb{F}[\mathcal{W} \oplus \mathcal{V}^m]^G$ um conjunto fechado a geradores com respeito a*

(a) a polarização Pol_m^m, ou seja, $\mathrm{Pol}_m^m(S) \subset alg_{\mathbb{F}}(S)$;

(b) a composição $\Psi_I^* \circ \mathrm{Pol}_m^{m+1}$, isto é, $\Psi_I^* \circ \mathrm{Pol}_m^{m+1}(S) \subset alg_{\mathbb{F}}(S)$.

Então, para todo os pares $(\underline{v}, \underline{v}')$, $(\underline{u}, \underline{u}')$ de $(\mathcal{W} \oplus \mathcal{V}^m)^2$ com $(\underline{v}, \underline{v}') \approx (\underline{u}, \underline{u}')$ as seguintes condições são equivalentes:

- *$\underline{v}, \underline{v}'$ são separados por S;*
- *$\underline{u}, \underline{u}'$ são separados por S.*

Demonstração. Obviamente, a afirmação do teorema é válida se considerarmos a equivalência $\overset{G}{\approx}$ ao invês da equivalência $\approx$. Assim, a conclusão do teorema segue das Afirmações 1 e 2 a seguir.

Afirmação 1. O resultado do teorema é válido para a equivalência $\overset{\mathrm{lin}}{\approx}$.

Suponhamos que $\underline{v}, \underline{v}'$ não são separados por S. Como "$\overset{\mathrm{lin}}{\approx}$" é uma equivalência, para finalizar a demonstração da Afirmação 1, é suficiente mostrar que $\underline{u}, \underline{u}'$ não são separados por S.

Seja $u_k \oplus u'_k = \sum_{r=1}^{l} \alpha_{k,r}(v_r \oplus v'_r)$ para todo $k \in [m]$, onde $\alpha_{k,r} \in \mathbb{F}$. Pela parte (a) da Observação 3.2.2, para cada $f \in S$ temos
$$f(\underline{u}) = \sum \underline{\alpha}^{\Delta(h)} h(\underline{v}) \quad \text{e} \quad f(\underline{u}') = \sum \underline{\alpha}^{\Delta(h)} h(\underline{v}'),$$

onde ambos somatórios são tomados sobre todos os elementos $h \in \mathrm{Pol}_m^m(f)$. Uma vez que $\mathrm{Pol}_m^m(f) \subset \mathrm{alg}_{\mathbb{F}}(S)$, teremos $h(\underline{v}) = h(\underline{v}')$ para todo $h \in \mathrm{Pol}_m^m(f)$. Portanto, $\underline{u}, \underline{u}'$ não são separados por S, donde segue o resultado.

Afirmação 2. O resultado do teorema é válido para a equivalência $\overset{I}{\approx}$.

Suponhamos que $\underline{v}, \underline{v}'$ não são separados por S. Como "$\overset{I}{\approx}$" é uma equivalência, para completar esta demonstração é suficiente mostrar que $\underline{u}, \underline{u}'$ não são separados por S.

Seja $u_k \oplus u_k' = v_k \oplus v_k' + \alpha_k(I \oplus I)$ para todo $k \in [m]$, onde $\alpha_k \in \mathbb{F}$.

Segue da parte (a) da Observação 3.2.2 que, para cada $f \in S$ temos

$$f(\underline{u}) = \sum \alpha_1^{\xi_1} \cdots \alpha_m^{\xi_m}\, h(\Psi_I(\underline{v})) \quad \text{e} \quad f(\underline{u}') = \sum \alpha_1^{\xi_1} \cdots \alpha_m^{\xi_m}\, h(\Psi_I(\underline{v}')),$$

onde ambos somatórios são tomados sobre todos os elementos $h \in \mathrm{Pol}_m^{m+1}(f)$ com $\underline{a}^{\Delta(h)} = a_{1,1}^{\delta_1} \cdots a_{m,m}^{\delta_m}\, a_{1,m+1}^{\xi_1} \cdots a_{m,m+1}^{\xi_m}$ para alguns $\delta_1, \ldots, \delta_m, \xi_1, \ldots, \xi_m \geq 0$ (veja Definição 3.2.1 para os detalhes). Uma vez que $h(\Psi_I(\underline{v})) = (\Psi_I^* \circ h)(\underline{v})$, $h(\Psi_I(\underline{v}')) = (\Psi_I^* \circ h)(\underline{v}')$, e $\Psi_I^* \circ h \in \mathrm{alg}_{\mathbb{F}}(S)$, temos $h(\Psi_I(\underline{v})) = h(\Psi_I(\underline{v}'))$. Logo, $\underline{u}, \underline{u}'$ não são separados por S, como queríamos demonstrar. □

3.2.2 O caso de múltiplos espaços

Nesta seção iremos estender as definições e o teorema da Secão 3.2.1 para o caso em que $\mathcal{H} = \mathcal{V}_1^{m_1} \oplus \cdots \oplus \mathcal{V}_s^{m_s}$, para G-módulos de dimensão finita $\mathcal{V}_1, \ldots, \mathcal{V}_s$ sobre $\mathbb{F}$ com dimensões $\dim \mathcal{V}_1 = n_1, \ldots, \dim \mathcal{V}_s = n_s$, onde a ação de G em $\mathcal{H}$ é diagonal e $m_1, \ldots, m_s \geq 1$. Dado um elemento $\underline{v} \in \mathcal{H}$, escrevemos $\underline{v} = (\underline{v}^{(1)}, \ldots, \underline{v}^{(s)})$ para $\underline{v}^{(k)} = (v_1^{(k)}, \ldots, v_{m_k}^{(k)}) \in \mathcal{V}_k^{m_k}$ com $1 \leq k \leq s$. A próxima definição foi dada em [24, página 559].

Definição 3.2.7 (Polarização para o caso de múltiplos espaços)**.** Para $l_1, \ldots, l_s \geq 1$ a polarização

$$\mathrm{Pol}_{m_1,\ldots,m_s}^{l_1,\ldots,l_s} : \mathbb{F}[\mathcal{V}_1^{m_1} \oplus \cdots \oplus \mathcal{V}_s^{m_s}] \to \mathbb{F}[\mathcal{V}_1^{l_1} \oplus \cdots \oplus \mathcal{V}_s^{l_s}]$$

é a composição de polarizações $\mathrm{Pol}_{m_s}^{l_s} \circ \cdots \circ \mathrm{Pol}_{m_1}^{l_1}$, onde $\mathrm{Pol}_{m_k}^{l_k} : \mathbb{F}[\mathcal{W}_k \oplus \mathcal{V}_k^{m_k}] \to \mathbb{F}[\mathcal{W}_k \oplus \mathcal{V}_k^{l_k}]$ para $\mathcal{W}_k = \mathcal{V}_1^{l_1} \oplus \cdots \oplus \mathcal{V}_{k-1}^{l_{k-1}} \oplus \mathcal{V}_{k+1}^{m_{k+1}} \oplus \cdots \oplus \mathcal{V}_s^{m_s}$ para todo $1 \leq k \leq s$.

De modo análogo ao feito na seção anterior, temos as seguintes relações de equivalência.

Definição 3.2.8 (Equivalências)**.** Suponhamos que $(\underline{v}, \underline{v}')$, $(\underline{u}, \underline{u}')$ pertencem a $(\mathcal{V}_1^{m_1} \oplus \cdots \oplus \mathcal{V}_s^{m_s})^2$ e $I = (I_1, \ldots, I_s) \in \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_s$ é um vetor G-invariante. Então

- $(\underline{v}, \underline{v}') \overset{\text{lin}}{\approx} (\underline{u}, \underline{u}')$ se, e só se, $(\underline{v}^{(k)}, \underline{v}'^{(k)}) \overset{\text{lin}}{\approx} (\underline{u}^{(k)}, \underline{u}'^{(k)})$ para todos $1 \leq k \leq s$;
- $(\underline{v}, \underline{v}') \overset{G}{\approx} (\underline{u}, \underline{u}')$ se, e só se, existem $g_1, g_2 \in G$ tais que $g_1 \cdot \underline{v} = \underline{u}$ e $g_2 \cdot \underline{v}' = \underline{u}'$;
- $(\underline{v}, \underline{v}') \overset{I}{\approx} (\underline{u}, \underline{u}')$ se, e só se, $(\underline{v}^{(k)}, \underline{v}'^{(k)}) \overset{I_k}{\approx} (\underline{u}^{(k)}, \underline{u}'^{(k)})$ para todo $1 \leq k \leq s$;
- $(\underline{v}, \underline{v}') \approx (\underline{u}, \underline{u}')$ se, e só se, o par $(\underline{u}, \underline{u}')$ pode ser obtido a partir de $(\underline{v}, \underline{v}')$ como o resultado de aplicações das equivalências definidas acima.

É possível mostrar que todas as relações em $(\mathcal{V}_1^{m_1} \oplus \cdots \oplus \mathcal{V}_s^{m_s})^2$ dadas na Definição 3.2.8 são de fato relações de equivalência.

