UNICAMP

UNIVERSIDADE ESTADUAL DE
CAMPINAS

Instituto de Matemática, Estatística e
Computação Científica

RAMON CÓDAMO BRAGA DA COSTA

Identidades Fracas Matriciais com Ação de Grupo Finito, Propriedade de Specht e Identidades de Laurent

Campinas

2023

Ramon Códamo Braga da Costa

Identidades Fracas Matriciais com Ação de Grupo Finito, Propriedade de Specht e Identidades de Laurent

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: Plamen Emilov Kochloukov

Este trabalho corresponde à versão final da Tese defendida pelo aluno Ramon Códamo Braga da Costa e orientada pelo Prof. Dr. Plamen Emilov Kochloukov.

Campinas

2023

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Silvania Renata de Jesus Ribeiro - CRB 8/6592

C823i	Costa, Ramon Códamo Braga da, 1984- Identidades fracas matriciais com ação de grupo finito, propriedade de Specht e identidades de Laurent / Ramon Códamo Braga da Costa. – Campinas, SP : [s.n.], 2023. Orientador: Plamen Emilov Kochloukov. Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica. 1. Identidade polinomial. 2. Identidades polinomiais graduadas. 3. Propriedade de Specht. 4. Álgebras de grupo. 5. Grupos finitos. I. Kochloukov, Plamen Emilov, 1958-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: Weak identities of matrices with finite group actions, Specht property and Laurent identities
Palavras-chave em inglês:
Polynomial identity
Graded polynomial identities
Specht property
Group algebras
Finite groups
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Plamen Emilov Kochloukov [Orientador]
Mikhailo Dokuchaev
Adriano Adrega de Moura
Claudemir Fideles Bezerra Júnior
Dimas José Gonçalvez
Data de defesa: 18-08-2023
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-3762-2538
- Currículo Lattes do autor: http://lattes.cnpq.br/3408770584857053

Tese de Doutorado defendida em 18 de agosto de 2023 e aprovada

pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). PLAMEN EMILOV KOCHLOUKOV

Prof(a). Dr(a). MIKHAILO DOKUCHAEV

Prof(a). Dr(a). ADRIANO ADREGA DE MOURA

Prof(a). Dr(a). CLAUDEMIR FIDELES BEZERRA JUNIOR

Prof(a). Dr(a). DIMAS JOSÉ GONÇALVES

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.

À minha família.

Agradecimentos

Deveria ser sempre fácil agradecer às pessoas que foram importantes em uma longa e trabalhosa jornada, mas invariavelmente somos tentados frequentemente a mensurar a contribuição de cada um nesse processo e esse é um problema sem solução. Deste modo, já deixo aqui registrados, de maneira mais imprecisa, os mais sinceros agradecimentos a todos que direta ou indiretamente contribuíram para esse desfecho, em especial aos meus amigos da pós-graduação.

Sou eternamente grato à minha esposa Graziela, que por diversas vezes precisou ser forte, sobretudo nos momentos em que estive longe enquanto nossa maior fonte de amor, nossa filha Luiza, esteve doente.

Sou eternamente grato aos meus familiares. Particularmente, sou grato à dona Edith Ribeiro da Silva, minha avó. Mulher forte que cuidou de três filhos sozinha, pouco acesso teve à educação formal e como se isso fosse pouco, recentemente envolveu-se em mais uma batalha da qual saiu vitoriosa, a luta contra o câncer.

Sou grato à UNICAMP como um todo, mas devo deixar registrados aqui meus mais sinceros agradecimentos ao meu orientador, professor Plamen, que sugeriu os principais temas deste trabalho, que sempre ajudou-me quando necessário e sempre conseguiu algum tempo, ainda não sei como, para esclarecer às minhas, possivelmente pueris, dúvidas. E claro, não poderia deixar de agradecer ao professor Plamen por toda ajuda na correção de erros cometidos por mim na escrita deste trabalho. Sou grato por todos os conselhos, mas também pelas conversas informais; curiosamente, por vezes isso ajudou muito. Por fim, correndo o risco de cometer, acidentalmente, o crime da bajulação, devo dizer que não são todos que têm a oportunidade de trabalhar com alguém como o professor Plamen, pessoa de reconhecida capacidade e experiência, só tenho, portanto, a agradecer.

Agradeço também a todos os membros da banca por dedicar parte preciosa de seu tempo para análise deste trabalho.

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

Resumo

Neste trabalho obtemos uma base de identidades com ação de um grupo finito de automorfismos para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$. Estes grupos são os subgrupos finitos do grupo de automorfismos de $M_2(\mathbb{C})$, tais grupos são conhecidos há muito tempo (formalmente desde aproximadamente 1870, embora ainda na Grécia antiga fosse conhecida a descrição dos poliedros regulares). Eles consistem dos subgrupos finitos de $PGL_2(\mathbb{C})$, os quais são $\mathbb{Z}_n$, D_n, A_4, A_5 e S_4. De modo semelhante ao que foi feito para $M_2(\mathbb{C})$ por A. Berele [6] e $sl_2(\mathbb{C})$ por P. Koshlukov e A. D. M. Mortari [32], precisávamos de base de identidades fracas $\mathbb{Z}_2$-graduadas para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$, mas esta base ainda não era conhecida, então primeiramente exibimos uma tal base. Mostramos também, considerando apenas anéis (unitários) associativos, comutativos e Noetherianos, que o ideal de identidades $\mathbb{Z}_2$-graduadas do par $(M_2(A), sl_2(A))$ satisfaz a Propriedade de Specht, a qual afirma (neste caso) que todo ideal de identidades fracas $\mathbb{Z}_2$-graduadas que contém todas as identidades fracas graduadas do par $(M_2(A), sl_2(A))$ possui base finita. No último capítulo, mostramos que as identidades de Laurent do grupo de unidades da álgebra relativamente livre $\mathcal{F} = \langle y_1, y_2 \mid y_1^2 = y_2^2 = 0 \rangle$ são as mesmas que as do grupo linear geral $GL_2(F)$ se F é qualquer corpo infinito quadraticamente fechado. Estas identidades são importantes, pois mostram sob quais condições a chamada Conjectura de Hartley para identidades de Laurent continua válida.

Palavras-chave: Identidades polinomiais. Identidades graduadas. Identidades de Laurent. Ação de grupo. Propriedade de Specht.

Abstract

In this work, we obtain a basis of the identities for the pair $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$ acted on by a finite group of automorphisms. These groups are the finite subgroups of the automorphism group of $M_2(\mathbb{C})$. They have been known for a long time (formally since around 1870, although in ancient Greece they knew a description of the regular polyhedra). These consist of the finite subgroups of $PGL_2(\mathbb{C})$, which are $\mathbb{Z}_n$, D_n, A_4, A_5 and S_4. Similarly to what was done for $M_2(\mathbb{C})$ by A. Berele [6] and for $sl_2(\mathbb{C})$ by P. Koshlukov and A. D. M. Mortari [32], we needed a basis of $\mathbb{Z}_2$-graded weak identities for the pair $(M_2(\ C), sl_2(\mathbb{C}))$, but this base was not yet known. Thus, we had describe such a basis. We also show, considering only associative, commutative, and Noetherian (unitary) rings, that the ideal of $\mathbb{Z}_2$-graded identities of the pair $(M_2(A), sl_2(A))$ satisfies the Specht property, which states (in this case) that every ideal of $\mathbb{Z}_2$-graded weak identities that contains all graded identities of the pair $(M_2(A), sl_2(A))$, has a finite basis. In the last chapter, we show that the Laurent identities of the group of units of the relatively free algebra $\mathcal{F} = \langle y_1, y_2 \mid y_1^2 = y_2^2 = 0\rangle$ are the same as those of the general linear group $GL_2(F)$ if F is any quadratically closed infinite field. These identities are important because they show under which conditions the Hartley Conjecture for Laurent identities remains valid.

Keywords: Polynomial identities. Graded identities. Laurent's identities. Group action. Specht property.

Sumário

Introdução

Seja F um corpo, $X = \{x_1, x_2, \ldots\}$ um conjunto enumerável de variáveis (não comutativas) e $F\langle X\rangle$ a álgebra associativa livre e livremente gerada por X sobre o corpo F. Seus elementos são chamados de polinômios não comutativos. Dizemos que uma F-álgebra associativa A satisfaz uma identidade polinomial $f \in F\langle X\rangle$, ou $f = 0$, se $f(a_1, \ldots, a_k) = 0$ para cada $a_1,\ldots,$ $a_k \in A$. Se uma álgebra satisfaz uma identidade polinomial não nula, dizemos que esta álgebra é uma PI-álgebra. Os primeiros trabalhos envolvendo o estudo de álgebras satisfazendo identidades polinomiais começaram por volta de 1922, de maneira bem implícita, com o artigo de M. Dehn [9], em uma tentativa de generalizar o Teorema de Pappus da geometria projetiva. Em 1937, W. Wagner [54], também trabalhando com geometria projetiva, obteve uma identidade polinomial satisfeita pela álgebra das matrizes 2×2. Álgebras satisfazendo identidades polinomiais, não triviais, são chamadas de PI-álgebras e o estudo de tais álgebras pertence ao campo da Matemática chamado de PI-teoria. Embora nos dias atuais esta seja uma área de pesquisa muito ativa, ela passou a ser objeto de maior atenção somente a partir de 1948 com o trabalho de I. Kaplansky [23]. Foi neste trabalho que surgiu pela primeira vez o termo "Polynomial Identity". Em 1950, A. S. Amitsur e J. Levitzki [3] provaram que a álgebra de matrizes $M_n(A)$, onde A é qualquer F-álgebra comutativa, satisfaz o polinômio standard St_{2n}. Este resultado foi muito celebrado e várias demonstrações foram dadas a este.

Se A é uma PI-álgebra, então o conjunto $Id(A)$ de todas as identidades satisfeitas por A é um ideal chamado de T-ideal, aqui a letra T vem de $Transformation$, uma referência aos elementos do anel de endomorfismos lineares da álgebra livre $F\langle X\rangle$. O motivo para isto é que todo T-ideal é invariante pela ação dos endomorfismos da álgebra $F\langle X\rangle$ e esta propriedade caracteriza os ideais de identidades, ou seja, todo ideal I que é invariante por endomorfismos é um T-ideal, pois $I = Id(F\langle X\rangle/I)$.

Há uma extensa lista de álgebras que satisfazem identidades polinomiais. Fazem parte desta lista as álgebras comutativas, as anticomutativas, as álgebras algébricas de grau limitado, as álgebras de dimensão finita, as álgebras nilpotentes e muitas outras. Vários problemas podem ser abordados quando se estudam álgebras com identidades polinomiais. Dentre estes estão aqueles que propõem a obtenção de informações a respeito da estrutura das álgebras que satisfazem algum tipo de identidade polinomial, por exemplo,

I. Kaplansky [23] provou o seguinte:

Teorema 0.1. *Seja A uma F-álgebra primitiva e suponha que A satisfaz uma identidade polinomial de grau n. Então:*

1. *$A \cong M_t(D)$, para alguma álgebra de divisão D sobre F e $t > 0$;*

2. *Se K é o centro de D, então $dim_K A = m^2$, com $1 \leqslant m \leqslant n/2$;*

3. *$A \subseteq E \otimes_K A \cong M_m(E)$, sendo E um subcorpo maximal de D.*

Uma outra classe de problemas, a qual é o objeto principal deste trabalho, consiste em determinar uma base de identidades polinomiais para o ideal formado por todas as identidades satisfeitas por uma dada álgebra. Em outras palavras, queremos obter um conjunto de identidades a partir do qual podemos gerar (de um certo modo) todas as demais.

Em geral é muito difícil encontrar base de identidades para uma dada álgebra, mas existem alguns bons casos de sucesso. Seja V um espaço vetorial com base e_1,e_2, $\ldots$, e $E = E(V)$ a álgebra de Grassmann de V, ou seja, E é a álgebra com base formada por 1 e os monômios $e_{i_1} \cdots e_{i_k}$, $i_1 < i_2 < \cdots < i_k$, satisfazendo $e_ie_j = -e_je_i$, $e_i^2 = 0$. Se $char F \neq 2$, as duas últimas relações equivalem. (Se $char F = 2$ E é comutativa.)

No ano de 1973, Krakowski e Regev [34] obtiveram uma base de identidades para a álgebra de Grassmann E de um espaço vetorial de dimensão infinita, formada pela identidade $[x_1, x_2, x_3] = 0$. Ressaltamos que este mesmo resultado foi obtido antes de Krakowski e Regev por Latyshev; vale destacar que em [34] foi obtida informação muito detalhada sobre a estrutura do T-ideal de E. Em 2001, a mesma base foi obtida por Giambruno e Koshlukov [18], desta vez considerando corpos infinitos de característica diferente de 2. Também é conhecida base de identidades se considerarmos a álgebra de Grassmann de um espaço vetorial de dimensão finita, mas nesse caso precisamos acrescentar à base anterior o polinômio standard [13]. Para encerrar a lista de exemplos, devemos observar que são conhecidas bases para a álgebra $UT_n(F)$ das matrizes triangulares superiores e também para a álgebra $E \otimes E$, ver [13].

Ainda hoje não conhecemos base de identidades para a álgebra de matrizes $n \times n$, se $n > 2$. No caso $n = 2$ e F é um corpo infinito de característica diferente de 2, são conhecidas bases. Em 1973, considerando corpo de característica zero, Razmyslov [45] determinou uma base finita de identidades para o T-ideal de $M_2(F)$ formada por 9 identidades de grau no máximo 6. Alguns anos mais tarde, V. S. Drensky [12] determinou uma base minimal para $M_2(F)$ em característica zero. Para corpos infinitos de característica $p > 2$, o problema foi resolvido por Koshlukov [29] e uma base minimal foi obtida para a maioria dos casos. Em característica 2, o problema continua em aberto e acredita-se que neste caso não há base finita. Agora, sobre corpos finitos, Yu. N. Malt'sev e E. N. Kuzmin [41] descreveram uma base finita para $M_2(F)$. Eles provaram o seguinte:

Teorema 0.2. *O ideal de identidades de $M_2(GF(q))$, $q = p^n$, é gerado pelos polinômios*

1. $f_1(x, y) = (x - x^q)(y - y^{q^2})(1 - [x, y]^{q-1})$;
2. $f_2(x, y) = (x - x^q) \circ (y - y^q) - [(x - x^q) \circ (y - y^q)]^q$,

sendo $[x, y] = xy - yx$ *e* $x \circ y = xy + yx$.

Também são conhecidas bases de identidades para $M_3(F)$ e $M_4(F)$ se F é um corpo finito, ver [15] e [16]. É natural, portanto, perguntar quando o T-ideal de uma álgebra com identidades possui uma base finita. Em 1950, W. Specht [50] fez exatamente esta pergunta, a qual ficou conhecida como Problema de Specht.

Toda álgebra associativa sobre corpo de característica zero possui base finita de suas identidades polinomiais?

Em 1987, A. R. Kemer [26] deu uma resposta positiva para o Problema de Specht e para isso precisou fazer uso das chamadas identidades polinomiais graduadas, as quais definiremos em breve. O Problema de Specht não possui resposta positiva, em geral, se a característica do corpo é diferente de zero. Em 1999, A.Ya. Belov [4] obteve, para cada corpo de característica positiva, um T-ideal que não possui base finita. Ainda em 1999, Shchigolev [49] e A. V Grishin [21] obtiveram outros contraexemplos.

Dizemos que uma álgebra A, ou o seu T-ideal $Id(A)$, possui a propriedade de Specht se cada T-ideal contendo $Id(A)$ (inclusive o próprio $Id(A)$) possui base finita. Como consequência imediata do resultado de Kemer, toda álgebra associativa sobre corpo de característica zero possui a propriedade de Specht. Em 1973, Kruse [35] provou o seguinte.

Teorema 0.3. *As identidades satisfeitas por qualquer anel finito são finitamente baseadas.*

Como consequência do teorema anterior, obtem-se que $M_n(F)$ satisfaz a propriedade de Specht se F é um corpo finito. A mesma conclusão pode ser obtida do trabalho de L'vov [40]. Como dito anteriormente, temos base finita para $M_2(F)$ se $char F \neq 2$ e F é infinito, mas não sabemos se $M_2(F)$ satisfaz a propriedade de Specht se $char F \neq 0$.

Definição 0.4. *Dizemos que uma álgebra A é graduada por um grupo G, ou G-graduada, se pode ser escrita como uma soma direta de subespaços $A^{(g)}$, $g \in G$, de modo que $A^{(g)}A^{(h)} \subseteq A^{(gh)}$, para cada g, $h \in G$. Dizemos que os elementos de $A^{(g)}$ são homogêneos e possuem grau de homogeneidade (ou grau homogêneo) g e que $A^{(g)}$ é um subespaço homogêneo para cada $g \in G$.*

Como no caso de identidades polinomiais, podemos construir uma álgebra associativa livre G-graduada e, neste caso, faz sentido então falar de identidades polinomiais G-graduadas. Seja G um grupo e $X = \cup_{g\in G} X^{(g)}$ uma união disjunta de conjuntos enumeráveis $X^{(g)} = \{x_i^{(g)} \mid i \geqslant 1\}$. Agora podemos munir a álgebra associativa livre, livremente gerada por X, de uma G-graduação $F\langle X\rangle = \oplus_{g\in G} F\langle X\rangle^{(g)}$, onde para cada $g \in G$, $F\langle X\rangle^{(g)}$ denota o subespaço gerado pelos monômios $x_{i_1}^{(g_1)} \cdots x_{i_k}^{(g_k)}$ tais que $g = g_1 \cdots g_k$. Esta álgebra é livre na classe das álgebras G-graduadas. Uma identidade polinomial graduada para A é apenas um elemento $f(x_1^{(g_1)}, \ldots, x_k^{(g_k)}) \in F\langle X\rangle$ para o qual $f(a_1, \ldots, a_k) = 0$, sejam quais forem os elementos $a_i \in A^{(g_i)}$.

Como já comentamos, as identidades graduadas foram usadas por Kemer como uma ferramenta essencial para obter uma resposta ao Problema de Specht. Isso foi um incentivo adicional para que tais álgebras tenham se tornado um objeto atrativo na PI-teoria e muita pesquisa tem sido realizada neste campo.

Seja F um corpo infinito. Podemos tornar a álgebra de matrizes 2×2, uma álgebra $\mathbb{Z}_2$-graduada fazendo $M_2(F) = M_2^{(0)} \oplus M_2^{(1)}$, com $M_2^{(0)} = \{ae_{11} + de_{22} \mid a, d \in F\}$ e $M_2^{(1)} = \{be_{12} + ce_{21} \mid b, c \in F\}$. Em 1992, Di Vincenzo [10] considerando $char F = 0$, obteve uma base finita de identidades $\mathbb{Z}_2$-graduadas para $M_2(F)$. Esta é formada pelos polinômios $[y_1, y_2]$ e $z_1z_2z_3 - z_3z_2z_1$, onde y_i tem grau de homogeneidade 0 e z_i tem grau de homogeneidade 1. A mesma base foi obtida por P. Koshlukov e S. Azevedo [30], mas desta vez para corpo infinito de característica diferente de 2. Na verdade a demonstração que obtiveram continua válida se considerarmos domínio de integridade infinito no lugar de corpo. No mesmo artigo, Koshlukov e Azevedo descreveram uma base de identidades $\mathbb{Z}_2$-graduadas para

$$E \otimes E = (E_0 \otimes E_0 \oplus E_1 \otimes E_1) \oplus (E_0 \otimes E_1 \oplus E_1 \otimes E_0),$$

sendo E_0 o centro de E, ou seja, E_0 é o espaço vetorial gerado por 1 e por todos os monômios $e_{i_1} \cdots e_{i_k} \in E$ de grau par, enquanto que E_1 é o espaço gerado pelos monômios de grau ímpar. Ainda no mesmo trabalho, os autores obtiveram base de identidades $\mathbb{Z}_2$-graduadas para a importante álgebra de matrizes 2×2 sobre a álgebra de Grassmann

$$M_{1,1}(E) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in E_0, b, c \in E_1 \right\},$$

sendo a graduação dada por $M_{1,1}(E) = B_0 \oplus B_1$, com

$$B_0 = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix},$$

para a, $d \in E_0$ e b, $c \in E_1$. A base obtida para $M_{1,1}(E)$ e $E \otimes E$ coincidem se $char F = 0$ e consiste de duas identidades $[y_1, y_2]$ e $z_1z_2z_3 + z_3z_2z_1$, a mesma base obtida por Di Vincenzo

[10]. Por outro lado, se $charF = p > 2$, então adiciona-se a identidade $y_1^p z_1 - z_1 y_1^p$ (a qual não é identidade para $M_{1,1}(E)$), para obter-se base das identidades graduadas de $E \otimes E$.

Di Vincenzo [10] também mostrou que $M_{1,1}(E)$ e $E \otimes E$ são PI-equivalentes, ou seja, possuem as mesmas identidades ordinárias se $charF = 0$. Este resultado já era conhecido há algum tempo, pois segue da teoria de estrutura de Kemer [25] para variedades de álgebras. No entanto Di Vincenzo demonstrou este resultado sem usar teoria estrutural. Em 1999, Vasilovsky forneceu uma base de identidades $\mathbb{Z}_n$-graduadas para a álgebra das matrizes $n \times n$, ver [53].

Agora, em um cenário mais geral, resultados recentes [1, 51] garantem que para qualquer grupo finito G e corpo F de característica zero, o ideal de identidades G-graduadas de qualquer PI-álgebra G-graduada é finitamente baseado. Isso mostra, por exemplo, que a álgebra $\mathbb{Z}_2$-graduada $M_2(F)$ ou, mais geralmente, $M_n(F)$ com $\mathbb{Z}_n$-graduação, satisfaz a propriedade de Specht, e o mesmo para $E \otimes E$ e $M_{1,1}(E)$.

Definição 0.5. *Seja A uma F-álgebra associativa. Dizemos que um polinômio $f \in F\langle X\rangle$ é um polinômio central para A se*

1. *f não é uma identidade polinomial para A;*
2. *O termo constante de f é nulo;*
3. *$f(a_1, \dots, a_n) \in Z(A)$, para cada $a_1, \dots, a_n \in A$, onde $Z(A)$ denota o centro de A.*

O primeiro exemplo de polinômio central conhecido para $M_2(F)$, foi fornecido por Wagner e Hall e este é dado por $[x_1, x_2]^2$. Um outro exemplo de polinômio central, para a álgebra de Grassmann E, é o polinômio $[x_1, x_2]$.

Considere $V \subseteq A$ um subespaço de A e suponha que este gera A como álgebra. Então um polinômio $f \in F\langle X\rangle$ é dito uma identidade fraca para o par (A, V) se $f(v_1, \dots, v_n) = 0$ para cada $v_1, \dots, v_n \in V$. Identidades polinomiais fracas apareceram em PI-teoria pela primeira vez no ano de 1973 por meio dos trabalhos de Razmyslov [45, 44]. O objetivo de Razmyslov era resolver os dois seguintes, desafiadores, problemas em PI-teoria:

1. Determinar base de identidades para matrizes de ordem $n \geqslant 2$;
2. Mostrar a existência de polinômios centrais para a álgebra de matrizes de ordem arbitrária.

O segundo item foi conjecturado por Kaplansky [24] em 1970, até então o único polinômio central conhecido era o polinômio de Wagner–Hall para $M_2(F)$. Razmyslov [44] e Formanek [14] resolveram o segundo problema independentemente. Considerando corpo de característica zero e o par $(M_2(F), sl_2(F))$, Razmyslov [45] pôde resolver o primeiro problema para matrizes 2×2. No mesmo trabalho ele também determinou as identidades da álgebra de Lie $sl_2(F)$ em característica 0.

Como no caso de identidades ordinárias, ou identidades graduadas, o problema de determinar base de identidades fracas é, em geral, bem difícil. Razmyslov [45] obteve uma base de identidades fracas para o par $(M_2(F), sl_2(F))$ em característica zero. O mesmo resultado foi obtido por Koshlukov [28], desta vez considerando corpo infinito de característica diferente de 2. Em 2012, Koshlukov e Krasilnikov [31] encontraram uma base de identidades fracas $\mathbb{Z}_2$-graduadas para o par $(M_2(F), gl_2(F))$ considerando domínio de integridade infinito:

Teorema 0.6. *Sejam F um domínio de integridade infinito e $(M_2(F), gl_2(F))$ com a $\mathbb{Z}_2$-graduação natural. As seguintes identidades $\mathbb{Z}_2$-graduadas formam uma base de identidades graduadas para o par $(M_2(F), gl_2(F))$.*

$$[y_1, y_2], \quad z_1z_2z_3 - z_3z_2z_1, \quad [z_1z_2, y].$$

No Capítulo 2 demonstraremos os seguintes novos resultados. Aqui estamos considerando a $\mathbb{Z}_2$-graduação natural de $M_2(F)$.

Teorema 0.7. *Seja F um domínio de integridade infinito. As identidades*

$$[y_1, y_2], \quad z_1z_2z_3 - z_3z_2z_1, \quad yz + zy,$$

formam uma base de identidades fracas $\mathbb{Z}_2$-graduadas para o par $(M_2(F), sl_2(F))$.

Teorema 0.8. *Seja F um anel (com unidade) associativo, comutativo e Noetheriano. Então o ideal de identidades do par $\mathbb{Z}_2$-graduado $(M_2(F), sl_2(F))$ satisfaz a Propriedade de Specht.*

Um outro tipo de identidades que abordaremos aqui são as chamadas identidades polinomiais com ação de grupo. No caso de grupos abelianos finitos, estas podem ser estudadas via identidades graduadas e vice-versa. Identidades com ação de grupo são definidas de modo análogo às identidades polinomiais ordinárias e faremos isso com mais detalhes no Capítulo 1; a diferença principal é que as variáveis desta vez estão sob ação de elementos do grupo. Uma classe importante de álgebras com ação de grupo são as álgebras com involução. Neste caso, o grupo agindo na álgebra é formado por automorfismos e antiautomorfismos. Em 1969, S. A. Amitsur [3] mostrou que um anel com involução é PI se, e somente se, é *-PI. Aqui estamos interessados nos subgrupos finitos $G \subseteq Aut(A)$ agindo numa álgebra A.

Os subgrupos finitos $G \subseteq Aut(M_2(\mathbb{C}))$ são conhecidos há muito tempo e são: $\mathbb{Z}_n$, D_n, A_4, A_5 e S_4. Considerando cada um desses grupos, com exceção apenas de

$D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, A. Berele [6], exibiu uma base de identidades com ação de G para $M_2(\mathbb{C})$. Os subgrupos finitos de automorfismos da álgebra de Lie $sl_2(\mathbb{C})$ são os mesmos que os de $M_2(\mathbb{C})$. Em posse disso, Koshlukov e Mortari [32] obtiveram base de identidades com ação para a álgebra de Lie $sl_2(\mathbb{C})$. No Capítulo 3, obteremos base de identidades fracas com ação para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$. Neste caso, como $Aut(M_2(\mathbb{C}), sl_2(\mathbb{C})) = Aut(M_2(\mathbb{C}))$, os grupos agindo serão os mesmos.

Seja G um grupo e $w(x_1, \ldots, x_n)$ uma palavra (não trivial) no grupo livre gerado livremente por $X = \{x_1, x_2, \ldots\}$. Dizemos que w (ou $w = 1$) é uma identidade de grupo, ou GI, para G se $w(g_1, \ldots, g_n) = 1$ para cada $g_1, \ldots, g_n \in G$. Uma pergunta natural a se fazer é:

Quando podemos obter informações (e quais) de uma álgebra A a partir de propriedades do seu grupo de unidades $U(A)$ e vice-versa?