O corolário abaixo segue imediatamente do Teorema 3.2.6:

Corolário 3.2.9. *Suponhamos que $I \in \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_s$ é um vetor G-invariante e que o subconjunto $S \subset \mathbb{F}[\mathcal{V}_1^{m_1} \oplus \cdots \oplus \mathcal{V}_s^{m_s}]^G$ é fechado a geradores com respeito a*

(a) a polarização $\mathrm{Pol}_{m_1,\ldots,m_s}^{m_1,\ldots,m_s}$;

(b) a composição $\Psi_{I_s}^* \circ \cdots \circ \Psi_{I_1}^* \circ \mathrm{Pol}_{m_1,\ldots,m_s}^{m_1+1,\ldots,m_s+1}$.

Então, para todos os pares $(\underline{v}, \underline{v}')$, $(\underline{u}, \underline{u}')$ de $(\mathcal{V}_1^{m_1} \oplus \cdots \oplus \mathcal{V}_s^{m_s})^2$ com $(\underline{v}, \underline{v}') \approx (\underline{u}, \underline{u}')$ as condições a seguir são equivalentes:

- *$\underline{v}, \underline{v}'$ são separados por S;*
- *$\underline{u}, \underline{u}'$ são separados por S.*

3.3 Geradores da álgebra $SI(m, p, q)$

Nesta seção iremos apresentar uma descrição de um conjunto gerador para a álgebra $SI(m, p, q)$. Entretanto, antes desta descrição fixemos as seguintes notações.

Iremos denotar por $M_0 \subset SI(m, p, q)$ o conjunto:

$$\det(X_1), \ldots, \det(X_m), \det(Y_1), \ldots, \det(Y_p), \det(Z_1), \ldots, \det(Z_q)$$

e por $M_2 \subset SI(m, p, q)$ o seguinte conjunto:

(a) $\mathrm{tr}(Y_{i_1} \cdots Y_{i_r})$, onde $r > 0$ e $1 \leq i_1 < \cdots < i_r \leq p$;

(b) $\mathrm{tr}(Z_{j_1} \cdots Z_{j_s})$, com $s > 0$ e $1 \leq j_1 < \cdots < j_s \leq q$;

(c) $\mathrm{tr}(Y_{i_1} \cdots Y_{i_r} \cdot X_k \cdot Z_{j_1} \cdots Z_{j_s} \cdot X_k^*)$, para $r, s > 0$, $1 \leq k \leq m$, $1 \leq i_1 < \cdots < i_r \leq p$, e $1 \leq j_1 < \cdots < j_s \leq q$;

(d) $\mathrm{tr}(Y_{i_1} \cdots Y_{i_r} \cdot X_{k_1} \cdot Z_{j_1} \cdots Z_{j_s} \cdot X_{k_2}^* \cdots X_{k_{2t-1}} X_{k_{2t}}^*)$, onde $r, s \geq 0$, $t > 0$, $1 \leq k_1 < \cdots < k_{2t} \leq m$, $1 \leq i_1 < \cdots < i_r \leq p$, e $1 \leq j_1 < \cdots < j_s \leq q$.

Consideremos M_1 o conjunto que consiste dos semi-invariantes de M_2, os quais satisfazem as seguintes condições adicionais, respectivamente:

(a) $r \leq 3$;

(b) $s \leq 3$;

(c) $r, s \leq 2$;

(d) $t \leq 2$; ademais, se $t = 1$, então $r, s \leq 2$; se $t = 2$, então $r = s = 0$.

Temos a seguinte descrição de um conjunto gerador para $SI(m, p, q)$, dada por Lopatin em [4].

Proposição 3.3.1. [4, Lema 8.6] *Um conjunto gerador minimal para* $SI(m, p, q)$ *é dado por:*

- $M_0 \cup M_1$, *se* $\mathrm{char}\,\mathbb{F} \neq 2$;
- $M_0 \cup M_2$, *se* $\mathrm{char}\,\mathbb{F} = 2$.

Conforme comentado anteriormente, nosso principal interesse é obter uma descrição de um conjunto separador minimal para $SI(m, p, q)$ (veja Teorema 3.4.17). Vale destacar que os casos parciais onde $m = p = 0$, bem como $p = q = 0$, foram considerados anteriormente e temos as caracterizações a seguir.

Proposição 3.3.2. [23, Teorema 1.1] *Seja* $\mathbb{F}$ *um corpo infinito. Então, o conjunto*

$$\begin{aligned} \mathrm{tr}(Y_i), \det(Y_i), &\quad 1 \leq i \leq p, \\ \mathrm{tr}(Y_{i_1} Y_{i_2}), &\quad 1 \leq i_1 < i_2 \leq p, \\ \mathrm{tr}(Y_{i_1} Y_{i_2} Y_{i_3}), &\quad 1 \leq i_1 < i_2 < i_3 \leq p. \end{aligned}$$

é um conjunto separador minimal para $S(2, p) = SI(0, p, 0)$.

Proposição 3.3.3. [32, Teorema 6.1] *Seja* $\mathbb{F}$ *um corpo algebricamente fechado. Então o conjunto*

$$\begin{array}{rl} \det(X_1), \ldots, \det(X_m), & \\ \operatorname{tr}(X_{k_1} X_{k_2}^*), & 1 \le k_1 < k_2 \le m, \\ \operatorname{tr}(X_{k_1} X_{k_2}^* X_{k_3} X_{k_4}^*), & 1 \le k_1 < \cdots < k_4 \le m. \end{array}$$

é um conjunto separador minimal para $R(2, m) = SI(m, 0, 0)$.

Na formulação da Proposição 3.3.3 o conjunto separador minimal para $R(2, m)$ de [32] é reescrito em termos dos geradores da Proposição 3.3.1. A equivalência das duas formulações segue do Lema 3.3.4, o qual será exposto a seguir, junto com o Lema 4.2 de [32] (ou, equivalentemente, das partes (C′), (D′) do Lema 4.1 de [4]).

Antes da formulação do Lema 3.3.4, observemos que denotando por X, Y, X_i, Y_i $(i > 1)$ matrizes 2×2 arbitrárias sobre uma $\mathbb{F}$-álgebra comutativa com unidade. Temos A^* $(X^*)^* = X$, $(XY)^* = Y^* X^*$, $\operatorname{tr}(X^*) = \operatorname{tr}(X)$, e ainda $\det(X^*) = \det(X)$. Além disso, observemos também que vale

$$\operatorname{tr}(XY^*) = \operatorname{tr}(X^* Y) = \operatorname{tr}(X) \operatorname{tr}(Y) - \operatorname{tr}(XY). \tag{3.2}$$

Recordemos agora algumas definições dadas em [32]. O elemento $\langle X | Y \rangle$ é definido como o coeficiente de $\alpha\beta$ em $\det(\alpha X + \beta Y)$ para todos $\alpha, \beta \in \mathbb{F}$. Para $t \ge 2$, $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t \in \mathbb{F}$ e $1 \le i \le t$ denotaremos por $\widetilde{X_i}$ ($\widetilde{Y_i}$, respectivamente) a matriz $2t \times 2t$ dividida em $t \times t$ blocos de tamanho 2×2, onde o único bloco não nulo é $\alpha_i X_i$ ($\beta_i Y_i$, respectivamente) na posição (i, i) ($(i, i+1)$ para $i < t$ e $(t, 1)$ para $i = t$, respectivamente). Por definição, $\xi(X_1, \ldots, X_t, Y_1, \ldots, Y_t)$ é o coeficiente de $\alpha_1 \cdots \alpha_t \beta_1 \cdots \beta_t$ no determinante

$$\det(\widetilde{X_1} + \cdots + \widetilde{X_t} + \widetilde{Y_1} + \cdots + \widetilde{Y_t}). \tag{3.3}$$

Lema 3.3.4. *Temos*

(a) $\langle X | Y \rangle = \operatorname{tr}(XY^*)$,

(b) $\xi(X_1, \ldots, X_t, Y_1, \ldots, Y_t) = (-1)^{t+1} \operatorname{tr}(X_1^* Y_1 \cdots X_t^* Y_t)$.

Demonstração. A parte (a) segue imediatamente da fórmula (3.2).

Consequentemente, aplicando (3.2), não é difícil ver que $\operatorname{tr}(X_1^* Y_1 \cdots X_t^* Y_t)$ é igual a

$$\sum_{r=0}^{t} \sum_{1 \le i_1 < \cdots < i_r \le t} (-1)^{r+t} \operatorname{tr}(X_{i_1}) \cdots \operatorname{tr}(X_{i_r}) \operatorname{tr}(X_1 Y_1 \cdots \widehat{X_{i_1}} Y_{i_1} \cdots \widehat{X_{i_r}} Y_{i_r} \cdots X_t Y_t), \tag{3.4}$$

onde no último produto de matrizes não temos $X_{i_1}, \dots, X_{i_r}$. Observemos que os únicos produtos não nulo de matrizes $\widetilde{X}_1, \dots, \widetilde{X}_t, \widetilde{Y}_1, \dots, \widetilde{Y}_t$ são

$$\widetilde{X}_i\widetilde{X}_i, \quad \widetilde{X}_i\widetilde{Y}_i, \quad \widetilde{Y}_i\widetilde{X}_{i+1}, \quad \widetilde{Y}_i\widetilde{Y}_{i+1} \text{ para } 1 \le i \le t,$$

onde $\widetilde{X}_{t+1}$ ($\widetilde{Y}_{t+1}$, respectivamente) significa $\widetilde{X}_1$ ($\widetilde{Y}_1$, respectivamente). Assim, aplicando a fórmula de Amitsur (vide [36]) a (3.3) e usando (3.4), concluímos a demonstração da parte (b). □

3.4 Construção de um conjunto separador minimal para $SI(m, p, q)$

Nesta seção iremos construir um conjunto separador minimal para a álgebra $SI(m, p, q)$. Neste intuito, consideremos o conjunto a seguir.