Se A tem "muitas" unidades, é razoável tentar responder a questão acima. Por volta de 1980, B. Hartley conjecturou que se G é um grupo de torção e $U(FG)$, o grupo de unidades da álgebra de grupo FG, satisfaz uma identidade de grupo, então FG satisfaz uma identidade polinomial. Este problema foi resolvido completamente apenas em 1999 por Liu [39]. Um apanhado histórico mais completo pode ser encontrado no Capítulo 4.

Sejam F um corpo, $X = \{X_1, X_2, \ldots\}$ um conjunto de símbolos, e denote por $\langle X_1, X_2, \ldots\rangle$ o grupo livre e livremente gerado por X. Seja $\mathcal{F}_L = F\langle X_1^{\pm 1}, X_2^{\pm 1}, \ldots\rangle$ a álgebra do grupo livre gerado por X. Seus elementos são chamados de polinômios de Laurent (em variáveis não comutativas). Os elementos de $\mathcal{F}_L$ são chamados de polinômios de Laurent e uma identidade polinomial de Laurent (ou LPI) para $U(A)$ é um polinômio de Laurent f que satisfaz $f(a_1, \ldots, a_n) = 0$, para cada $a_1, \ldots, a_n \in U(A)$. Assim, uma identidade de grupo nada mais é do que um caso particular de uma identidade de Laurent da forma $w - 1 \in \mathcal{F}_L$. Surge então, de modo natural, a seguinte pergunta:

Se G é um grupo de torção e $U(FG)$ satisfaz uma identidade de Laurent, então FG satisfaz alguma identidade polinomial?

O. Broche, J. Gonçalves e Á. Del Río [8] deram uma resposta a esta questão, considerando "boas" identidades de Laurent. Eles provaram que se o grupo de unidades de FG satisfaz uma identidade de Laurent que não é satisfeita pelo grupo de unidades da álgebra relativamente livre

$$\mathcal{F} = \langle y_1, y_2 \mid y_1^2 = y_2^2 = 0\rangle,$$

então FG satisfaz alguma identidade polinomial. No Capítulo 4, mostramos que as identidades de $U(\mathcal{F})$ são matriciais se o corpo é infinito e quadraticamente fechado, ou seja, se além de infinito, as equações $x^2 - a = 0$ tem solução em F, para cada $a \in F$.

Os resultados dos capítulos 2, 3 e 4 são novos. Os do capítulo 4 foram submetidos para publicação e os dos capítulo 2 e 3 estão em fase final de redação.

Capítulo 1

Preliminares

1.1 Identidades Polinomiais

Neste capítulo apresentaremos algumas definições e resultados importantes que serão utilizados nos capítulos seguintes, particularmente a chamada dualidade entre graduação e ação por grupo abeliano finito. A principal referência para este capítulo é o livro "Polynomial Identities and Asymptotic Methods" dos autores A. Giambruno e M. Zaicev [20]. Todas as álgebras consideradas aqui, a menos que seja dito o contrário, serão associativas com unidade.

Seja $X = \{x_1, x_2, \ldots\}$ um conjunto enumerável de variáveis e F um corpo. Denote por $F\langle X\rangle$ o espaço vetorial com base formada por todas as palavras $x_{i_1}x_{i_2}\cdots x_{i_n}$, $n \geqslant 0$. Agora defina $(x_{i_1}x_{i_2}\cdots x_{i_n})(x_{j_1}x_{j_2}\cdots x_{j_m}) = x_{i_1}x_{i_2}\cdots x_{i_n}x_{j_1}x_{j_2}\cdots x_{j_m}$. Estendendo por linearidade, esta operação torna $F\langle X\rangle$ uma álgebra associativa unitária. Esta álgebra satisfaz a seguinte propriedade universal: dada qualquer F-álgebra A associativa e qualquer função $\alpha\colon X \to A$, existe um único homomorfismo de álgebras $\widetilde{\alpha}\colon F\langle X\rangle \to A$ que estende α. Dizemos que $F\langle X\rangle$ é a álgebra associativa (unitária) livre e livremente gerada por X. Se $L\langle X\rangle$ é a subálgebra de Lie de $F\langle X\rangle^{(-)}$ gerada por X, então $L\langle X\rangle$ é a álgebra de Lie livre livremente gerada por X e também satisfaz a propriedade universal acima se trocarmos álgebras associativas por álgebras de Lie. Os elementos de $F\langle X\rangle$ são chamados de polinômios (não comutativos) e os elementos de $L\langle X\rangle$ são chamados de polinômios de Lie. A cardinalidade do conjunto X é o posto de $F\langle X\rangle$ (e de $L\langle X\rangle$).

Definição 1.1. *Seja $f \in F\langle X\rangle$. Dizemos que $f(x_1, \ldots, x_n)$ (ou $f = 0$) é uma identidade polinomial para uma álgebra A, se $f(a_1, \ldots, a_n) = 0$ para quaisquer elementos a_1, $\ldots$, $a_n \in A$. Uma álgebra satisfazendo uma identidade polinomial, não nula, é dita uma PI-álgebra.*

Embora a definição acima refira-se a álgebras sobre corpos, podemos definir de modo análogo identidades polinomiais para álgebras sobre anéis comutativos arbitrários.

Note que um polinômio f é uma identidade polinomial para uma álgebra A se $f \in Ker\,\phi$ para cada homomorfismo $\phi\colon F\langle X\rangle \to A$. Analogamente definimos identidades polinomiais para álgebras de Lie, trocando $F\langle X\rangle$ por $L\langle X\rangle$.

Exemplo 1.2. *Toda álgebra comutativa satisfaz a identidade* $[x_1, x_2] = 0$.

O polinômio dado por $St_n(x_1, \ldots, x_n) = \sum (sgn\,\sigma) x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$, com σ percorrendo todas as permutações no grupo simétrico S_n, é chamado de polinômio standard de grau n e surge com frequência em PI-teoria.

Teorema 1.3 (Amitsur-Levitzki, [2])**.** *A álgebra das matrizes* $M_n(F)$ *satisfaz o polinômio standard* $St_{2n} = 0$.

No mesmo artigo Amitsur e Levitzki mostram que $2n$ é o grau mínimo de uma identidade polinomial satisfeita por $M_n(F)$ e que uma identidade polinomial multilinear de grau $2n$ ($char F \neq 2$ ou $n > 2$), ou seja, uma identidade cujo grau em cada variável é igual a 1 em todos os seus monômios, é um múltiplo do polinômio standard. Várias demonstrações para esse teorema foram obtidas e, talvez, a mais simples seja a de Rosset [20, p.18]. Curiosamente, Swan [52] forneceu uma prova usando teoria de grafos. A demonstração dada por Amitsur e Levitzki faz uso de métodos combinatórios.

Exemplo 1.4. *Toda álgebra* A *de dimensão finita* n *satisfaz alguma identidade polinomial. Basta notar que* $St_{n+1}(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_{n+1}) = 0$ *e que quaisquer* $n+1$ *elementos de* A *são linearmente dependentes. Logo,* $St_{n+1}(a_1, \ldots, a_{n+1}) = 0$ *para quaisquer* $a_1, \ldots,$ $a_{n+1} \in A$.

Exemplo 1.5. *Seja* $A = M_2(F)$ *e* $a \in sl_2(F)$. *Então, pelo Teorema de Cayley-Hamilton, temos* $a^2 + det(a)I = 0$, *pois* $tr(a) = 0$. *Logo,* $a^2 = -det(a)I$ *é uma matriz escalar. Por outro lado, sabemos que* $[M_2(F), M_2(F)] \subseteq sl_2(F)$, *logo* $[[x_1, x_2]^2, x_3] = 0$ *é uma identidade polinomial para* $M_2(F)$ *(identidade de Hall).*

Definição 1.6. *Dizemos que um ideal* $I \subseteq F\langle X\rangle$ *é um* T*-ideal se este é invariante por todo endomorfismo* ϕ *de* $F\langle X\rangle$, *ou seja, se* $\phi(I) \subseteq I$.

Note que o conjunto formado por todas as identidades polinomiais de A é um T-ideal. Denotaremos este ideal por $Id(A)$.

Definição 1.7. *Sejam* f, $g \in F\langle X\rangle$. *Dizemos que* f *é uma consequência de* g *se* f *pode ser escrito na forma* $f = \sum u_i g(w_{i1}, \ldots, w_{in}) v_i$, *com* u_i, v_i, $w_{ij} \in F\langle X\rangle$. *Dizemos que* f *e* g *são equivalentes se são consequência um do outro.*

Definição 1.8. *Seja* $S \subseteq F\langle X\rangle$ *e* I *a interseção de todos os* T*-ideais que contêm* S. *Dizemos que* I *é o* T*-ideal gerado por* S *e que* S *é uma base para* I.

Observe que S é uma base para I se, e somente se, cada elemento $f \in I$ pode ser escrito como uma soma de consequências de elementos de S, ou seja, se $f = \sum u_i s_i(w_{i1}, \ldots, w_{in}) v_i$ com u_i, v_i, $w_{in} \in F\langle X \rangle$ e $s_i \in S$. Analogamente, define-se T-ideal, base de T-ideal, etc. para álgebras de Lie.

Neste trabalho faremos uso de vários tipos de identidades polinomiais, dentre estas estão as chamadas identidades polinomiais graduadas. Álgebras satisfazendo esse tipo de identidades têm sido cada vez mais estudadas e a principal motivação para seu estudo veio com os trabalhos de A. R. Kemer. No artigo [26] intitulado “Finite basis property of identities of associative algebras”, Kemer mostra que o T-ideal de toda PI-álgebra associativa sobre corpo de característica zero possui base finita. Álgebras graduadas desempenharam um papel crucial na demonstração desse resultado. Em 1999, A. Y. Belov [4, 5] deu os primeiros contraexemplos em característica positiva. A identidade de Hall e o polinômio standard de grau 4 geram uma base (minimal) [12] para $M_2(F)$ se $char\ F = 0$. Também são conhecidas bases (finitas) de identidades sobre corpos infinitos de característica diferente de 2, ver [29].

Definição 1.9. *Seja G um grupo. Uma álgebra A (não necessariamente associativa) é G-graduada se pode ser escrita como soma direta de subespaços $A = \oplus_{g \in G} A^{(g)}$ tais que $A^{(g)} A^{(h)} \subseteq A^{(gh)}$ para cada g, $h \in G$. Os subespaços $A^{(g)}$ são chamados de componentes homogêneas de A e cada elemento $a \in A^{(g)}$ é chamado de elemento homogêneo de grau g. Um subespaço $B \subseteq A$ é graduado (ou homogêneo) se $B = \oplus_{g \in G}(A^{(g)} \cap B)$.*

Exemplo 1.10. *Qualquer álgebra A possui uma G-graduação, seja qual for o grupo G. Basta pôr $A^{(e)} = A$ e $A^{(g)} = (0)$ se $g \neq e$, esta é a chamada graduação trivial.*

Exemplo 1.11. *Seja $G = \mathbb{Z}$ e $F\langle X \rangle$ a álgebra associativa unitária livremente gerada por X e, para cada $g \in G$, $F\langle X \rangle^{(g)}$ o subespaço gerado por todos os monômios de grau g se $g \geqslant 0$ e $F\langle X \rangle^{(g)} = 0$ se $g < 0$. Então $F\langle X \rangle$ possui G-graduação $F\langle X \rangle = \oplus_{g \in G} F\langle X \rangle^{(g)}$.*

Exemplo 1.12. *Seja $A = M_2(F)$ a álgebra de matrizes de ordem 2. Sejam $M_2^{(0)}$ e $M_2^{(1)}$, respectivamente, o subespaço das matrizes diagonais e o subespaço das matrizes com diagonal principal nula. Então $M_2(F)$ possui a seguinte $\mathbb{Z}_2$-graduação chamada natural:*

$$M_2(F) = M_2^{(0)} \oplus M_2^{(1)}.$$

Exemplo 1.13. *Toda álgebra de grupo $A = FG$ é naturalmente graduada por G. Basta definir $A^{(g)} = span\{g\}$. Uma outra graduação natural é a seguinte: considere um subgrupo normal $H \trianglelefteq G$ e $B^{(t)} = \oplus_{gH = t} A^{(g)}$, para cada $t \in G/H$. Então $A = \oplus_{t \in G/H} B^{(t)}$ é uma G/H-graduação.*

Seja G um grupo e $X = \bigcup_{g \in G} X_g$ uma união disjunta, com $X_g = \{x_1^{(g)}, x_2^{(g)}, \ldots\}$. Se $m = x_{i_1}^{(g_1)} x_{i_2}^{(g_2)} \cdots x_{i_n}^{(g_n)}$ é um monômio na álgebra associativa livre $F\langle X \rangle$, então dizemos que m tem grau de homogeneidade $g = g_1 \cdots g_n$. Agora, escreva $F\langle X\rangle = \oplus_{g\in G} F\langle X\rangle^{(g)}$, sendo $F\langle X\rangle^{(g)}$ o subespaço gerado por todos os monômios de grau de homogeneidade g. É claro que $F\langle X\rangle^{(g)} F\langle X\rangle^{(h)} \subseteq F\langle X\rangle^{(gh)}$, ou seja, $F\langle X\rangle$ é uma álgebra G-graduada. Esta álgebra é livre na classe de todas as álgebras associativas G-graduadas, ou seja, satisfaz a seguinte propriedade universal: dada qualquer álgebra $A = \oplus_{g\in G} A^{(g)}$ G-graduada e dada qualquer função $\alpha\colon X \to A$ tal que $\alpha(X^{(g)}) \subseteq A^{(g)}$, existe um único homomorfismo de álgebras $\widetilde{\alpha}\colon F\langle X\rangle \to A$ que estende α. Observe que o homomorfismo $\widetilde{\alpha}$ satisfaz $\widetilde{\alpha}(F\langle X\rangle^{(g)}) \subseteq A^{(g)}$. Qualquer homomorfismo $f\colon B \to A$ entre álgebras G-graduadas (não necessariamente associativas) tal que $f(B^{(g)}) \subseteq A^{(g)}$ é chamado de homomorfismo de álgebras G-graduadas. É comum também dizermos que α é uma função graduada ou mapa graduado. Como no caso ordinário, podemos definir monomorfismo, epimorfismo e isomorfismo de álgebras graduadas. Quando estivermos falando da álgebra livre G-graduada usaremos a notação $F\langle X\rangle^{gr}$ para evitarmos confusão. Os elementos de $F\langle X\rangle^{gr}$ são chamados de polinômios G-graduados.

Definição 1.14. *Seja G um grupo e A uma álgebra G-graduada. Dizemos que A satisfaz uma identidade polinomial G-graduada se existe um polinômio graduado não nulo $f = f(x_1^{(g_1)}, \ldots, x_n^{(g_n)}) \in F\langle X\rangle^{gr}$ tal que $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_i \in A^{(g_i)}$.*

Podemos definir de modo análogo ao caso ordinário, T-ideais de identidades graduadas, base de T-ideal, etc. O T-ideal de identidades graduadas de A será denotado por $Id^{gr}(A)$.

Exemplo 1.15. *Considere $M_2(F)$ com a $\mathbb{Z}_2$-graduação natural. Nestas codições, $M_2(F)$ satisfaz as identidades $\mathbb{Z}_2$-graduadas $[y_1, y_2] = 0$ e $z_1z_2z_3 - z_3z_2z_1 = 0$, com $y_i \in F\langle X\rangle^{(0)}$ e $z_i \in F\langle X\rangle^{(1)}$.*

Di Vincenzo [10] mostrou que sobre corpos de característica zero estas identidades formam uma base de identidades $\mathbb{Z}_2$-graduadas para $M_2(F)$. O mesmo resultado vale para corpos infinitos em característica diferente de 2 (ver [30]). Em 2002, S. K. Sehgal e M. V. Zaicev [47] provaram o seguinte resultado o qual fornece uma relação entre identidades polinomiais e identidades polinomiais graduadas no caso de álgebras de grupo.

Teorema 1.16. *Seja H um subgrupo normal de G de índice finito. Considere a G/H-graduação natural $FG = \oplus_{t\in G/H} B^{(t)}$. Se FG satisfaz uma identidade graduada, então FG satisfaz uma identidade polinomial.*

Definição 1.17. *Seja A uma álgebra, $\phi\colon G \to Aut(A)$ um homomorfismo de grupos, sendo $Aut(A)$ o grupo formado pelos automorfismos de A. Considere a ação $g(a) = \phi(g)(a)$, para cada $a \in A$ e $g \in G$. Dizemos então que A é uma álgebra com ação do grupo G ou que A é uma G-álgebra. Se a ação ϕ é injetiva, dizemos que a ação é fiel.*

Exemplo 1.18. *Seja $\sigma \in S_n$ uma permutação e $\sigma\colon X \to F\langle X\rangle$ a função dada por $\sigma(x_i) = x_{\sigma(i)}$ se $1 \leqslant i \leqslant n$ e $\sigma(x_k) = x_k$, $k > n$. Como $F\langle X\rangle$ é a álgebra livre, livremente gerada por X, podemos estender σ a um homomorfismo $\alpha_\sigma\colon F\langle X\rangle \to F\langle X\rangle$. Assim, S_n age em um polinômio f permutando as n primeiras variáveis e fixando as demais, ou seja, $\sigma \cdot f := \alpha_\sigma(f) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}, x_{n+1}, \ldots, x_k)$. Estendendo por linearidade esta ação à álgebra de grupo FS_n, tornamos o espaço vetorial P_n, formado pelos polinômios multilineares de grau n em $x_1, \ldots, x_n$, em um FS_n-módulo. Além disso, para cada σ, $\gamma \in S_n$ tem-se $\alpha_{\sigma\gamma} = \alpha_\sigma\alpha_\gamma$ e $\alpha_e = id$. Este módulo desempenha um papel muito importante no estudo de identidades polinomiais. Note que a função $\phi\colon S_n \to Aut(F\langle X\rangle)$ dada por $\phi(\sigma) = \alpha_\sigma$ é um homomorfismo de grupos e, portanto, $F\langle X\rangle$ é uma S_n-álgebra.*

Às vezes usamos a notação $g(a)$ ou, preferencialmente, a notação exponencial a^g para denotar a ação de $g \in G$ em $a \in A$.

Definição 1.19. *Sejam A e B duas G-álgebras. Dizemos que um homomorfismo de álgebras $h\colon A \to B$ é um homomorfismo de G-álgebras se este comuta com a ação de G, ou seja, $h(a^g) = h(a)^g$, para cada $a \in A$.*

Sejam G um grupo, X um conjunto de variáveis (não comutativas) e $F\langle X; G\rangle$ a F-álgebra associativa livre, livremente gerada por $X \times G = \{x^g = (x, g) \mid x \in X,\ g \in G\}$. O grupo G age naturalmente no conjunto $X \times G$. Para cada g, $h \in G$, defina $(x^g)^h = x^{hg}$ e $x^1 = x$. Agora se M e N são monômios em $X \times G$, defina $(MN)^g = M^g N^g$. Por fim, estendendo esta ação por linearidade, tornamos $F\langle X; G\rangle$ uma G-álgebra. Note que se $\alpha\colon X \to A$ é qualquer função de X em uma G-álgebra A, então existe um único homomorfismo de G-álgebras associativas $\widetilde{\alpha} : F\langle X; G\rangle \to A$ que estende α.

Definição 1.20. *$F\langle X; G\rangle$ é chamada de G-álgebra livre livremente gerada por X e seus elementos são chamados de G-polinômios.*

É comum escrevermos os G-polinômios $f(x_1^{g_1}, \ldots, x_n^{g_n})$. Porém, devemos notar que podem ocorrer variáveis repetidas.

Definição 1.21. *Seja A uma G-álgebra. Dizemos que A satisfaz uma G-identidade polinomial se existe um G-polinômio não nulo $f = f(x_1^{g_1}, \ldots, x_n^{g_n}) \in F\langle X; G\rangle$ tal que $f(a_1^{g_1}, \ldots, a_n^{g_n}) = 0$, para quaisquer $a_1, \ldots, a_n \in A$. Neste caso dizemos que f (ou $f = 0$) é uma G-identidade para A e que A é uma G-PI-álgebra.*

Como no caso de álgebras associativas, podemos definir o ideal de G-identidades, base de G-identidades etc. O ideal de G-identidades de A é chamado de G-ideal (ou G-T-ideal) e será denotado por $Id^G(A)$. Observe que se ϕ é uma ação de G em A e $H = Ker\phi$, então $\overline{G} = G/H$ age em A com $a^{gH} = a^g$, a função $\gamma\colon F\langle X; G\rangle \to F\langle X; \overline{G}\rangle$ dada por $\gamma(x^g) = x^{gH}$ é um bem definido epimorfismo de G-álgebras e $Id^G(A) = \gamma^{-1}(Id^{\overline{G}}(A))$.

Desta forma podemos sempre considerar, sem perda de generalidade, que a ação é fiel. É claro que se A satisfaz identidade polinomial, então satisfaz G-identidade polinomial, pois $f(x_1, \ldots, x_n)$ é uma identidade polinomial se, e somente se, $f(x_1^1, \ldots, x_n^1)$ é uma G-identidade. Por outro lado, não é verdade que G-PI implica em PI. Para ver isto, considere N uma álgebra tal que $N^2 = (0)$ e $A = N \oplus F\langle X\rangle$ a soma direta de N com a álgebra livre (não comutativa) livremente gerada por $X = \{x_1, x_2, \ldots\}$. Considere a seguinte função $\phi\colon A \to A$ dada por $\phi(a + b) = a - b$, com $a \in N$ e $b \in F\langle X\rangle$. Então ϕ é um automorfismo de ordem 2, logo $\mathbb{Z}_2 = \{I, \phi\} \subseteq Aut(A)$ age em A. Note que A satisfaz a $\mathbb{Z}_2$-identidade $f(x) = (x + x^{\phi})^2$, mas não é PI, pois possui uma subálgebra livre. Agora observe que, embora não tenhamos identidade polinomial, temos ainda identidade $\mathbb{Z}_2$-graduada. De fato, $A = A_0 \oplus A_1$, com $A_0 = F\langle X\rangle$ e $A_1 = N$, é uma $\mathbb{Z}_2$-graduação e $f(y) = y^{(1)}y^{(1)}$ é uma identidade graduada para A. Isto não é uma coincidência, na verdade veremos em breve que no caso de grupos abelianos finitos uma álgebra possui identidade graduada se, e somente se, possui identidade com ação. Acontece que estudar as identidades de álgebras com ação de grupo equivale a estudar as identidades polinomiais de álgebras graduadas e vice-versa. Isso será formalizado na chamada dualidade entre G-ação e G-graduação, a qual veremos na seção seguinte. Recorde que uma F-álgebra A é dita semissimples (à esquerda) se A visto como A-módulo à esquerda é semissimples.

Teorema 1.22 (Wedderburn-Artin)**.** *Seja A um anel semissimples à esquerda. Então $A = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ para adequados anéis de divisão $D_1, \ldots, D_k$ e inteiros positivos $n_1, \ldots, n_k$. Essa decomposição é única (a menos de uma reordenação) e existem exatamente k A-módulos à esquerda simples mutuamente não isomorfos.*

Teorema 1.23. *Seja A um anel semissimples e I um ideal à esquerda de A. Então, existe um idempotente $e \in A$ tal que $I = Re$. Além disso, se I é um ideal bilateral podemos tomar $e \in Z(A)$.*

Recordemos que um idempotente é dito minimal (resp. central) se gera um ideal minimal unilateral (resp. bilateral). Seja A uma F-álgebra e M um A-módulo. Dada qualquer extensão K de F, podemos estender os escalares de A e M de modo a obtermos uma K-álgebra $A^K = A \otimes_F K$ e um A^K-módulo $M^K = M \otimes_F K$ com ação $(a \otimes f_1)(m \otimes f_2) = am \otimes f_1 f_2$. O próximo resultado pode ser encontrado em [36].

Teorema 1.24. *Seja A uma F-álgebra (de qualquer dimensão) e sejam M um A-módulo irredutível com $\dim_F M < \infty$. As seguintes afirmações são equivalentes:*

a) $End(_A M) = F$;

b) A representação $\rho : A \to End(M_F)$ expressando a ação de A sobre M é sobrejetiva;

c) Para qualquer extensão $K \supseteq F$, M^K é um A^K-módulo simples;

d) Existe um corpo algebricamente fechado $K \supseteq F$ tal que M^K é um A^K-módulo irredutível.

Definição 1.25. *Se algum item (e portanto todos) do teorema anterior vale, então dizemos que M é absolutamente simples (ou absolutamente irredutível).*

Definição 1.26. *Seja A uma F-álgebra de dimensão finita. Dizemos que um corpo $K \supseteq F$ é um corpo de decomposição para A se qualquer A^K-módulo à esquerda irredutível é absolutamente irredutível.*

O próximo resultado fornece um outro modo de sabermos se um corpo é um corpo de decomposição de uma álgebra. No que segue $J(A^K)$ denota o radical de Jacobson de A^K.

Teorema 1.27. *Um corpo $K \supseteq F$ é um corpo de decomposição para A se, e somente se, $A^K/J(A^K)$ é um produto direto finito de álgebras matriciais sobre K.*

Definição 1.28. *Seja V um espaço vetorial sobre um corpo F e $GL(V)$ o conjunto formado por todos os automorfismos de V. Uma representação de um grupo G é um homomorfismo de grupos $\rho\colon G \to GL(V)$. Neste caso dizemos também que V é uma representação de G e que $\dim V$ é o grau ou a dimensão da representação.*

Aqui todas as representações serão de dimensão finita. Lembramos que se $\rho\colon G \to GL(V)$ é uma representação, então V tem estrutura de FG-módulo se definirmos $gv = \rho(g)(v)$, para cada $g \in G$ e $v \in V$ e estendermos a ação por linearidade a FG. Reciprocamente, se V é um FG-módulo, obtemos uma representação $\rho\colon G \to GL(V)$ se definirmos $\rho(g)(v) = gv$, para cada $g \in G$ e $v \in V$.

Definição 1.29. *Duas representações $\rho_1\colon G \to GL(V_1)$ e $\rho_2\colon G \to GL(V_2)$, do mesmo grupo G, são ditas equivalentes se V_1 e V_2 são FG-módulos isomorfos.*

Observe que ρ_1 e ρ_2 são equivalentes se, e somente se, existe um isomorfismo de espaços vetoriais $f\colon V_1 \to V_2$ tal que $f \circ \rho_1 = \rho_2 \circ f$.

Definição 1.30. *Uma representação $\rho\colon G \to GL(V)$ é irredutível se V é um FG-módulo irredutível. Dizemos que ρ (ou V) é completamente redutível se V é uma soma direta de seus submódulos irredutíveis.*

Teorema 1.31 (Maschke)**.** *Seja G um grupo finito e $\operatorname{char} F = p \geqslant 0$. Então FG é semissimples se, e somente se, $p = 0$ ou $p > 0$ e $p \nmid |G|$.*

Como consequência do Teorema de Wedderburn-Artin, obtém-se o seguinte corolário.

Corolário 1.32. *Seja G um grupo finito e $charF = p \geqslant 0$. Se $p = 0$ ou $p > 0$ e $p \nmid |G|$, então*

$$FG \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k),$$

sendo $D_1, \ldots, D_k$ F-álgebras de divisão de dimensão finita.

Definição 1.33. *Seja $\rho\colon G \to GL(V)$ uma representação de G. Então a função $\chi_\rho\colon G \to F$ dada por $\chi_\rho(g) = tr(\rho(g))$ é chamada de caráter da representação e a dimensão de V é chamada de grau do caráter χ_ρ.*

Embora neste trabalho estejamos interessados no corpo dos números complexos, poderíamos considerar corpos mais gerais. A parte importante aqui é que a álgebra de grupo FG decomponha-se em soma direta finita de álgebras matriciais sobre F.