Para todos $i, i_1, i_2, i_3 \in [p]$, $j, j_1, j_2, j_3 \in [q]$, $k, k_1, \dots, k_4 \in [m]$ denotemos por M_{sep} o seguinte conjunto:

$$\begin{array}{rll}
\det(X_k),\ \det(Y_i),\ \det(Z_j) & & \\
\operatorname{tr}(Y_{i_1}\cdots Y_{i_r}),\ \operatorname{tr}(Z_{j_1}\cdots Z_{j_s}) & \text{para} & 1 \le r, s \le 3,\ i_1 < \cdots < i_r,\ j_1 < \cdots < j_s \\
\operatorname{tr}(X_{k_1}X_{k_2}^*) & \text{com} & k_1 < k_2 \\
\operatorname{tr}(Y_iX_{k_1}Z_jX_{k_2}^*) & \text{onde} & k_1 \le k_2 \\
\operatorname{tr}(Y_{i_1}Y_{i_2}X_kZ_jX_k^*),\ \operatorname{tr}(Y_iX_kZ_{j_1}Z_{j_2}X_k^*) & \text{para} & i_1 < i_2,\ j_1 < j_2, \\
\operatorname{tr}(Y_iX_{k_1}X_{k_2}^*),\ \operatorname{tr}(X_{k_1}Z_jX_{k_2}^*) & \text{com} & k_1 < k_2 \\
\operatorname{tr}(Y_{i_1}Y_{i_2}X_{k_1}X_{k_2}^*),\ \operatorname{tr}(X_{k_1}Z_{j_1}Z_{j_2}X_{k_2}^*) & \text{onde} & i_1 < i_2,\ j_1 < j_2,\ k_1 < k_2 \\
\operatorname{tr}(X_{k_1}X_{k_2}^*X_{k_3}X_{k_4}^*) & \text{para} & k_1 < \cdots < k_4.
\end{array}$$

Nosso objetivo será mostrar que M_{sep} é um conjunto separador minimal para $SI(m, p, q)$. Para tal, iremos consider a separabilidade e minimalidade desse conjunto nas subseções a seguir.

3.4.1 Separabilidade de M_{sep}

Nesta seção iremos considerar $\mathbb{F}$ um corpo algebricamente fechado. A relação de equivalência $\approx$ sobre o conjunto de pares de elementos de $\mathcal{H}(m, p, q)$ é definida como um caso parcial da Definição 3.2.8 para $s = 3$, $\mathcal{V}_1 = \mathcal{V}_2 = \mathcal{V}_3 = M_2$, e $I = (0, E, E)$. Escrevemos $\underline{A} \sim \underline{B}$ para $\underline{A}, \underline{B}$ de $\mathcal{H}(m, p, q)$ se $(\underline{A}, \underline{A}) \approx (\underline{B}, \underline{B})$. As equivalências $\overset{\text{lin}}{\approx}$, $\overset{G}{\approx}$, $\overset{I}{\approx}$ sobre $\mathcal{H}(m, p, q)^2$ e as equivalências $\overset{\text{lin}}{\sim}$, $\overset{G}{\sim}$, $\overset{I}{\sim}$ sobre $\mathcal{H}(m, p, q)$ são definidas analogamente. Por uma questão de completude, iremos explicitamente definir essas equivalências para $(\underline{A}, \underline{B})$, $(\underline{C}, \underline{D})$ do $\mathcal{H}(m, p, q)^2$:

- $(\underline{A}, \underline{B}) \overset{\text{lin}}{\approx} (\underline{C}, \underline{D})$ se, e só se,

$$\begin{array}{rcl} \operatorname{span}_{\mathbb{F}}\{(A_k, B_k) \,|\, 1 \leq k \leq m\} & = & \operatorname{span}_{\mathbb{F}}\{(C_k, D_k) \,|\, 1 \leq k \leq m\}, \\ \operatorname{span}_{\mathbb{F}}\{(A'_i, B'_i) \,|\, 1 \leq i \leq p\} & = & \operatorname{span}_{\mathbb{F}}\{(C'_i, D'_i) \,|\, 1 \leq i \leq p\}, \\ \operatorname{span}_{\mathbb{F}}\{(A''_i, B''_j) \,|\, 1 \leq j \leq q\} & = & \operatorname{span}_{\mathbb{F}}\{(C''_j, D''_j) \,|\, 1 \leq j \leq q\}; \end{array}$$

- $(\underline{A}, \underline{B}) \overset{G}{\approx} (\underline{C}, \underline{D})$ se, e só se, $g_1\underline{A} = \underline{C}$ e $g_2\underline{B} = \underline{D}$, para algum g_1, g_2 de $G = SL(2) \times SL(2)$;

- $(\underline{A}, \underline{B}) \overset{I}{\approx} (\underline{C}, \underline{D})$ se, e só se,

$$\begin{array}{rl} \text{para cada} 1 \leq i \leq p \text{ existe } \beta_i \in \mathbb{F} & \text{tal que } \ (C'_i, D'_i) = (A'_i, B'_i) + \beta_i(I_2, I_2), \\ \text{para cada } 1 \leq j \leq q \text{ existe } \gamma_j \in \mathbb{F} & \text{tal que } \ (C''_j, D''_j) = (A''_j, B''_j) + \gamma_j(I_2, I_2). \end{array}$$

Lema 3.4.1. *O subconjunto M_{sep} de $SI(m,p,q) = \mathbb{F}[\mathcal{H}(m,p,q)]^G$ é fechado a geradores, com respeito à:*

(a) a polarização $\operatorname{Pol}_{m,p,q}^{m,p,q}$;

(b) a composição $\Psi^*_{I''} \circ \Psi^*_{I'} \circ \Psi^*_I \circ \operatorname{Pol}_{m,p,q}^{m+1,p+1,q+1}$.

Demonstração. **(a)** Pela definição de polarização, $\operatorname{Pol}_{m,p,q}^{m,p,q}(M_{\text{sep}})$ é o seguinte conjunto:

$$\begin{array}{rll} \det(X_k),\ \det(Y_i),\ \det(Z_j) & & \\ \operatorname{tr}(Y_{i_1} \cdots Y_{i_r}),\ \operatorname{tr}(Z_{j_1} \cdots Z_{j_s}) & \text{para} & 1 \leq r \leq \min\{3, p\},\ 1 \leq s \leq \min\{3, q\} \\ \operatorname{tr}(Y_i X_k Z_j X_k^*) & & \\ \operatorname{tr}(Y_{i_1} Y_{i_2} X_k Z_j X_k^*) & \text{onde} & p \geq 2 \\ \operatorname{tr}(Y_i X_k Z_{j_1} Z_{j_2} X_k^*) & \text{com} & q \geq 2 \\ \operatorname{tr}(X_{k_1} X_{k_2}^*) & \text{para} & m \geq 2 \\ \operatorname{tr}(Y_i X_{k_1} X_{k_2}^*),\ \operatorname{tr}(X_{k_1} Z_j X_{k_2}^*) & \text{onde} & m \geq 2 \\ \operatorname{tr}(Y_i X_{k_1} Z_j X_{k_2}^*) & \text{com} & m \geq 2 \\ \operatorname{tr}(Y_{i_1} Y_{i_2} X_{k_1} X_{k_2}^*) & \text{para} & p \geq 2,\ \ m \geq 2 \\ \operatorname{tr}(X_{k_1} Z_{j_1} Z_{j_2} X_{k_2}^*) & \text{onde} & q \geq 2,\ m \geq 2 \\ \operatorname{tr}(X_{k_1} X_{k_2}^* X_{k_3} X_{k_4}^*) & \text{com} & m \geq 4, \end{array}$$

onde $i, i_1, \ldots, i_s \in [p]$, $j, j_1, \ldots, j_s \in [q]$, $k, k_1, \ldots, k_4 \in [m]$. Notemos que para cada matrizes A, B, C, de ordem 2, temos $AA^* = \det(A)E$,

$$\operatorname{tr}(A^2 B) = \operatorname{tr}(A)\operatorname{tr}(B) - \det(A)\operatorname{tr}(B),$$

$$\operatorname{tr}(BAC) = -\operatorname{tr}(ABC) + \operatorname{tr}(A)\operatorname{tr}(BC) + \operatorname{tr}(B)\operatorname{tr}(AC) + (\operatorname{tr}(AB) - \operatorname{tr}(A)\operatorname{tr}(B))\operatorname{tr}(C).$$

Essas fórmulas implicam que o conjunto $\mathrm{Pol}_{m,p,q}^{m,p,q}(M_{\mathrm{sep}})$ está contido na álgebra gerada por M_{sep}.