Exemplo 1.34. *Seja $G = \langle g \rangle$ um grupo cíclico finito e F um corpo com $charF = p \geqslant 0$. Se $p \nmid |G|$ e existe raíz $|G|$-primitiva da unidade em F, então F é um corpo de decomposição para G e*

$$FG \cong \overbrace{F \oplus \cdots \oplus F}^{|G| \ parcelas}.$$

Para ver isso, considere o epimorfismo $\phi\colon F[x] \to FG$ dado por $x \mapsto g$. Então $FG \cong F[x]/(x^{|G|} - 1)$ e como o polinômio $x^{|G|} - 1$ possui $|G|$-raízes distintas segue que

$$FG \cong F[x]/(x^{|G|} - 1) \cong \overbrace{F \oplus \cdots \oplus F}^{|G| \ parcelas}.$$

Recordemos que se G_1 e G_2 são grupos, então a álgebra do grupo $G_1 \times G_2$ é isomorfa à álgebra $FG_1 \otimes FG_2$. Agora, se G é um grupo abeliano finito e F é como anteriormente, então pelo Teorema Fundamental dos Grupos Abelianos finitos, podemos escrever $G = C_1 \times \cdots \times C_k$, sendo cada C_i um subgrupo cíclico finito de ordem ϵ_i. Assim, $|G| = \epsilon_1 \cdots \epsilon_k$ e, pelo que vimos no exemplo anterior, FC_i é uma soma direita de ϵ_i cópias de F. Logo,

$$FG \cong (\overbrace{F \oplus \cdots \oplus F}^{\epsilon_1}) \otimes \cdots \otimes (\overbrace{F \oplus \cdots \oplus F}^{\epsilon_k}) \cong \overbrace{F \oplus \cdots \oplus F}^{|G| \text{ parcelas}},$$

ou seja, F é um corpo de decomposição para FG. Os seguintes resultados podem ser encontrados em [36].

Teorema 1.35. *Seja G um grupo finito e F um corpo. Se $V_1, \ldots, V_k$ é uma lista completa de representações irredutíveis não equivalentes e $D_i = End_{FG}(V_i)$ com $n_i = dim_{D_i} V_i$. Então:*

a) $FG/J(FG) \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$;

b) Como FG-módulo à esquerda $FG/J(FG) \cong n_1V_1 \oplus \cdots \oplus n_kV_k$;

c) $dim_F V_i = n_i \dim_F D_i$;

d) $|G| = \dim_F J(FG) + \sum_{i=1}^{k} n_i^2 \dim_F D_i$.

No caso particular em que F é um corpo algebricamente fechado e $char F \nmid |G|$, temos $F \cong D_i$ e, portanto, $FG \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$, com $n_i = \dim_F V_i$ tal que $|G| = \sum_{i=1}^{k} n_i^2$. Esta é a decomposição da álgebra de grupo FG prevista pelo Teorema de Wedderburn-Artin. Na verdade, podemos até refinar um pouco mais essa decomposição se observarmos que o elemento $e = |G|^{-1} \sum_{g \in G} g$ é um idempotente central e que $eFG = FGe \cong F$ é um ideal bilateral minimal (por dimensão). Logo, F aparece na decomposição de FG, ou seja, G possui representação de grau 1. Sejam $e_1, \ldots, e_k$ os idempotentes centrais dados pela decomposição de Wedderburn de FG, G finito e F um corpo de decomposição tal que $char F \nmid |G|$. Para cada $g \in G$, denote por C_g a soma de todos os elementos da classe de conjugação de g e χ_i o caráter irredutível correspondente a V_i.

Teorema 1.36.

a) $e_i = \dfrac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$;

b) $C_g = m_g \sum_i \chi_i(g)e_i/n_i$, *sendo m_g a cardinalidade da classe de conjugação de g.*

Teorema 1.37 (Primeira e Segunda Relação de Ortogonalidade)**.**

a) $\sum_g \chi_i(g^{-1})\chi_j(g) = \delta_{i,j}|G|$, *sendo $\delta_{i,j}$ o delta de Kronecker;*

b) $\sum_i \chi_i(g)\chi_i(h^{-1}) = \delta|C_G(g)|$, *com $\delta = 1$ se g e h são conjugados e $\delta = 0$ caso contrário, sendo $C_G(g)$ o centralizador de g em G.*

De agora em diante, G será sempre um grupo finito e $F = \mathbb{C}$. Seja $C(G)$ o espaço vetorial formado por todas as funções classe $f\colon G \mapsto \mathbb{C}$, ou seja, funções constantes em cada classe de conjugação, e considere o produto interno $(,)$ em $C(G)$ dado por $(\chi, \psi) = 1/|G| \sum_{g \in G} \chi(g)\psi(g^{-1})$. É claro que cada caráter de G é uma função classe. Observe que o Teorema 1.37 nos diz que os caracteres irredutíveis são ortonormais com respeito a $(,)$. Na verdade é possível mostrar que os caracteres irredutíveis formam uma base ortonormal para o espaço das funções classe. Para mais detalhes ver [48] ou [36]. Estendendo cada caráter χ por linearidade podemos supor que χ é uma transformação linear $\chi\colon \mathbb{C}G \to \mathbb{C}$. O seguinte resultado [20] é bem conhecido e será importante mais tarde na demonstração da dualidade entre ação e graduação.

Observação 1.38. *Suponha que G seja um grupo abeliano finito. Então:*

- $\chi_i(e_j) = \delta_{i,j}$;
- $ge_i = \chi_i(g)e_i$.

Demonstração. Como G é abeliano as representações irredutíveis são todas de grau 1. Logo, para cada caráter χ e g, $h \in G$ temos $\chi(gh) = \chi(g)\chi(h)$. Assim

$$\chi_i(e_j) = \chi_i(\frac{1}{|G|}\sum_{g\in G}\chi_j(g^{-1}g)) = \frac{1}{|G|}\sum_{g\in G}\chi_j(g^{-1})\chi_i(g) = \delta_{i,j}$$

e

$$\begin{aligned} ge_i &= \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})hg = \frac{1}{|G|}\sum_{s\in G}\chi_i(s^{-1}g)s = \frac{1}{|G|}\sum_{s\in G}\chi_i(s^{-1})\chi_i(g)s \\ &= \chi_i(g)\frac{1}{|G|}\sum_{s\in G}\chi_i(s^{-1})s = \chi_i(g)e_i. \end{aligned}$$

□

1.2 Dualidade entre ação por grupo finito abeliano e graduação

Como dito na seção anterior, G será um grupo abeliano finito de ordem n e $F = \mathbb{C}$. Mas, nesta seção poderíamos considerar qualquer corpo de decomposição para G, por exemplo, poderíamos considerar qualquer corpo de característica zero contendo raíz n-ésima primitiva da unidade. Seja $\widehat{G}$ o conjunto formado por todos os caracteres irredutíveis de G. Como G é abeliano finito, $\widehat{G}$ coincide com o conjunto de todos os homomorfismos $\chi\colon G \to \mathbb{C}^*$. Dados χ_1, $\chi_2 \in \widehat{G}$, defina $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. Então $\chi_1\chi_2 \in \widehat{G}$ e, com essa operação, $\widehat{G}$ tem estrutura de grupo. Este é o grupo dual de G. O seguinte resultado pode ser visto em [33], pag. 439.

Teorema 1.39. *Seja G um grupo abeliano finito e $\widehat{G}$ o seu grupo dual. Então $\widehat{G} \cong G$.*

Seja A uma G-álgebra, $\widehat{G} = \{\chi_1, \ldots, \chi_n\}$ e $e_1, \ldots, e_n$ os idempotentes centrais de $\mathbb{C}G$. Considere agora os subespaços $A^{(\chi_i)} = \{a \in A \mid a^g = \chi_i(g)a, g \in G\}$. Como $1 = e_1 + \cdots + e_n$, podemos escrever, para cada $a \in A$, $a = a^{e_1} + \cdots + a^{e_n}$ e, portanto, $a^g = a^{ge_1} + \cdots + a^{ge_n} = \chi_1(g)a^{e_1} + \cdots + \chi_n(g)a^{e_n}$. Agora, se $a \in A^{(\chi_i)}$, então $a^g = \chi_i(g)a$, para cada $g \in G$, e $a^{ge_j} = \chi_i(g)a^{e_j}$. Por outro lado, como os idempotentes e_i's são dois a dois ortogonais temos $a^{ge_j} = \chi_j(g)a^{e_j}$ e assim $(\chi_i(g) - \chi_j(g))a^{e_j} = 0$, para cada $g \in G$. Com isso obtemos $a^{e_i} = a$ e $a^{e_j} = 0$, se $j \neq i$. Reciprocamente, se $a^{e_i} = a$, então para cada $g \in G$, tem-se $(a^{e_i})^g = a^{ge_i} = \chi_i(g)a^{e_i}$, ou seja, $a^{e_i} \in A^{(\chi_i)}$. Isso mostra que $A^{(\chi_i)} = \{a \in A \mid a^{e_i} = a\}$. Como $a^g = \chi_1(g)a^{e_1} + \cdots + \chi_n(g)a^{e_n}$, temos também que

$$A = \bigoplus_{\chi\in\widehat{G}} A^{(\chi)}.$$

A decomposição acima fornece para A uma estrutura de álgebra $\widehat{G}$-graduada. Para ver isso, considere dois elementos $a \in A^{(\chi_i)}$ e $b \in A^{(\chi_j)}$. Então, para cada $g \in G$, $(ab)^g = a^g b^g = \chi_i(g)\chi_j(g)(ab) = (\chi_i\chi_j)(g)(ab)$, isso mostra que $A^{(\chi_i)}A^{(\chi_j)} \subseteq A^{(\chi_i\chi_j)}$. Mais tarde precisaremos lidar com subálgebras de Lie $L \subseteq A^{(-)}$ invariantes pela ação de G. Neste caso é importante notar que a demonstração acima continua válida se considerarmos L no lugar de A, ou seja, L herda a $\widehat{G}$-graduação de A.

Exemplo 1.40. *Seja $G = \{1, g\} \cong \mathbb{Z}_2$. Então existem dois caracteres χ_1 e χ_2 que são dados por $\chi_1(1) = \chi_1(g) = \chi_2(1) = 1$ e $\chi_2(g) = -1$. Assim, $A^{(\chi_1)} = \{a \in A \mid a^g = a\}$, $A^{(\chi_2)} = \{a \in A \mid a^g = -a\}$ e $A = A^{(\chi_1)} \bigoplus A^{(\chi_2)}$ é uma $\widehat{G}$-graduação.*

Como $G \cong \widehat{G}$, o que vimos acima é que para cada G-ação obtém-se uma G-graduação. Agora, suponha que $A = \oplus_{g\in G} A^{(g)}$ seja uma G-graduação. Dado um caráter $\chi \in \widehat{G}$, defina $\chi \colon A \to A \in Aut(A)$ da seguinte forma:

$$\chi(a) = \sum \chi(g)a_g,$$

com $a_g \in A^{(g)}$ para cada $g \in G$. A linearidade é imediata. Dados $a = \sum a_g$ e $b = \sum b_g$, com a_g, $b_g \in A_g$, temos

$$ab = \sum_{g,h} a_g b_h = \sum_h \sum_g (a_g b_{g^{-1}h}).$$

Logo, $\chi(ab) = \sum_h \sum_g \chi(h)(a_g b_{g^{-1}h})$. Por outro lado,

$$\chi(a)\chi(b) = (\sum_g \chi(g)a_g)(\sum_h \chi(h)b_h) = \sum_{g,h} \chi(gh)a_g b_h = \sum_h \sum_g \chi(h)a_g b_{g^{-1}h} = \chi(ab).$$

Por fim, se $\psi = \chi^{-1} \in \widehat{G}$, então para cada $a = \sum_{g\in G} a_g$, $a_g \in A^{(g)}$, temos $(\psi\chi)(a) = \sum(\psi\chi)(g)a_g = a$. Com isso, mostramos que uma G-graduação fornece uma $\widehat{G}$-ação. Note que, se $L \subseteq A^{(-)}$ é uma subálgebra de Lie que herda a G-graduação de A, então L é invariante pela ação de $\widehat{G}$.

Exemplo 1.41. *Seja $G = \mathbb{Z}_n = \langle g \rangle$ e $A = \oplus A^{(g)}$ uma álgebra G-graduada. Então $\widehat{G} = \{\chi_0, \ldots, \chi_{n-1}\}$, com $\chi_i(g^j) = \omega^{ij}$ e ω uma raiz n-ésima primitiva da unidade. Com isso, cada caráter χ_i determina um automorfismo de A dado por $\chi_i(a) = \sum \omega^{ij} a_{g^j}$, com $a = \sum a_{g^j}$.*

Teorema 1.42. *Seja A uma $\mathbb{C}$-álgebra e G um grupo abeliano finito. Qualquer G-graduação em A define uma $\widehat{G}$-ação e vice-versa. Nesta ação, um subespaço $V \subseteq A$ é G-graduado se, e somente se, este é invariante pela $\widehat{G}$-ação. Um elemento $a \in A$ é homogêneo na G-graduação se, e somente se, é um autovetor para cada $\chi \in \widehat{G}$.*

Demonstração. A dualidade já foi provada acima. Suponha que $V = \oplus V^{(g)}$ é um subespaço G-graduado de A. Com a ação anterior de $\widehat{G}$, temos $\chi(V^{(g)}) = V^{(g)}$, para cada $\chi \in \widehat{G}$ e

$g \in G$, logo $\chi(V) = V$. Agora suponha que $\chi(V) \subseteq V$. Se V não é um espaço G-graduado, então existem $g_1, \ldots, g_t \in G$ distintos e $v = v_{g_1} + \cdots + v_{g_t} \in V$ tal que $v_{g_i} \notin V$, para cada $i \in \{1, \ldots, t\}$. Escolha v de modo que t seja o menor possível. Escolha $\chi \in \widehat{G}$ de modo que $\chi(g_1) = \lambda$ e $\chi(g_2) = \mu$, com $\lambda \neq \mu$ (tal elemento existe devido às relações de ortogonalidade). Agora basta observar que o elemento $u = \lambda v - \chi(v) = (\lambda - \mu)v_{g_2} + \cdots + (\lambda - \chi(g_t))v_{g_t}$ pertence a V, mas isto contraria a minimalidade de t. Por fim, um elemento $a \in A$ é homogêneo se, e somente se, o subespaço V gerado por a é graduado, mas isto por sua vez equivale a dizer que V é invariante por $\widehat{G}$-ação e isto ocorre exatamente quando a é um autovetor para cada $\chi \in \widehat{G}$. □

Exemplo 1.43. *Seja g o automorfismo de $M_2(\mathbb{C})$ dado por $g(x) = BxB^{-1}$, com $B = e_{11} - e_{22}$. Então $G = \{1, g\} \cong \mathbb{Z}_2$ age em $M_2(\mathbb{C})$ e esta ação induz a $\mathbb{Z}_2$-graduação $M_2(\mathbb{C}) = M_2^{(\chi_1)} \oplus M_2^{(\chi_2)}$, com $M_2^{(\chi_1)} = \{a \in M_2(\mathbb{C}) \mid g(a) = a\}$ e $M_2^{(\chi_2)} = \{a \in M_2(\mathbb{C}) \mid g(a) = -a\}$. Note que, se $a = pe_{11} + qe_{12} + re_{21} + se_{22}$, então $g(a) = a$ ocorre apenas quando $q = r = 0$. Por outro lado, $g(a) = -a$ equivale a $p = s = 0$, ou seja, a $\widehat{G}$-graduação obtida é a $\mathbb{Z}_2$-graduação natural.*

Consideremos novamente um subgrupo abeliano finito $G \subseteq Aut(A)$. Por definição, sabemos que G age como grupo de automorfismos para a G-álgebra livre $\mathbb{C}\langle X; G\rangle$ e, portanto, $\mathbb{C}\langle X; G\rangle = \oplus_{\chi \in \widehat{G}} \mathbb{C}\langle X; G\rangle^{(\chi)}$ é uma $\widehat{G}$-graduação. Com esta graduação, a G-álgebra livre tem a seguinte importante propriedade.

Lema 1.44. *Sejam A uma álgebra, $G \subseteq Aut(A)$ um grupo abeliano finito e $\phi\colon \mathbb{C}\langle X; G\rangle \to A$ um homomorfismo. São equivalentes:*

a) ϕ é um homomorfismo de G-álgebras;

b) ϕ é um homomorfismo de álgebras $\widehat{G}$-graduadas.

Demonstração. Sejam $A = \oplus_{i=1}^{n} A^{(\chi_i)}$, $f = f^{e_i} \in \mathbb{C}\langle X; G\rangle^{(\chi_i)}$ e $\phi(f) = a$. Suponha que ϕ comuta com ação de G. Então, para cada $g \in G$, tem-se $\phi(f^g) = \phi(f)^g = a^g$ e como e_i é uma combinação linear dos elementos de G, segue que $a = \phi(f) = \phi(f^{e_i}) = a^{e_i} \in A^{(\chi_i)}$, ou seja, $\phi(\mathbb{C}\langle X; G\rangle^{(\chi_i)}) \subseteq A^{(\chi_i)}$. Isso mostra que ϕ é um homomorfismo de álgebras $\widehat{G}$-graduadas. Agora suponha que ϕ preserva $\widehat{G}$-graduação. Sejam $x \in X$ e $\phi(x) = b$, com $b = b_1 + \cdots + b_n$ e $b_i \in A^{(\chi_i)}$. É suficiente provar que $\phi(x^g) = b^g$ para cada $g \in G$. Recordemos que se $a \in A^{(\chi_i)}$, então $a^{e_i} = a$ e $a^{e_j} = 0$ se $i \neq j$. Logo, $b^{e_i} = b_1^{e_i} + \cdots + b_n^{e_i} = b_i$. Além disso, $\phi(x) = \phi(x^{e_1 + \cdots + e_n}) = \phi(x^{e_1}) + \cdots + \phi(x^{e_n})$ e, por hipótese, $\phi(x^{e_i}) \in A^{(\chi_i)}$. Logo $\phi(x^{e_i}) = b^{e_i}$, $i \geqslant 1$. Para cada $g \in G$, podemos escrever $x^g = x^{g(e_1 + \cdots + e_n)} = \sum \chi_i(g) x^{e_i}$. Assim $\phi(x^g) = \sum \chi_i(g)\phi(x^{e_i}) = \sum \chi_i(g) b^{e_i} = b^{g(e_1 + \cdots + b_n)} = b^g$, ou seja, $\phi(x^g) = b^g$. □

Neste momento, estamos em condições de provar o principal resultado deste capítulo.

Proposição 1.45. *Seja $G \subseteq Aut(A)$ um grupo abeliano finito e considere a graduação $\mathbb{C}\langle X; G\rangle = \oplus_{\chi\in\widehat{G}}\mathbb{C}\langle X; G\rangle^{(\chi)}$. Então $\mathbb{C}\langle X; G\rangle$ é a álgebra livre $\widehat{G}$-graduada de posto enumerável e $id^G(A) = id^{gr}(A)$.*

Demonstração. Observe que $\widetilde{X} = \{x^{e_i} \mid x \in X, i = 1, \ldots, n\}$ gera a álgebra $\mathbb{C}\langle X; G\rangle$. Mostraremos que $\widetilde{X}$ é um conjunto de geradores graduados da $\widehat{G}$-álgebra graduada $\mathbb{C}\langle X; G\rangle$. Seja $B = \oplus B^{(\chi_i)}$ uma álgebra $\widehat{G}$-graduada e $\phi\colon \widetilde{X} \to B$ qualquer função com $\phi(x_j^{e_i}) = b_{ij} \in B^{(\chi_i)}$, para cada $x_j \in X$ e $i \in \{1, \ldots, n\}$. Pelo Teorema 1.42, sabemos que G (canonicamente isomorfo ao bidual) age em B. Como $\mathbb{C}\langle X; G\rangle$ é a álgebra livre com ação de G, existe um homomorfismo de G-álgebras $\widetilde{\phi}\colon \mathbb{C}\langle X; G\rangle \to B$ tal que $\widetilde{\phi}(x_j) = b_{1j} + \cdots + b_{nj}$. Como $\widetilde{\phi}(x_j^{e_i}) = \widetilde{\phi}(x_j)^{e_i}$ e $(b_{1j} + \cdots + b_{nj})^{e_i} = b_{ij}$, temos $\widetilde{\phi}(x_j^{e_i}) = b_{ij} = \phi(x_j^{e_i})$, ou seja, $\widetilde{\phi}$ é um homomorfismo de G-álgebras estendendo ϕ e este é um homomorfismo $\widehat{G}$-graduado segundo o Lema 1.44, ou seja, $\mathbb{C}\langle X; G\rangle$ é uma álgebra livre $\widehat{G}$-graduada. Agora, considere um G-polinômio $f = f(x_1^{g_1}, \ldots, x_k^{g_k}) \in Id^G(A)$ e escreva $x_i^{g_j} = \sum_s \chi_s(g_j)x_i^{e_s}$. Assim, f pode ser reescrito como um polinômio nas indeterminadas graduadas $x_i^{e_j}$

$$f(x_1^{g_1}, \ldots, x_k^{g_k}) = h(x_1^{e_1}, \ldots, x_1^{e_n}, \ldots, x_k^{e_1}, \ldots, x_k^{e_n}).$$

Sejam $c_1^1, \ldots, c_1^n, \ldots, c_k^1, \ldots, c_k^n$ elementos arbitrários em A, $c_i^j \in A^{(\chi_j)}$ e

$$a_i = (\sum_s \chi_s(g_j)c_i^s)^{g_j^{-1}}.$$

Então, $a_i^{g_j} = \sum_s \chi_s(g_j)c_i^s$ e, portanto, $a_i^{e_s} = c_i^s$ para cada i, $s \geqslant 1$. Como f é uma identidade para A,

$$0 = f(a_1^{g_1}, \ldots, a_k^{g_k}) = h(a_1^{e_1}, \ldots, a_1^{e_n}, \ldots, a_k^{e_1}, \ldots, a_k^{e_n}) = h(c_1^1, \ldots, c_1^n, \ldots, c_k^1, \ldots, c_k^n).$$

Assim, $f(x_1^{g_1}, \ldots, x_k^{g_k}) = h(x_1^{e_1}, \ldots, x_1^{e_n}, \ldots, x_k^{e_1}, \ldots, x_k^{e_n}) \in Id^{gr}(A)$. Suponha que

$$f(x_1^{e_1}, \ldots, x_1^{e_n}, \ldots, x_k^{e_1}, \ldots, x_k^{e_n}) \in Id^{gr}(A).$$

Escreva $e_j = \sum \alpha_{sj}g_s$. Assim, $x_i^{e_j} = \sum \alpha_{sj}x_i^{g_s}$ e então podemos reescrever f como um G-polinômio nas indeterminadas $x_i^{g_j}$

$$f(x_1^{e_1}, \ldots, x_1^{e_n}, \ldots, x_k^{e_1}, \ldots, x_k^{e_n}) = h(x_1^{g_1}, \ldots, x_1^{g_n}, \ldots, x_k^{g_1}, \ldots, x_k^{g_n}).$$

Como para cada $a_1, \ldots, a_k \in A$, tem-se $a_i^{e_j} = \sum \alpha_{sj}a_i^{g_s} \in A^{(\chi_i)}$ e $f \in Id^{gr}(A)$, segue que

$$0 = f(a_1^{e_1}, \ldots, a_1^{e_n}, \ldots, a_k^{e_1}, \ldots, a_k^{e_n}) = h(a_1^{g_1}, \ldots, a_1^{g_n}, \ldots, a_k^{g_1}, \ldots, a_k^{g_n}).$$

Logo, $f(x_1^{e_1}, \ldots, x_1^{e_n}, \ldots, x_k^{e_1}, \ldots, x_k^{e_n}) = h(x_1^{g_1}, \ldots, x_1^{g_n}, \ldots, x_k^{g_1}, \ldots, x_k^{g_n}) \in Id^G(A)$. $\square$

Antes de encerrarmos este capítulo, note que um subconjunto $S \subseteq \mathbb{C}\langle X; G\rangle$ gera $Id^G(A)$ como um G-ideal se, e somente se, gera $Id^G(A)$ como um ideal $\widehat{G}$-graduado. Por exemplo, digamos que $Id^G(A)$ é gerado por S como um G-ideal. Seja J o ideal de identidades $\widehat{G}$-graduadas gerado por S. Como J é invariante por endomorfismos da álgebra $\widehat{G}$-graduada livre e estes são, pelo Lema 1.44, endomorfismos da G-álgebra livre, então J é um G-ideal contendo S. Mas $Id^G(A)$ é o menor G-ideal que contém S, portanto, $Id^G(A) \subseteq J \subseteq Id^{gr}(A) = Id^G(A)$. A recíproca é provada de modo análogo.

Considere $M_2(\mathbb{C})$ com a ação de $\mathbb{Z}_2 = \{1, g\}$ dada no exemplo 1.43 e também com a $\mathbb{Z}_2$-graduação natural. Em 1992, Di Vincenzo [10] provou que $M_2(\mathbb{C})$ possui uma base $\mathbb{Z}_2$-graduada formada por duas identidades: $[y_1, y_2] = 0$ e $z_1z_2z_3 - z_3z_2z_1 = 0$, com y_i correspondendo às variáveis pares e z_i às variáveis ímpares. Em posse deste resultado, A. Berele [6] obteve a seguinte base para $M_2(\mathbb{C})$ com $\mathbb{Z}_2$-ação. Seja $\pi_0 = 1 + g$ e $\pi_1 = 1 - g$, então os $\mathbb{Z}_2$-polinômios $[\pi_0(x_1), \pi_0(x_2)] = 0$ e $\pi_1(x_1)\pi_1(x_2)\pi_1(x_3) - \pi_1(x_3)\pi_1(x_2)\pi_1(x_1) = 0$ formam uma base para $Id^{\mathbb{Z}_2}(M_2(\mathbb{C}))$. Resultado semelhante foi obtido por P. Koshlukov e A. Mortari [32] para a álgebra de Lie $sl_2(\mathbb{C})$ considerando a $\mathbb{Z}_2$-graduação natural. No capítulo 3, faremos um estudo sobre as chamadas identidades fracas com ação de grupo finito, mas antes disso precisaremos provar um análogo do resultado de Di Vincenzo para o caso das identidades fracas $\mathbb{Z}_2$-graduadas. É o que faremos no capítulo a seguir.

Capítulo 2

Identidades Fracas Graduadas e a Propriedade de Specht

2.1 Identidades fracas $\mathbb{Z}_2$-graduadas

Ao longo do texto A será uma álgebra associativa unitária sobre o domínio de integridade D e G um grupo abeliano. Nesta seção estamos interessados em estudar as identidades fracas $\mathbb{Z}_2$-graduadas do par $(M_2(D), sl_2(D))$ considerando a $\mathbb{Z}_2$-graduação natural. Analogamente ao que ocorre com as classes de álgebras, precisaremos definir antes de tudo um objeto livre na classe dos pares graduados. O principal resultado desta seção é a Proposição 2.19.