(b) Para obter o conjunto $\Psi_{I''}^* \circ \Psi_{I'}^* \circ \Psi_I^* \circ \mathrm{Pol}_{m,p,q}^{m+1,p+1,q+1}$, faremos as substituições a seguir no conjunto $\mathrm{Pol}_{m,p,q}^{m,p,q}(M_{\mathrm{sep}})$ da parte (a):

$$p \to p+1,\ q \to q+1,\ Y_{p+1} \to E,\ Z_{q+1} \to E.$$

Logo, a conclusão da demonstração é feito como em (a). □

De forma similar ao feito no capítulo anterior, buscaremos estabelecer formas mais simples para os pares de elementos de $\mathcal{H}(m,p,q)$. Consideremos agora alguns resultados auxiliares que irão nos auxiliar na obtenção dessas formas.

Se para cada elemento $A \in S$ de um conjunto $S \subset M_{2\times 2}$ tivermos $\det(A) = 0$, então escreveremos simplesmente $\det(S) = 0$. Nos resultados a seguir o símbolo $*$ representa qualquer elemento de $\mathbb{F}$.

Lema 3.4.2. *Para cada* $\underline{A} = (A_1', A_2') \in \mathcal{H}(0,2,0)$ *temos*

$$\underline{A} \overset{\mathrm{lin},\, I}{\sim} \left(\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \right).$$

Demonstração. Obviamente, $\underline{A} \overset{I}{\sim} (B_1, B_2)$ para

$$B_1 = \begin{pmatrix} 0 & * \\ * & \beta_1 \end{pmatrix} \quad \text{e} \quad B_2 = \begin{pmatrix} 0 & * \\ * & \beta_2 \end{pmatrix}.$$

Se $\beta_1 = 0$, então temos o resultado. Suponhamos então que $\beta_1 \neq 0$. Caso $\beta_2 = 0$, basta aplicar $(B_1, B_2) \overset{\mathrm{lin}}{\sim} (B_2, B_1)$ para completar a demonstração. Caso contrário, temos $(B_1, B_2) \overset{\mathrm{lin}}{\sim} (B_1 - (\beta_1/\beta_2)B_2, B_2)$, donde segue o resultado. □

Lema 3.4.3. *Para cada* $\underline{A} = (A_1, A_2)$ *e* $\underline{B} = (B_1, B_2)$ *de* $\mathcal{H}(2,0,0)$ *satisfazendo* $(A_1, A_2) \overset{\mathrm{lin}}{\sim} (B_1, B_2)$, *as seguintes condições são equivalentes:*

(a) $\det(\mathrm{span}_{\mathbb{F}}(A_1, A_2)) = 0$*;*

(b) $\det(\mathrm{span}_{\mathbb{F}}(B_1, B_2)) = 0$*;*

(c) $\det(A_1) = \det(A_2) = 0$ *e* $\operatorname{tr}(A_1 A_2^*) = 0$.

Demonstração. A fórmula de Amitsur [36] para matrizes 2×2 unida a fórmula dada em(3.2) implica que para cada $\alpha_1, \alpha_2 \in \mathbb{F}$, temos

$$\det(\alpha_1 A_1 + \alpha_2 A_2) = \alpha_1^2 \det(A_1) + \alpha_2^2 \det(A_2) + \alpha_1\alpha_2 \operatorname{tr}(A_1 A_2^*). \tag{3.5}$$

Logo, as condições (a) e (c) são equivalentes.

Suponhamos válida a condição (c). Sejam $B_1 = \alpha_1 A_1 + \alpha_2 A_2$ e $B_2 = A_2$ para $\alpha_1, \alpha_2 \in \mathbb{F}$. Aplicando a fórmula (3.5) e a igualdade $\operatorname{tr}(A_2 A_2^*) = 2\det(A_2)$, obtemos $\det(B_1) = \det(B_2) = 0$ e $\operatorname{tr}(B_1 B_2^*) = \alpha_1 \operatorname{tr}(A_1 A_2^*) + \alpha_2 \operatorname{tr}(A_2 A_2^*) = 0$. Repetindo este raciocínio, concluímos que (c) implica (b). Temos então o resultado. □

A próxima observação segue da equivalência entre as condições (a) e (c) do Lema 3.4.3.

Observação 3.4.4. Para cada $\underline{A} = (A_1, A_2)$ e $\underline{B} = (B_1, B_2)$ de $\mathcal{H}(2,0,0)$, com $f(\underline{A}) = f(\underline{B})$ para todo $f \in \{\det(X_1),\ \det(X_2),\ \operatorname{tr}(X_1 X_2^*)\}$, as condições a seguir são equivalentes:

(a) $\det(\operatorname{span}_{\mathbb{F}}(A_1, A_2)) = 0$;

(b) $\det(\operatorname{span}_{\mathbb{F}}(B_1, B_2)) = 0$;

(c) $\det(A_1) = \det(A_2) = 0$ e $\operatorname{tr}(A_1 A_2^*) = 0$.

Por fim, temos

Lema 3.4.5. *Para cada* $\underline{A} = (E_{11}, A_2)$ *e* $\underline{B} = (E_{11}, B_2)$ *elementos de* $\mathcal{H}(2,0,0)$, *tais que* $\det(\operatorname{span}_{\mathbb{F}}(E_{11}, A_2)) = \det(\operatorname{span}_{\mathbb{F}}(E_{11}, B_2)) = 0$, *temos*

$$(\underline{A}, \underline{B}) \overset{\text{lin}}{\approx} ((E_{11}, C), (E_{11}, D)) \quad \text{para} \quad C = \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \text{ e } D = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}$$

com $\det(C) = \det(D) = 0$.

Demonstração. Observemos que $(\underline{A}, \underline{B}) \overset{\text{lin}}{\approx} ((E_{11}, C), (E_{11}, D))$, para $C = \begin{pmatrix} 0 & * \\ * & c \end{pmatrix}$ e $D = \begin{pmatrix} * & * \\ * & d \end{pmatrix}$. O Lema 3.4.3 assegura que $\det(C) = \det(D) = 0$ e ainda $\operatorname{tr}(E_{11}C^*) = \operatorname{tr}(E_{11}D^*) = 0$. Então, segue da fórmula (3.2) que $c = d = 0$. □

De posse desses resultados passemos agora a obtenção das formas canônicas desejadas.

Proposição 3.4.6. *Seja $\mathbb{F}$ um corpo algebricamente fechado e suponhamos que $\underline{C}, \underline{D}$ de $\mathcal{H}(2,2,1)$ satisfazem as seguintes condições:*

(a) $\det(\mathrm{span}_{\mathbb{F}}(C_1, C_2)) = \det(\mathrm{span}_{\mathbb{F}}(D_1, D_2)) = 0$*;*

(b) $\mathrm{span}_{\mathbb{F}}(C_1, C_2) \neq 0$ *e* $\mathrm{span}_{\mathbb{F}}(D_1, D_2) \neq 0$*.*

Então, $(\underline{C}, \underline{D}) \approx (\underline{A}, \underline{B})$ *para algum par* $\underline{A}, \underline{B}$ *de* $\mathcal{H}(2,2,1)$ *satisfazendo*

$$\begin{array}{lll} \text{(I)} & \underline{A} & = \left(E_{11}, \quad \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}; \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}; \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}\right), \\ \text{(II)} & \underline{B} & = \left(E_{11}, \quad \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}; \begin{pmatrix} * & * \\ * & * \end{pmatrix}, \begin{pmatrix} * & * \\ * & * \end{pmatrix}; \begin{pmatrix} * & * \\ * & * \end{pmatrix}\right) \end{array}$$

com $\det(A_2) = \det(B_2) = 0$*.*

Demonstração. Uma vez que $((C_1, C_2), (D_1, D_2)) \overset{\text{lin}}{\approx} ((C_2, C_1), (D_2, D_1))$ em $\mathcal{H}(2,0,0)$, aplicando a condição (b), podemos assumir que ocorre um dos seguintes casos:

1. $C_1 \neq 0$ e $D_1 \neq 0$;

2. $C_1 \neq 0$, $C_2 = 0$, $D_1 = 0$, e $D_2 \neq 0$.

Observemos que podemos reduzir o caso 2 para o caso 1, considerando a equivalência $((C_1, C_2), (D_1, D_2)) \overset{\text{lin}}{\approx} ((C_1 + C_2, C_2), (D_1 + D_2, D_2)) = ((C_1, C_2), (D_2, D_2))$ em $\mathcal{H}(2,0,0)$. Notemos que após a redução as condições (a) e (b) continuam válidas.

Como $C_1 \neq 0$ e $\det(C_1) = 0$, obtemos que $C_1 \overset{G}{\sim} \alpha E_{11}$ em $\mathcal{H}(1,0,0)$ para algum $\alpha \in \mathbb{F}$ não-nulo. Para $g = \mathrm{diag}(\alpha^{-1}, \alpha)$ de $SL(2)$, temos $(g, 1) \cdot \alpha E_{11} = E_{11}$ em $\mathcal{H}(1,0,0)$. De modo análogo, considerando D_1, obtemos $((C_1, C_2), (D_1, D_2)) \overset{G}{\approx} ((E_{11}, C_2), (E_{11}, D_2))$ em $\mathcal{H}(2,0,0)^2$. Pelo Lema 3.4.3, temos $\det(\mathrm{span}_{\mathbb{F}}(E_{11}, C_2)) = \det(\mathrm{span}_{\mathbb{F}}(E_{11}, D_2)) = 0$. Em outras palavras, podemos assumir que $C_1 = D_1 = E_{11}$. A forma requirida para $((C_1, C_2), (D_1, D_2))$ de $\mathcal{H}(2,0,0)^2$, segue do Lema 3.4.5.