Definição 2.1. *Seja (A, L) um par onde A é uma álgebra associativa unitária e L é uma subálgebra de Lie de $A^{(-)}$. Quando L gera A, dizemos que o par é do tipo associativo-Lie e se $Y \subseteq L$ gera L dizemos que Y gera o par.*

Exemplo 2.2. *Se L é uma álgebra de Lie e $U = U(L)$ é sua álgebra universal envolvente, então (U, L) é um par do tipo associativo-Lie.*

Exemplo 2.3. *Se A é uma álgebra associativa unitária, então $(A, A^{(-)})$ é um par associativo-Lie.*

Exemplo 2.4. *Um par associativo-Lie muito importante e que será estudado nesse capítulo é o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

Definição 2.5. *Sejam $A = \oplus_{g\in G} A_g$ uma álgebra associativa G-graduada e $L \subseteq A^{(-)}$ uma álgebra de Lie tal que $L = \oplus_{g\in G} L_g$, com $L_g = A_g \cap L$. Então dizemos que o par (A, L) é G-graduado, ou apenas graduado quando estiver claro a qual grupo nos referimos.*

Definição 2.6. *Um homomorfismo de pares $f\colon (A, L) \to (A', L')$ é um homomorfismo de álgebras associativas $f\colon A \to A'$ tal que $f(L) \subseteq L'$. O homomorfismo f de pares é sobrejetor* *se $f(A) = A'$ e $f(L) = L'$. Dizemos também que f é injetor se for um monomorfismo de álgebras associativas. Por fim, f é um isomorfismo de pares se for injetor e sobrejetor.*

Definição 2.7. *Sejam (A, L) e (A', L') pares G-graduados. Um homomorfismo de pares graduados é um homomorfismo de pares $f\colon (A, L) \to (A', L')$ tal que $f(A_g) \subseteq A'_g, \forall g \in G$.*

De modo análogo ao que foi feito anteriormente, podemos definir isomorfismo de pares graduados.

Definição 2.8. *Seja $\mathcal{C}$ uma classe de pares G-graduados. Dizemos que um par $(A, L) \in \mathcal{C}$ gerado por um conjunto $Y \subseteq \bigcup A_g$ é relativamente livre em Y, com respeito à classe $\mathcal{C}$, se dado qualquer par $(A', L') \in \mathcal{C}$ e qualquer função $\alpha\colon Y \to L'$ tal que $\alpha(Y \cap A_g) \subseteq L'_g$ $(\forall g \in G)$, existe um único homomorfismo de pares G-graduados $\widetilde{\alpha}\colon (A, L) \to (A', L')$ que estende α. A cardinalidade de Y é o posto de (A, L). Caso $\mathcal{C}$ seja classe de todos os pares graduados por G, diremos que (A, L) é um par livre, livremente gerado por Y, na classe dos pares G-graduados.*

Sejam X um conjunto infinito enumerável e G um grupo tais que $X = \bigcup_{g \in G} X_g$ (união disjunta), com $X_g = \{x_1^{(g)}, x_2^{(g)}, \ldots\}$ e $D\langle X\rangle = \oplus_{g \in G} D\langle X\rangle_g$ a D-álgebra G-graduada livre e livremente gerada por X. Então a álgebra de Lie $L\langle X\rangle \subseteq D\langle X\rangle$ gerada por X possui graduação $L\langle X\rangle = \oplus L\langle X\rangle_g$, com $L\langle X\rangle_g = D\langle X\rangle_g \cap L\langle X\rangle$. Como no caso de álgebras associativas, prova-se que o par $(D\langle X\rangle, L\langle X\rangle)$ G-graduado é livre, livremente gerado por X, na classe dos pares G-graduados.

Definição 2.9. *Um ideal $I \subseteq D\langle X\rangle$ é dito um T-ideal fraco G-graduado se é invariante por todo endomorfismo do par G-graduado livre $(D\langle X\rangle, L\langle X\rangle)$.*

Definição 2.10. *Sejam $f = f(x_1^{(g_1)}, \ldots, x_n^{(g_n)}) \in D\langle X\rangle$ e (A, L) um par G-graduado. Dizemos que f é uma identidade fraca graduada do par (A, L) se $f(b_1, \ldots, b_n) = 0, \forall b_i \in L\langle X\rangle_{g_i}$.*

Definição 2.11. *Seja $S \subseteq D\langle X\rangle$ e I a interseção de todos os T-ideais fracos G-graduados que contêm S. Dizemos que o ideal I é o T-ideal fraco graduado gerado por S e que S é uma base para I.*

Note que I coincide com o ideal

$$J = \{\sum u_i f(w_{i1}, \ldots, w_{in}) v_i \mid u_i, v_i \in D\langle X\rangle, f(x_1^{(g_1)}, \ldots, x_n^{(g_n)}) \in S, w_{ij} \in L\langle X\rangle_{g_j}\}.$$

Se (A, L) é um par G-graduado, então o conjunto $Id(A, L)$ de todas as identidades fracas graduadas do par é um T-ideal fraco graduado e homogêneo. Na verdade todo ideal homogêneo I que é invariante por endomorfismos do par G-graduado $(D\langle X\rangle, L\langle X\rangle)$ é obtido dessa forma:

$$I = Id(D\langle X\rangle/I, (L\langle X\rangle + I)/I).$$

Para ver isso note que se $f = f(x_1^{(g_1)}, \ldots, x_n^{(g_n)}) \in D\langle X\rangle$, então dados $e_i^{(g_i)} \in L\langle X\rangle_{g_i}$ tem-se $f(e_1^{(g_1)}, \ldots, e_n^{(g_n)}) + I = f(e_1^{(g_1)} + I, \ldots, e_n^{(g_n)} + I)$, $\forall e_i^{(g_i)} \in L\langle X\rangle_{g_i}$, portanto f é uma identidade do par $(D\langle X\rangle/I, (L\langle X\rangle + I)/I)$ se, e somente se, $f(e_1^{(g_1)}, \ldots, e_n^{(g_n)}) \in I$ para todas as avaliações (graduadas) nos elementos de $L\langle X\rangle$. Mas, todos os endomorfismos do par livre $(D\langle X\rangle, L\langle X\rangle)$ são dados dessa forma e isto prova a afirmação.

Definição 2.12. *Seja $S \subseteq D\langle X\rangle$. A classe de todos os pares G-graduados (A, L) tais que $S \subseteq Id(A, L)$, denotada por $\mathcal{V}(S)$, é chamada de variedade de pares G-graduados determinada por S.*

Podemos provar de modo análogo ao Teorema 1.2.4 de [20] que

Teorema 2.13. *Sejam (A, L) um par G-graduado e $I = Id(A, L)$. O par*

$$(D\langle X\rangle/I, (L\langle X\rangle + I)/I)$$

é um par associativo-Lie G-graduado relativamente livre gerado pelo conjunto $\overline{X}$, onde $\overline{X} = \{x + I \mid x \in X, x \notin I\}$ na variedade determinada por I.

Demonstração. Seja $(A', L') \in \mathcal{V} = \mathcal{V}(I)$ e $\alpha : \overline{X} \to L'$ tal que $\alpha(x^{(g)} + I) \in L'_g \subseteq L'$. Precisamos encontrar um homomorfismo de álgebras associativas estendendo α da forma

$$\widetilde{\alpha} : D\langle X\rangle/I \to A',$$

com $\widetilde{\alpha}((D\langle X\rangle_g + I)/I) \subseteq A'_g, \forall g \in G$ e $\widetilde{\alpha}((L\langle X\rangle + I)/I) \subseteq L'$. Defina $\beta : X \to L'$ por $\beta(x) = \alpha(x + I)$ para $x \notin I$ e $\beta(x) = 0$ caso contrário. Dessa forma existe um homomorfismo $\widetilde{\beta} : D\langle X\rangle \to A'$ de álgebras associativas que estende β (homomorfismo de pares G-graduados). Agora se $f \in I$, então $f \in Id(A', L')$ de onde conclui-se que $f \in Ker\widetilde{\beta}$ e $I \subseteq Ker\widetilde{\beta}$. Defina $\widetilde{\alpha} : D\langle X\rangle/I \to A'$ por $\widetilde{\alpha}(a + I) = \widetilde{\beta}(a)$. Como $I \subseteq Ker\widetilde{\beta}$ segue que $\widetilde{\alpha}$ é um bem definido homomorfismo de álgebras associativas e $\widetilde{\alpha}(x^{(g)} + I) = \widetilde{\beta}(x^{(g)}) = \alpha(x^{(g)} + I)$. Portanto $\widetilde{\alpha}$ estende α e, além disso, satisfaz $\widetilde{\alpha}((D\langle X\rangle_g + I)/I) \subseteq A'_g$ e $\widetilde{\alpha}((L\langle X\rangle + I)/I) \subseteq L'$. □

Seja $A = D[a_i, b_i, c_i \mid i \geqslant 1]$ a D-álgebra associativa comutativa livre livremente gerada por $\{a_i, b_i, c_i \mid i \geqslant 1\}$. Considere a D-álgebra associativa (unitária) $R \subseteq M_2(A)$ e a D-álgebra de Lie $S \subseteq M_2(A)^{(-)}$ ambas geradas por

$$Y_i = \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \quad \text{e} \quad Z_i = \begin{pmatrix} 0 & b_i \\ c_i & 0 \end{pmatrix}, \; i \geqslant 1.$$

Observe que os monômios nas variáveis Y_i e Z_i são sempre matrizes diagonais ou matrizes com diagonal principal nula e, por definição, tais monômios são elementos de R, então podemos escrever $R = R_0 \oplus R_1$, sendo R_0 o D-submódulo de R gerado por matrizes diagonais de R e R_1 o D-submódulo de R gerado por matrizes com diagonal principal nula. Observe também que $R_iR_j \subseteq R_{i+j}, i, j \in \mathbb{Z}_2$ e, portanto, R é uma álgebra $\mathbb{Z}_2$-graduada. Por fim, note que $S = S_0 \oplus S_1$, com $S_i = (R_i \cap S)$ e, assim, (R, S) é um par associativo-Lie $\mathbb{Z}_2$-graduado.

Quando um par (A, L) for $\mathbb{Z}_2$-graduado escreveremos $Id(A, L) = T_2(A, L)$ e diremos que este é um T_2-ideal fraco. Além disso, se S gerar $T_2(A, L)$, diremos que S gera $T_2(A, L)$ como um T_2-ideal fraco.

Considere as álgebras $\mathbb{Z}_2$-graduadas $M_2(D) = M_2^{(0)} \oplus M_2^{(1)}$, sendo $M_2^{(0)}$ o submódulo das matrizes diagonais e $M^{(1)}$ o submódulo das matrizes com diagonal principal nula. A álgebra de Lie $sl_2(D)$ herda essa graduação, ou seja:

$$sl_2(D) = sl_2^{(0)} \oplus sl_2^{(1)},$$

onde $sl_2^{(i)} = M_2^{(i)} \cap sl_2(D)$ e $[sl_2^{(i)}, sl_2^{(j)}] \subseteq sl_2^{(i+j)}$ com $i, j \in \mathbb{Z}_2$.
Os dois resultados a seguir são demonstrados de modo análogo ao Teorema 1.4.4 de [20].

Lema 2.14. *Suponha que D seja um domínio de integridade infinito. Então o par (R, S), definido anteriormente, satisfaz as seguintes propriedades:*

a) $T_2(M_2(D), sl_2(D)) \subseteq T_2(R, S)$*;*

b) Seja $Y = \{Y_i, Z_i | \, i \geqslant 1\}$*. Então dada uma função* $\alpha\colon Y \to sl_2(D)$ *tal que* $\forall i \geqslant 1$, $\alpha(Y_i) \in sl_2^{(0)}$ *e* $\alpha(Z_i) \in sl_2^{(1)}$*, existe um único homomorfismo de pares $\mathbb{Z}_2$-graduados* $\widetilde{\alpha}\colon (R, S) \to (M_2(D), sl_2(D))$ *que estende* α*.*

Demonstração. $a)$ Seja $A = D[a_i, b_i, c_i | \, i \geqslant 1]$. Considere o isomorfismo natural

$$\alpha : M_2(D) \otimes_D A \to M_2(A)$$

dado por $\alpha((a_{ij}) \otimes f) = (a_{ij}f)$. Observe que $\alpha(sl_2(D) \otimes_D A) = sl_2(A)$. Considerando a $\mathbb{Z}_2$- graduação trivial $A = A_0 \oplus A_1$ com $A_1 = 0$, vê-se que α é um isomorfismo entre os pares $\mathbb{Z}_2$-graduados

$$(M_2(D) \otimes_D A, sl_2(D) \otimes_D A) \qquad \text{e} \qquad (M_2(A), sl_2(A)).$$

Além disso, $T_2(M_2(A), sl_2(A)) \subseteq T_2(R, S)$, pois $R \subseteq M_2(A)$ e $S \subseteq sl_2(A)$. Então só precisamos provar que $T_2(M_2(D), sl_2(D)) \subseteq T_2(M_2(A), sl_2(A))$. Mas, de modo análogo ao caso de álgebras associativas de [20, Lema 1.4.2] podemos provar que as identidades fracas $\mathbb{Z}_2$-graduadas são "estáveis", ou seja, invariantes por extensão de escalares. Isso conclui a demonstração.