Aplicando o Lema 3.4.2 a $(C_1', C_2') \in \mathcal{H}(0,2,0)$, podemos assumir que módulo a equivalência $\overset{\text{lin}, I}{\approx}$ o par (C_1', C_2') pertence ao conjunto

$$\left\{ \left(\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \right) \right\}.$$

Obviamente, módulo a equivalência $\overset{I}{\approx}$, podemos assumir que a matriz C_1'' é igual a

$$\begin{pmatrix} 0 & * \\ * & * \end{pmatrix}.$$

$\square$

Proposição 3.4.7. *Seja $\mathbb{F}$ um corpo algebricamente fechado. Suponhamos que $\underline{C}, \underline{D}$ de $\mathcal{H}(2,2,1)$ satisfaçam as seguintes condições:*

(a) $f(\underline{C}) = f(\underline{D})$ *para todo* $f \in \{\det(X_1),\ \det(X_2),\ \mathrm{tr}(X_1X_2^*)\}$;

(b) $\det(\mathrm{span}_{\mathbb{F}}(C_1, C_2)) \neq 0$.

Então, módulo permutações de $\underline{C}$ e $\underline{D}$, temos que $(\underline{C}, \underline{D}) \approx (\underline{A}, \underline{B})$ para elementos $\underline{A}, \underline{B}$ de $\mathcal{H}(2,2,1)$ satisfazendo

$$\begin{array}{lll} \text{(I)} & \underline{A} & = \left(E, \quad A_2; \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}; \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}\right), \\ \text{(II)} & \underline{B} & = \left(E, \quad B_2; \begin{pmatrix} * & * \\ * & * \end{pmatrix}, \begin{pmatrix} * & * \\ * & * \end{pmatrix}; \begin{pmatrix} * & * \\ * & * \end{pmatrix}\right) \end{array}$$

com o par (A_2, B_2) pertencente a lista:

(1) (E_{12}, E_{12});

(2) $(E_{12}, 0)$;

(3) $(\alpha E_{11}, \alpha E_{11})$ *para algum* $\alpha \in \mathbb{F}$.

Demonstração. A condição (b) implica que o determinante de alguma combinação linear de C_1 e C_2 é diferente de zero. Portanto, módulo a equivalência $\overset{\text{lin}}{\approx}$, podemos supor que $\det(C_1) \neq 0$. Logo, $\det(D_1) \neq 0$. Notemos que a fórmula 3.5 implica que as condições (a) e (b) continuam válidas.

Módulo a equivalência $\overset{G}{\approx}$, podemos assumir que $C_1 = D_1 = E$. Observemos que para cada $\underline{g} = (g, g) \in G$, com $g \in SL(2)$, temos $g \cdot (E, C_2) = (E, g\, C_2\, g^{-1})$. Portanto, módulo a equivalência $\overset{G}{\approx}$, podemos supor que ambas as matrizes C_2 e D_2 estão na forma normal de Jordan com os mesmos autovalores (veja condição (a)). Módulo permutações de $\underline{C}$ e $\underline{D}$, obtemos que (C_2, D_2) é um dos seguintes pares:

- $(\alpha E + E_{12}, \alpha E + E_{12})$, para $\alpha \in \mathbb{F}$;
- $(\alpha E + E_{12}, \alpha E)$, com $\alpha \in \mathbb{F}$;
- $(\alpha E_{11} + \beta E_{22}, \alpha E_{11} + \beta E_{22})$, onde $\alpha \neq \beta$ from $\mathbb{F}$.

Usando a equivalência $\stackrel{\text{lin}}{\approx}$, podemos reduzir estes casos aos casos (1), (2), (3), respectivamente, da formulação da proposição.

Além disso, podemos obter a forma requirida para $(C_1', C_2'; C_1'') \in \mathcal{H}(0,2,1)$, exatamente da mesma maneira que no último parágrafo da demonstração da Proposição 3.4.6. □

Proposição 3.4.8. *Seja* $\mathbb{F}$ *um corpo algebricamente fechado. Suponhamos que os elementos* $\underline{C}, \underline{D}$ *de* $\mathcal{H}(2,2,1)$*, satisfazendo as seguintes condições:*

(a) $\det(\mathrm{span}_{\mathbb{F}}(C_1, C_2)) = 0$ *e* $\mathrm{span}_{\mathbb{F}}(C_1, C_2) \neq 0$*;*

(b) $D_1 = D_2 = 0$*.*

Então, $(\underline{C}, \underline{D}) \approx (\underline{A}, \underline{B})$ *para elementos* $\underline{A}, \underline{B}$ *de* $\mathcal{H}(2,2,1)$ *satisfazendo*

$$
\begin{array}{llll}
\text{(I)} & \underline{A} & = & \left(E_{11}, \quad \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}; \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}; \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}\right), \\
\text{(II)} & \underline{B} & = & \left(0, \quad 0; \begin{pmatrix} * & * \\ * & * \end{pmatrix}, \begin{pmatrix} * & * \\ * & * \end{pmatrix}; \begin{pmatrix} * & * \\ * & * \end{pmatrix}\right)
\end{array}
$$

com $\det(A_2) = 0$*.*

Demonstração. A forma requirida para o par $(C_1, C_2) \in \mathcal{H}(2,0,0)$, bem como para o par $(C_1', C_2'; C_1'') \in \mathcal{H}(0,2,1)$, é obtida exatamente da mesma maneira como na demonstração de Proposição 3.4.6. □

Vejamos agora a seguinte observação, a qual nos permite refinar ainda mais as formas canônicas obtidas nas proposições anteriores.

Observação 3.4.9. Suponhamos que $\underline{A}, \underline{B} \in \mathcal{H}(2,2,1)$ satisfazem as condições (I) e (II) da Proposição 3.4.6 ou 3.4.7 ou 3.4.8. Se para algum par da lista

$$(A_1, B_1),\ (A_2, B_2),\ (A_1', B_1'),\ (A_2', B_2'),\ (A_1'', B_1'') \tag{3.6}$$

tivermos uma das entradas seguramente não nula, então módulo a equivalência $\overset{\text{lin}}{\approx}$ podemos assumir que esta entrada é igual a 1 (e $\underline{A}, \underline{B}$ continuam satisfazendo as condições (I) e (II)). Esta observação pode ser aplicada apenas uma vez a cada um dos pares da lista (3.6).

Consideremos agora as seguintes notações. Como os elementos de M_2 (veja Seção 3.1) são unicamente determinados pelos índices $\underline{i} = (i_1, \ldots, i_r)$, $\underline{j} = (j_1, \ldots, j_s)$, $\underline{k} = (k_1, \ldots, k_l)$ with $r, s \geq 0$ and $l > 0$, escreveremos $\theta_{\underline{j}}^{\underline{i}}(\underline{k})$ para o elemento correspondente de M_2. A saber,

- $\theta^{i_1,\ldots,i_r} = \mathrm{tr}(Y_{i_1} \cdots Y_{i_r})$ and $\theta_{j_1,\ldots,j_s} = \mathrm{tr}(Z_{j_1} \cdots Z_{j_s})$,
- $\theta_{j_1,\ldots,j_s}^{i_1,\ldots,i_r}(k) = \mathrm{tr}(Y_{i_1} \cdots Y_{i_r} \cdot X_k \cdot Z_{j_1} \cdots Z_{j_s} \cdot X_k^*)$,
- $\theta_{j_1,\ldots,j_s}^{i_1,\ldots,i_r}(k_1, \ldots, k_{2t}) = \mathrm{tr}(Y_{i_1} \cdots Y_{i_r} \cdot X_{k_1} \cdot Z_{j_1} \cdots Z_{j_s} \cdot X_{k_2}^* \cdots X_{k_{2t-1}} X_{k_{2t}}^*)$.

Dados $\underline{A}, \underline{B} \in \mathcal{H}(m, p, q)$, escreveremos $\Theta_{\underline{j}}^{\underline{i}}(\underline{k})$ para a equação $\theta_{\underline{j}}^{\underline{i}}(\underline{k})(\underline{A}) - \theta_{\underline{j}}^{\underline{i}}(\underline{k})(\underline{B})$ nas entradas de $\underline{A}, \underline{B}$.

Por fim, temos a seguinte proposição, a qual garante a separabilidade de M_{sep}.

Proposição 3.4.10. *Seja $\mathbb{F}$ um corpo algebricamente fechado. Suponhamos que elementos $\underline{A}, \underline{B} \in \mathcal{H}(2, 2, 1)$ não são separados por M_{sep}, onde $m = p = 2$ e $q = 1$. Então, $\underline{A}, \underline{B}$ não são separados por $h = \mathrm{tr}(Y_1 Y_2 X_1 Z_1 X_2^*)$.*

Demonstração. Suponhamos que $h(\underline{A}) \neq h(\underline{B})$. Notemos que a condição (a) da Proposição 3.4.7 é válida para $\underline{A}, \underline{B}$. Se $\det(\mathrm{span}_{\mathbb{F}}(A_1, A_2)) \neq 0$, então a condição da Proposição 3.4.7 é satisfeita para $\underline{A}, \underline{B}$. Do contrário, $\det(\mathrm{span}_{\mathbb{F}}(A_1, A_2)) = \det(\mathrm{span}_{\mathbb{F}}(B_1, B_2)) = 0$, pela Observação 3.4.4. Caso $A_1 = A_2 = B_1 = B_2 = 0$, devemos ter $h(\underline{A}) = h(\underline{B}) = 0$, o que é uma contradição. Portanto, é fácil ver que ou a condição da Proposição 3.4.6 ou a condição da Proposição 3.4.8 é válida para $\underline{A}, \underline{B}$. Pelo Lema 3.4.1, podemos aplicar o Corolário 3.2.9 a equivalência $\approx$ sobre $\mathcal{H}(2, 2, 1)$. Logo, aplicando as Proposições 3.4.6, 3.4.7, 3.4.8, respectivamente, podemos assumir que $\underline{A}$, $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.6, 3.4.7, 3.4.8, respectivamente. Assim, aplicando os Lemas 3.4.11, 3.4.12, 3.4.13 (veja a seguir), respectivamente, obtemos uma contradição. $\square$

Lema 3.4.11. *Suponhamos que $\underline{A}$ e $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.6, bem como as condições da Proposição 3.4.10. Então, $h(\underline{A}) = h(\underline{B})$.*

Demonstração. Uma vez que $\underline{A}$ e $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.6, considerando as equações Θ^1, Θ^2 e Θ_1, temos $b'_{14} = -b'_{11}$, $a'_{24} = b'_{21} + b'_{24}$ e $a''_{14} = b''_{11} + b''_{14}$, respectivamente.

Suponhamos que $a'_{13} \neq 0$, aplicando a Observação 3.4.9 a (A'_1, B'_1) podemos assumir que $a'_{13} = 1$. Então, pelas equações $\Theta^{1,2}$, $\det(A'_1) - \det(B'_1) = 0$, $\Theta^1_1(1)$ e $\Theta^1(1,2)$, obtemos $a'_{22} = -(a'_{12}a'_{23} - b'_{11}b'_{21} - b'_{13}b'_{22} - b'_{12}b'_{23} + b'_{11}b'_{24})$, $a'_{12} = (b'_{11})^2 + b'_{12}b'_{13}$, $a''_{12} = b'_{13}b''_{12}$ e $a_{22} = b_{22}b'_{13}$, respectivamente. Agora consideremos $b''_{12} \neq 0$, novamente aplicando a Observação 3.4.9 a (A''_1, B''_1) podemos assumir que $b''_{12} = 1$. Logo, de $\det(A''_1) - \det(B''_1)$, $\Theta^2_1(1)$ e $\Theta_1(1,2)$, concluímos $b''_{13} = a''_{13}b'_{13} + b''_{11}b''_{14}$, $b'_{23} = a'_{23}b'_{13}$ e $b_{23} = a_{23}b'_{13}$. Portanto, $\Theta^{1,2}_1(1,2) = -(a'_{23}b'_{11} - b'_{21})\Theta^1_1(1,2)$, e uma vez que $\underline{A}, \underline{B}$ não são separados por M_{sep}, devemos ter $h(\underline{A}) = h(\underline{B})$. Por outro lado, suponhamos $b''_{12} = 0$. Neste caso, se $b_{22} = 0$ ou $b''_{11} = 0$ obviamente temos $h(\underline{A}) = h(\underline{B})$. Assim, podemos considerar $b_{22}, b''_{11} \neq 0$, e consequentemente de $\Theta^1_1(1,2)$ and $\Theta^2_1(1,2)$, concluímos que $b'_{13} = b'_{23} = 0$, donde segue $h(\underline{A}) = h(\underline{B})$.

Suponhamos agora $a'_{13} = 0$. Neste caso, notemos que se $b''_{12} = 0$, então devemos ter $\Theta^{1,2}_1(1,2) = a'_{12}a'_{23}\Theta_1(1,2) + b''_{11}\Theta^{1,2}(1,2)$, daí uma vez que $\underline{A}, \underline{B}$ não são separados por M_{sep}, devemos ter $h(\underline{A}) = h(\underline{B})$. Logo, podemos assumir que $b''_{12} \neq 0$, e particularmente $b''_{12} = 1$. Considerando as equações $\Theta^1_1(1)$, $\det(A'_1) - \det(B'_1) = 0$, $\Theta^2_1(1)$ e $\Theta_1(1,2)$, obtemos $b'_{13} = 0$, $b'_{11}0$, $b'_{23} = a'_{23}a''_{12}$ e $b_{23} = a_{23}a''_{12}$, respectivamente. Assim, se $a_23 = 0$, então $h(\underline{A}) = h(\underline{B})$. Por outro lado, se $a_23 \neq 0$, então obtemos $\Theta^{1,2}_1(1,2) = \dfrac{a'_{23}}{a_{23}}\Theta^1_1(1)$. Portanto, como $\underline{A}, \underline{B}$ não são separados por M_{sep}, devemos ter $h(\underline{A}) = h(\underline{B})$. □

Lema 3.4.12. *Suponhamos que $\underline{A}$ e $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.7, bem como as condições da Proposição 3.4.10. Então, $h(\underline{A}) = h(\underline{B})$.*

Demonstração. Uma vez que $\underline{A}$ e $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.7, temos que o par (A_2, B_2) é um dos pares da lista:

(1) (E_{12}, E_{12});

(2) $(E_{12}, 0)$;

(3) $(\alpha E_{11}, \alpha E_{11})$, para algum $\alpha \in \mathbb{F}$.

Assim, analizaremos cada caso separadamente.

1. Suponhamos que o par (A_2, B_2) é igual a (E_{12}, E_{12}). Então, das igualdades Θ^1, Θ^2 e Θ_1, obtemos $b'_{14} = -b'_{11}$, $a'_{24} = b'_{21} + b'_{24}$ e $a''_{14} = b''_{11} + b''_{14}$. Além disso, de $\Theta^1(1,2)$, $\Theta^2(1,2)$ e $\Theta_1(1,2)$, podemos concluir $a'_{13} = b'_{13}$, $a'_{23} = b'_{23}$ e $a''_{13} = b''_{13}$, respectivamente.

Consideremos $b''_{13} \neq 0$, aplicando a Observação 3.4.9 a (A''_1, B''_1), podemos assumir que $b''_{13} = 1$. Daí, aplicando as igualdades $\Theta^1_1(1,2)$ e $\Theta^2_1(1,2)$, obtemos $b'_{11} = b'_{13}b''_{11}$ e $b'_{21} = b'_{23}b''_{11}$. Ademais, pelas equações $\Theta^1_1(1)$ e $\Theta^2_1(1)$, podemos expressar a'_{12} e a'_{22}, respectivamente. Notemos que se $b'_{13} = 0$, então $h(\underline{A}) = \boldsymbol{h}(\underline{B})$, donde segue o resultado. Por outro lado, supondo $b'_{13} \neq 0$, devemos ter $\Theta^{1,2}_1(1,2) = \dfrac{b'_{23}b''_{13}}{b'_{13}}(\det(A'_1) - \det(B'_1))$. Logo, uma vez que $\underline{A}$ e $\underline{B}$ não são separados por M_{sep}, concluímos que $h(\underline{A}) = h(\underline{B})$.

Consideremos agora $b''_{13} = 0$. Neste caso, a igualdade $\det(A''_1) - \det(B''_1) = 0$, implica $b''_{11} = 0$ ou $b''_{14} = 0$. Se $b''_{11} = 0$, então temos $h(\underline{A}) = h(\underline{B})$. Por outro lado, se $b''_{11} \neq 0$ e $b''_{14} = 0$, das equações $\Theta^1_1(1,2)$ e $\Theta^2_1(1,2)$, obtemos $b_{13} = b_{23} = 0$, portanto também teremos $h(\underline{A}) = h(\underline{B})$, o que conlcuí a demosntração.

2. Suponhamos que o par (A_2, B_2) é igual a $(E_{12}, 0)$. Neste caso, considerando a igualdade $\Theta_1(1,2)$, concluímos que $a''_{13} = 0$, donde segue $h(\underline{A}) = h(\underline{B})$.

3. Por fim, suponhamos que o par (A_2, B_2) é igual a $(\alpha E_{11}, \alpha E_{11})$. Notemos que se $\alpha = 0$, então $h(\underline{A}) = h(\underline{B})$ e temos o resultado. Assim, podemos assumir $\alpha \neq 0$. Considerando as igualdades Θ^1, Θ^2 e Θ_1, obtemos $b'_{14} = -b'_{11}$, $a'_{24} = b'_{21} + b'_{24}$ e $a''_{14} = b''_{11} + b''_{14}$, respectivamente. Além disso, das equações $\Theta^1(1,2)$, $\Theta^2(1,2)$ e $\Theta_1(1,2)$, concluímos $b'_{11} = b'_{21} = b''_{11} = 0$. Portanto, temos $\Theta^{1,2}_1(1,2) = b''_{14}\Theta^{1,2}(1,2)$. Logo, uma vez que $\underline{A}, \underline{B}$ não são separados por M_{sep}, segue que $h(\underline{A}) = h(\underline{B})$. □

Lema 3.4.13. *Suponhamos que $\underline{A}$ e $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.8, bem como as condições da Proposicão 3.4.10. Então, $h(\underline{A}) = h(\underline{B})$.*

Demonstração. Uma vez que $\underline{A}$ e $\underline{B}$ satisfazem as condições (I) e (II) da Proposição 3.4.8, concluímos que $\Theta^{1,2}_1(1,2) = -a_{23}a'_{12}\Theta^2_1(1)$. Portanto,uma vez que $\underline{A}$ e $\underline{B}$ não são separados por M_{sep}, obtemos $h(\underline{A}) = h(\underline{B})$. □

3.4.2 Minimalidade de M_{sep}

Conforme comentamos na Seção 1.3, determinar se um conjunto separador é ou não minimal pode ser uma tarefa bastante árdua. Assim, antes de mostrarmos que

M_{sep} é um conjunto separador minimal para $SI(m,p,q)$, iremos considerar o conceito de suporte de um invariante, bem como algumas de suas propriedades.

Suponhamos que $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_m$ é uma decomposição de um G-módulo sobre $\mathbb{F}$. Então, o suporte de um elemento $\underline{a} = (a_1, \ldots, a_m)$ de $\mathcal{H}$, é definido como sendo $\mathrm{supp}(\underline{a}) = (\delta_1, \ldots, \delta_m)$ para

$$\delta_i = \begin{cases} 0, & \text{if } a_i = 0 \\ 1, & \text{if } a_i \neq 0 \end{cases}.$$

A decomposição de $\mathcal{H}$ induz a $\mathbb{N}^m$-gradução em $\mathbb{F}[\mathcal{H}]$ dada pelos multigraus. Definimos o suporte de um elemento $\mathbb{N}^m$-homogêneo $f \in \mathbb{F}[\mathcal{H}]$ de multigrau $\mathrm{mdeg}\, f = \underline{d}$, como sendo $\mathrm{supp}(f) = (\delta_1, \ldots, \delta_m)$ para

$$\delta_i = \begin{cases} 0, & \text{if } d_i = 0 \\ 1, & \text{if } d_i > 0 \end{cases}.$$

A ordem parcial em $\mathbb{N}^m$ induz a ordem parcial no conjunto de todos os possíveis suportes $\{0,1\}^m$. Na observação a seguir não é necessário requerir que $\mathbb{F}[\mathcal{H}]^G$ seja $\mathbb{N}^m$-graduado pelo multigrau.

Observação 3.4.14. Sejam $\underline{a} \in \mathcal{H}$ e $f \in \mathbb{F}[\mathcal{H}]$ um elemento $\mathbb{N}^m$-homogêneo com $\mathrm{supp}(a) \not\geq \mathrm{supp}(f)$. Então, temos $f(\underline{a}) = 0$.

Observação 3.4.15. Seja M um subconjunto $\mathbb{N}^m$-homogêneo de $\mathbb{F}[\mathcal{H}]^G$ e $f \in M$. Então, $M \backslash \{f\}$ não é um conjunto separador se existem $\underline{a}, \underline{b}$ de $\mathcal{H}$ tais que

(a) $f(\underline{a}) \neq f(\underline{b})$;

(b) para cada $h \in M \backslash \{f\}$ com $\mathrm{supp}(h) \leq \mathrm{supp}(f)$ tivermos $h(\underline{a}) = h(\underline{b})$.

Demonstração. Denotemos $\mathrm{supp}(f) = \underline{\delta}$ e definamos $\underline{a'} \in \mathcal{H}$ por $a'_i = 0$ caso $\delta_i = 0$ e $a'_i = a_i$ se $\delta_i = 1$. Então, $\mathrm{supp}(\underline{a'}) \leq \underline{\delta}$ e $h(\underline{a'}) = h(\underline{a})$ para cada $h \in M$ with $\mathrm{supp}(h) \leq \underline{\delta}$. Definamos também $\underline{b'}$ de maneira similar a $\underline{a'}$. Substituindo $\underline{a'}$ por $\underline{a}$ e $\underline{b'}$ por $\underline{b}$ no enunciado da observação, podemos assumir que $\mathrm{supp}(\underline{a}) \leq \underline{\delta}$ e $\mathrm{supp}(\underline{b}) \leq \underline{\delta}$. Logo, o resultado segue da Observação 3.4.14. □

Consideremos agora a proposição a seguir, a qual nos permite garantir a minimalidade do conjunto M_{sep}.

Proposição 3.4.16. *Qualquer subconjunto próprio de* M_{sep} *não é um conjunto separador para* $SI(m,p,q)$.

Demonstração. Seja f um elemento de M_{sep}. Pela observação 3.4.15, para mostrar que $M_{\text{sep}} \backslash \{f\}$ não é um conjunto separador para $SI(m,p,q)$ é suficiente construir $\underline{A}$ e $\underline{B}$ de $\mathcal{H}(m,p,q)$ tais que

(a) $f(\underline{A}) \neq f(\underline{B})$;

(b) para $h \in M_f$, temos $h(\underline{A}) = h(\underline{B})$, onde M_f é definido como o conjuntos de todos $h \in M_{\text{sep}} \backslash \{f\}$ com $\operatorname{supp}(h) \leq \operatorname{supp}(f)$.

Se f pertence a $SI(0,p,0)$ ou $SI(0,0,q)$, então a Proposição 3.3.2 implica que $M_{\text{sep}} \backslash \{f\}$ não é separador.

Por simetria, sem perda de generalidade podemos assumir que f é um dos elementos da seguinte lista:

$$\det(X_1), \quad \theta(1,2) = \operatorname{tr}(X_1 X_2^*), \quad \theta(1,2,3,4) = \operatorname{tr}(X_1 X_2^* X_3 X_4^*),$$

$$\theta_1^1(1) = \operatorname{tr}(Y_1 X_1 Z_1 X_1^*), \quad \theta_1^{12}(1) = \operatorname{tr}(Y_1 Y_2 X_1 Z_1 X_1^*), \quad \theta_{12}^1(1) = \operatorname{tr}(Y_1 X_1 Z_1 Z_2 X_1^*),$$

$$\theta^1(1,2) = \operatorname{tr}(Y_1 X_1 X_2^*), \quad \theta^{12}(1,2) = \operatorname{tr}(Y_1 Y_2 X_1 X_2^*),$$

$$\theta_1(1,2) = \operatorname{tr}(X_1 Z_1 X_2^*), \quad \theta_{12}(1,2) = \operatorname{tr}(X_1 Z_1 Z_2 X_2^*),$$

$$\theta_1^1(1,2) = \operatorname{tr}(Y_1 X_1 Z_1 X_2^*),$$

onde estamos utilizando as notações da Seção 3.3. Observemos que para valores pequenos de m,p,q, não precisamos considerar certos elementos da lista dada acima, por exemplo, se $m < 4$, então não consideramos $\theta(1,2,3,4)$, etc.

Suponhamos que um elemento f da lista acima satisfaz a condição que

$$\operatorname{supp}(f) = (\underbrace{1,\ldots,1}_{d},0,\ldots,0;\underbrace{1,\ldots,1}_{d'},0,\ldots,0;\underbrace{1,\ldots,1}_{d''},0,\ldots,0)$$

para algum $\underline{d} = (d,d',d'') \in \mathbb{N}^3$. Então, construímos

$$\underline{A} = (A_1,\ldots,A_d,0,\ldots,0;A_1',\ldots,A_{d'}',0,\ldots,0;A_1'',\ldots,A_{d''}'',0,\ldots,0),$$

$$\underline{B} = (B_1,\ldots,B_d,0,\ldots,0;B_1',\ldots,B_{d'}',0,\ldots,0;B_1'',\ldots,B_{d''}'',0,\ldots,0)$$

satisfazendo as condições (a) e (b) como segue:

- se $f = \det(X_1)$, então $\underline{d} = (1,0,0)$ e tomamos

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad B_1 = 0;$$

- se $f = \theta(1,2)$, temos $\underline{d} = (2,0,0)$ e basta considerar

$$A_1 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = E \quad \text{e} \quad B_1 = B_2 = 0;$$

- para $f = \theta(1,2,3,4)$, então $\underline{d} = (4,0,0)$ e consideramos

$$A_1 = B_1 = E,\ A_2 = B_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad A_3 = E_{22},\ A_4 = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix},\ B_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

- para $f = \theta_1^1(1)$, temos $\underline{d} = (1,1,1)$ e tomamos

$$A_1 = B_1 = E_{12},\ A_1' = A_1'' = E_{21},\ B_1' = B_1'' = 0;$$

- se $f = \theta_1^{12}(1)$, teremos $\underline{d} = (1,2,1)$ e basta tomar

$$A_1 = E_{22},\ A_1' = E_{12},\ A_2' = E_{11},\ A_1'' = -E_{21},$$

$$B_1 = E_{21},\ B_1' = E_{12},\ B_2' = E_{22},\ B_1'' = E_{12}.$$

- se $f = \theta^1(1,2)$, temos $\underline{d} = (2,1,0)$ e consideramos

$$A_1 = B_1 = E_{11},\ A_2 = 0,\ B_2 = E_{12},\ A_1' = B_1' = E_{21};$$

- para $f = \theta^{12}(1,2)$, temos $\underline{d} = (2,2,0)$ e tomamos

$$A_1 = B_1 = E_{11},\ A_2 = B_2 = E_{12},\ A_1' = B_1' = E_{21},\ A_2' = E_{22},\ B_2' = E_{11};$$

- para $f = \theta_1^1(1,2)$, então $\underline{d} = (2,1,1)$ e basta considerar

$$A_1 = B_1 = E_{11}, A_2 = E_{21}, B_2 = -E_{11} + E_{21}, A_1' = B_1' = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_1'' = B_1'' = E_{12}.$$

Para $m = p = q = 2$ o isomorfismo ι^* introduzido na Observação 3.1.2 manda

$$\det(X_1),\ \det(X_2),\ \theta^{\underline{i}},\ \theta_{\underline{j}},\ \theta_{\underline{j}}^{\underline{i}}(1),\ \theta_{\underline{j}}^{\underline{i}}(2),\ \theta^{\underline{i}}(1,2),\ \theta_{\underline{j}}(1,2), \quad \text{respectivamente,} \quad \text{para}$$

$$\det(X_2),\ \det(X_1),\ \theta_{\underline{i}},\ \theta^{\underline{j}},\ \theta_{\underline{i}}^{\underline{j}}(2),\ \theta_{\underline{j}}^{\underline{i}}(2),\ \theta_{\underline{i}}(1,2),\ \theta^{\underline{j}}(1,2), \quad \text{respectivamente,}$$

para todos $\underline{i} = (i_1, \ldots, i_r)$, $\underline{j} = (j_1, \ldots, j_s)$ com $0 \leq r, s \leq 2$. Portanto, podemos reduzir os casos em que f é um dos elementos $\theta_{12}^1(1)$, $\theta_1(1,2)$, $\theta_{12}(1,2)$, $\theta_{12}^1(1,2)$, para os casos já considerados acima. Segue então o resultado. $\square$

Portanto, unindo as Proposições 3.3.1, 3.4.10 e 3.4.16, temos o teorema a seguir:

Teorema 3.4.17. *Sejam* $\mathbb{F}$ *um corpo algebricamente fechado de característica diferente de dois e* $m, p, q \geq 0$ *não todos nulos. Então, o conjunto* M_{sep} *é um conjunto separador minimal para* $SI(m, p, q)$*.*

Referências

[1] A.A. Lopatin, *The algebra of invariants of* 3×3 *matrices over a field of arbitrary characteristic*, Commun. Algebra **32** (2004), no. 7, 2863–2883.

[2] A.A. Lopatin, *The invariant ring of triples of* 3×3 *matrices over a field of arbitrary characteristic*, Sibirsk. Mat. Zh. **45** (2004), No. 3, 624–633 (Russian). English translation: Siberian Mathematical Journal **45** (2004), No. 3, 513–521.

[3] A.A. Lopatin, *Relatively free algebras with the identity* $x^3 = 0$, Commun. Algebra **33** (2005), no. 10, 3583–3605.

[4] A.A. Lopatin, *Minimal generating set for semi-invariants of quivers of dimension two*, Linear Algebra and its Applications, **434** (2011), no. 8, 1920–1944.

[5] A. Lopatin, F. Reimers, *Separating invariants for multisymmetric polynomials*, arXiv: 1911.04850v1, submitted.

[6] C. Procesi, *The invariant theory of* $n \times n$ *matrices*, Adv. Math. **19** (1976), 306–381.

[7] C. Procesi, *Computing with* 2×2 *matrices*, J. Algebra **87** (1984), 342–359.

[8] D. Đoković, *Poincaré series of some pure and mixed trace algebras of two generic matrices*, J. Algebra **309** (2007), 654–671.

[9] D. Đoković, *On orthogonal and special orthogonal invariants of a single matrix of small order*, Lin. Multilin. Algebra **57** (2009) no. 4, 345–354.

[10] F. B. Cavalcante, A. Lopatin, *Separating invariants of three nilpotent* 3×3 *matrices*, Linear Algebra and its Applications, 607 (2020), pp. 9–28.

[11] F. Reimers, *Separating invariants for two copies of the natural* S_n*-action*, Communications in Algebra **48** (2020), 1584–1590.

[12] G. Ivanyos, Y. Qiao and K.V. Subrahmanyam, *On generating the ring of matrix semi-invariants*, arXiv:1508.01554v1, 2015.

[13] G. Ivanyos, Y. Qiao and K.V. Subrahmanyam, *Non-commutative Edmonds' problem and matrix semi-invariants*, Comput. Complexity *26* (2017), no. 3, 717-763.

[14] G. Kemper, A. Lopatin, F. Reimers, *Separating invariants over finite fields*, in preparation.

[15] H. Derksen, G. Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, 130. Springer-Verlag, Berlin, 2002. x+268 pp.

[16] H. Derksen, G. Kemper, *Computational invariant theory (second edition)*, Encyclopaedia of Mathematical Sciences, 130. Springer-Verlag, Berlin, Heidelberg, 2015. xxii+366 pp.

[17] H. Derksen, V. Makam, *Hilbert series and degree bounds for matrix (semi-)invariants*, J. Algebra **454** (2016), 14–28.

[18] H. Derksen, V. Makam, *Polynomial degree bounds for matrix semi-invariants*, Adv. Math. **310** (2017), 44–63.

[19] H. Derksen, V. Makam, *Generating invariant rings of quivers in arbitrary characteristic*, J. Algebra **489** (2017), 435–445.

[20] H. Derksen, V. Makam, *Degree bounds for semi-invariant rings of quivers*, J. Pure Appl. Algebra **222** (2018), no. 10, 3282–3292.

[21] H. Derksen, V. Makam, *Weyl's polarization theorem in positive characteristic*, Transformation Groups (2020), https://doi.org/10.1007/s00031-020-09559-3.

[22] H. Derksen, V. Makam, *Algorithms for orbit closure separation for invariants and semi-invariants of matrices*, arXiv: 1801.02043v2.

[23] I. Kaygorodov, A. Lopatin, Yu. Popov, *Separating invariants for* 2×2 *matrices*, Linear Algebra and its Applications **559** (2018), 114–124.

[24] J. Draisma, G. Kemper, D. Wehlau, *Polarization of separating invariants*, Canad. J. Math. **60**, (2008) No. 3, 556–571.

[25] K.S. Sibirskii, *Algebraic invariants of a system of matrices*, Sibirsk. Mat. Zh. **9** (1968), No. 1, 152–164 (Russian). English translation: Soviet Math. Dokl. **8** (1967), 36–40.

[26] M. Domokos, *Relative invariants of* 3×3 *matrix triples*, Linear and Multilinear Algebra **47** (2000), no. 2, 175–190.

[27] M. Domokos, *Poincaré series of semi-invariants of* 2×2 *matrices*, Linear Algebra Appl. **310** (2000), no. 1-3, 183–194.

[28] M. Domokos, V. Drensky, *Gröbner bases for the rings of special orthogonal and* 2×2 *matrix invariants*, J. Algebra **243** (2001), no. 2, 706–716.

[29] M. Domokos, S.G. Kuzmin, A.N. Zubkov, *Rings of matrix invariants in positive characteristic*, J. Pure Appl. Algebra **176** (2002), 61–80.

[30] M. Domokos, *Typical separating invariants*, Transform. Groups **12** (2007), 49–63.

[31] M. Domokos, V. Drensky, *Defining relation for semi-invariants of three by three matrix triples*, J. Pure Appl. Algebra **216** (2012), no. 10, 2098–2105.

[32] M. Domokos, *Characteristic free description of semi-invariants of* 2×2 *matrices*, J. Pure Appl. Algebra **224** (2020), no. 5, 106220.

[33] M. Domokos, *Addendum to "Characteristic free description of semi-invariants of* 2×2 *matrices"*, J. Pure Appl. Algebra **224** (2020), no. 6, 106270.

[34] M. Nagata, *On the 14th problem of Hilbert*, Amer. J. Math. 81 (1959), 766-772.

[35] R.J.S. Ferreira, A. Lopatin, *Minimal generating and separating sets for* $O(3)$*-invariants of several matrices*, arXiv: 1810.10397v1, submitted.

[36] S.A. Amitsur, *On the characteristic polynomial of a sum of matrices*, Linear and Multilinear Algebra **8** (1980), 177–182.

[37] S. Donkin, *Invariants of several matrices*, Invent. Math. **110** (1992), 389–401

[38] T. A. Springer, *Invariant Theory*, Lect. Notes Math. 585, Springer, 1977

[39] V. Drensky, L. Sadikova, *Generators of invariants of two* 4×4 *matrices*, C. R. Acad. Bulgare Sci. **59** (2006), No. 5, 477–484.

[40] Y. Teranishi, *The ring of invariants of matrices*, Nagoya Math. J. **104** (1986), 149–161.