$b)$ Sejam $Y_i = a_ie_{11} - a_ie_{22}$, $Z_i = b_ie_{12} + c_ie_{21}$, $i \geqslant 1$ e $\alpha\colon Y \to sl_2(D)$. Digamos que $\alpha(Y_i) = p_ie_{11} - p_ie_{22}$ e $\alpha(Z_i) = q_ie_{12} + r_ie_{21}$, para todo $i \geqslant 1$. Seja $\beta\colon A \to D$ o homomorfismo dado por $\beta(a_i) = p_i$, $\beta(b_i) = q_i$ e $\beta(c_i) = r_i$. Estenda a um homomorfismo $\widetilde{\beta}\colon M_2(A) \to M_2(D)$ fazendo $\widetilde{\beta}((a_{ij})) = (\beta(a_{ij}))$. Por fim, seja $\gamma\colon R \to M_2(D)$ a restrição de $\widetilde{\beta}$ a R. Note que $\gamma(S) \subseteq sl_2(D)$ e $\gamma(R_i) \subseteq M_2^i(D)$ e, portanto, γ é um homomorfismo de pares $\mathbb{Z}_2$-graduados que estende α. A unicidade decorre do fato de dois tais homomorfismos coincidirem no conjunto gerador Y. □

Teorema 2.15. *Seja D um domínio de integridade infinito. Então o par (R, S) é o par associativo-Lie $\mathbb{Z}_2$-graduado relativamente livre de posto enumerável na variedade determinada por $T_2(M_2(D), sl_2(D))$.*

Demonstração. Queremos provar que se $I = T_2(M_2(D), sl_2(D))$, então

$$(R, S) \cong (D\langle X\rangle/I, (L\langle X\rangle + I)/I).$$

Seja $\alpha\colon (D\langle X\rangle, L\langle X\rangle) \to (R, S)$ o homomorfismo de pares $\mathbb{Z}_2$-graduados dado por $\alpha(x_i^{(0)}) = Y_i$, $\alpha(x_i^{(1)}) = Z_i$, $\forall i \geqslant 1$. Para cada $f \in I$, temos (pelo item (a) do Lema 2.14) que

$$\begin{aligned} \alpha(f(x_1^{(0)}, x_1^{(1)}, \ldots, x_n^{(0)}, x_n^{(1)})) &= f(\alpha(x_1^{(0)}), \alpha(x_1^{(1)}), \ldots, \alpha(x_n^{(0)}), \alpha(x_n^{(1)})) \\ &= f(Y_1, Z_1, \ldots, Y_n, Z_n) \\ &= 0 \end{aligned}$$

portanto $f \in Ker\alpha$. Suponha que $f = f(x_1^{(0)}, x_1^{(1)}, \ldots, x_n^{(0)}, x_n^{(1)}) \in Ker\,\alpha$. Escolha $a_1^{(j)}, \ldots, a_n^{(j)} \in sl_2^{(j)}$, $j = 0, 1$. Defina

$$\gamma\colon \{Y_i, Z_i |\, i \geqslant 1\} \to sl_2(D)$$

por $Y_i \mapsto a_i^{(0)}$, $Z_i \mapsto a_i^{(1)}$. Pelo item b) do Lema 2.14 podemos estender γ a um homomorfismo de pares $\mathbb{Z}_2$-graduados $\gamma\colon (R, S) \to (M_2(D), sl_2(D))$, consequentemente

$$\begin{aligned} 0 &= \gamma(f(Y_1, Z_1, \ldots, Y_n, Z_n)) \\ &= f(\gamma(Y_1), \gamma(Z_1), \ldots, \gamma(Y_n), \gamma(Z_n)) \\ &= f(a_1^{(0)}, a_1^{(1)}, \ldots, a_n^{(0)}, a_n^{(1)}) \end{aligned}$$

e como os $a_i^{(j)}$ foram escolhidos arbitrariamente segue que $f \in I$ e isso mostra que $I = Ker\alpha$. Note que a imagem de α contém um gerador de (R, S) e, portanto, existe um isomorfismo $\overline{\alpha}\colon D\langle X\rangle/I \to R$ tal que $\overline{\alpha}((L\langle X\rangle + I)/I) = S$ e $\overline{\alpha}((D\langle X\rangle_i + I)/I) \subseteq R_i$, $i = 0, 1$. □

Lema 2.16. *Os seguintes polinômios são identidades fracas $\mathbb{Z}_2$-graduadas para o par $(M_2(D), sl_2(D))$:*

1. $[y_1, y_2]$,

2. $z_1z_2z_3 - z_3z_2z_1$,

3. $y_1z_1 + z_1y_1$,

com $y_i \in D\langle X\rangle_0$ *e* $z_j \in D\langle X\rangle_1$.

Demonstração. De verificação imediata. □

Seja I o T_2-ideal fraco gerado pelas identidades do lema anterior e B o conjunto dos monômios:

a) $y_{a_1}y_{a_2}\cdots y_{a_k}$,

b) $y_{a_1}y_{a_2}\cdots y_{a_k}z_{i_1}z_{j_1}\cdots z_{i_n}\widehat{z_{j_n}}$,

para quaisquer $k \geqslant 0$, $n > 0$, $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k$, $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_n$, $j_1 \leqslant j_2 \leqslant \cdots \leqslant j_n$ e $\widehat{z_{j_n}}$ significa que a parcela z_{j_n} pode não aparecer.

Lema 2.17. *Seja I como anteriormente, então:*

$$D\langle X\rangle/I = \langle\{m + I|\, m \in B\}\rangle.$$

Demonstração. Seja $m = y_{i_1}z_{j_1}y_{i_2}\ldots y_{i_r}z_{j_r}$, $r \geqslant 0$ (alguns fatores podem ser expressões vazias). Pela identidade 3 do Lema 2.16, podemos colocar os y_{i_s} à esquerda dos z_{j_k}, ou seja, $m = \pm y_{i_1}y_{i_2}\ldots y_{i_r}z_{j_1}\ldots z_{j_r}$ módulo I. Por outro lado a identidade 1 do mesmo lema nos permite colocar os y_{i_s} em ordem crescente e por fim a identidade 2 nos permite reordenar os z_{j_s} das posições "pares" e o mesmo para aqueles das posições ímpares. Isso prova o lema. □

A demonstração do lema a seguir faz uso de matrizes genéricas e é semelhante à demonstração da Proposição 5 de [30] (ver também [31]).

Lema 2.18. *Seja D um domínio de integridade infinito. Nenhuma combinação linear não trivial dos elementos de B é uma identidade fraca $\mathbb{Z}_2$-graduada para o par $(M_2(D), sl_2(D))$.*

Demonstração. Considere os geradores do par (R, S),

$$Y_i = \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix}, \qquad Z_i = \begin{pmatrix} 0 & b_i \\ c_i & 0 \end{pmatrix}.$$

Se m_1 é um monômio do tipo a), então

$$m_1(Y_{i_1}, Y_{i_2}, \ldots, Y_{i_k}) = \begin{pmatrix} a_{i_1}a_{i_2}\cdots a_{i_k} & 0 \\ 0 & (-1)^k a_{i_1}a_{i_2}\cdots a_{i_k} \end{pmatrix}.$$

Como a variável Y_i de maior índice corresponde à variável a_i de maior índice, podemos recuperar os monômios do tipo a) a partir da matriz resultante, ou seja,

$$m_1(Y_{i_1}, Y_{i_2}, \ldots, Y_{i_k}) = m_1'(Y_{i_1}, Y_{i_2}, \ldots, Y_{i_k}) \Leftrightarrow m_1 = m_1'.$$

Agora note que os monômios do tipo a) geram apenas matrizes com entradas nos a_i's e os a_i, b_i e c_i são algebricamente independentes, portanto apenas precisamos verificar se os monômios do tipo b) são linearmente independentes. Considere um monômio

$$m_2(z_{i_1}, z_{j_1}, \ldots, \widehat{z_{j_n}}) = z_{i_1} z_{j_1} \cdots \widehat{z_{j_n}}$$

do tipo b) com $k = 0$. Então

$$m_2(Z_{i_1}, Z_{j_1}, \ldots, \widehat{Z_{j_n}}) = (b_{i_1} c_{j_1} \cdots b_{i_n} c_{j_n}) e_{11} + (c_{i_1} b_{j_1} \cdots c_{i_n} b_{j_n}) e_{22},$$

se a variável z_{j_n} ocorre. Caso contrário, teremos

$$m_2(Z_{i_1}, Z_{j_1}, \ldots, \widehat{Z_{j_n}}) = (b_{i_1} c_{j_1} \cdots b_{i_n}) e_{12} + (c_{i_1} b_{j_1} \cdots c_{i_n}) e_{21}.$$

Suponha que $m_2 = z_{i_1} z_{j_1} \cdots z_{i_n} \widehat{z_{j_n}}$ e $m_2' = z_{c_1} z_{d_1} \cdots z_{c_m} \widehat{z_{d_m}}$, com $n \geqslant m$, resultam em uma mesma matriz M quando avaliados nas matrizes

$$Z_{i_1}, Z_{j_1}, \ldots, Z_{i_n}, Z_{j_n}.$$

Como o grau dos monômios nas entradas de M é o mesmo de m_2 (e de m_2') temos $m = n$. Agora, note que $b_{c_1}, b_{c_2}, \ldots, b_{c_n}$ aparecem na escrita de M e o mesmo para $b_{i_1}, b_{i_2}, \ldots, b_{i_n}$ (na entrada e_{12} ou e_{11} , por exemplo), pois as variáveis z_{c_k} e z_{i_k} aparecem nas posições ímpares nos monômios m_2' e m_2, respectivamente. Consequentemente, obtemos que $\{z_{i_1}, \ldots, z_{i_n}\} = \{z_{c_1}, \ldots, z_{c_n}\}$, mas como os índices nas posições ímpares (na escrita de m_2 e m_2') estão em ordem crescente, a única possibilidade é que tenhamos $z_{c_k} = z_{i_k}, \forall k \geqslant 1$, ou seja, $m_2' = z_{i_1} z_{d_1} \cdots z_{i_n} z_{d_n}$. Analogamente, podemos mostrar que $z_{d_k} = z_{j_k}, \forall k \geqslant 1$ e isso mostra que $m_2 = m_2'$. Com isso, podemos recuperar estes monômios à partir da avaliação nas matrizes genéricas e de modo análogo verifica-se para monômios do tipo b) com $k > 0$. Desta forma, uma combinação linear dos elementos de B avaliados em (R, S) resultará em uma matriz cujas entradas são polinômios com os mesmos coeficientes que a combinação linear inicial, mas os a_i, b_k e c_s são algebricamente independentes e, então, uma tal combinação linear resultará em 0 apenas se todos os coeficientes forem nulos. □

Proposição 2.19. *Seja D um domínio de integridade infinito. As identidades do Lema 2.16 formam uma base de identidades fracas $\mathbb{Z}_2$-graduadas para o par $(M_2(D), sl_2(D))$.*

Demonstração. Consequência imediata dos Lemas 2.17 e 2.18. □

2.2 A Propriedade de Specht

Ao longo desta seção D será um anel comutativo, unitário e Noetheriano. Continuaremos denotando por I o T_2-ideal fraco gerado por: (1) $[y_1, y_2]$, (2) $z_1z_2z_3 - z_3z_2z_1$ e (3) $y_1z_1 + z_1y_1$, com $y_i \in D\langle X\rangle_0$ e $z_i \in D\langle X\rangle_1$. Recordemos que uma álgebra A (ou o seu T-ideal $Id(A)$) satisfaz a propriedade de Specht se todo T-ideal contendo $Id(A)$ possui base finita. De modo análogo, podemos definir a propriedade de Specht para álgebras graduadas, pares de álgebras etc. Nesta seção mostraremos que, munido da $\mathbb{Z}_2$-graduação natural, o par $(M_2(D), sl_2(D))$ satisfaz a propriedade de Specht. Aqui empregamos os mesmos métodos utilizados por E. P. Rezende e A. Krasilnikov em [46].

Convém observar que o Lema 2.17 continua válido para anéis comutativos com unidade. Além disso, a demonstração do lema a seguir repete palavra por palavra a demonstração do Lema 2.18.

Lema 2.20. *Seja B o conjunto formado por todos os monômios do tipo:*

a) $y_{a_1}y_{a_2}\cdots y_{a_k}$,

b) $y_{a_1}y_{a_2}\cdots y_{a_k}z_{c_1}z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}$,

com $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k$, $c_1 \leqslant c_2 \leqslant \cdots \leqslant c_m$, $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_m$, $k \geqslant 0$ *e* $m > 0$. *Então* $\{m + I \mid m \in B\}$ *é uma base para o D-módulo livre $D\langle X\rangle/I$.*

Sejam M_1 e M_2 o conjunto formado, respectivamente, pelos monômios dos tipos a) e b), $M = M_1 \cup M_2$ e $\widetilde{M} = \widetilde{M_1} \cup \widetilde{M_2}$, sendo $\widetilde{M_i}$ a imagem de M_i em $D\langle X\rangle/I$.

Definição 2.21. *Sejam $(A, \leqslant)$ um conjunto parcialmente ordenado e $B \subseteq A$. O fecho de B é o conjunto $cl(B) = \{a \in A \mid \exists b \in B,\, b \leqslant a\}$. Dizemos que B é fechado se $cl(B) = B$.*

Lema 2.22 (G. Higman [22])**.** *Seja A um conjunto parcialmente ordenado. São equivalentes:*

a) Toda sequência infinita $a_1, a_2, \ldots$ de elementos de A possui uma subsequência infinita não-decrescente $a_{i_1} \leqslant a_{i_2} \leqslant \cdots$ $(i_1 < i_2 < \cdots)$;

b) Se $a_1, a_2, \ldots$ é um sequência infinita de elementos de A, então existem inteiros i e j tais que $i < j$ e $a_i \leqslant a_j$;

c) Toda cadeia ascendente de subconjuntos fechados de A estabiliza;

d) Todo subconjunto não vazio fechado de A é o fecho de um conjunto finito;

e) Não existe sequência infinita estritamente decrescente, nem um número infinito de elementos mutuamente incomparáveis.

Definição 2.23. *Seja $\leqslant$ uma relação de ordem A. Se $\leqslant$ é uma ordem linear (uma ordem total) e todo subconjunto não-vazio de A possui um único elemento minimal, dizemos que A é bem ordenado e que $\leqslant$ é uma boa ordem. Se A é parcialmente ordenado e todo subconjunto não-vazio $B \subseteq A$ possui um número finito não-nulo de elementos minimais, dizemos que A é um conjunto parcialmente bem ordenado e que $\leqslant$ é uma boa ordem parcial.*

Note que um conjunto é parcialmente bem ordenado se, e somente se, satisfaz algum dos ítens do Lema 2.22. De fato, suponha que A é parcialmente bem ordenado. Sejam $a_1 \geqslant a_2 \geqslant \cdots$ uma sequência não-crescente em A e $B = \{a_i \mid i \geqslant 1\}$. Como B é não vazio, existe uma quantidade finita de elementos minimais, na verdade apenas um, pois B é totalmente ordenado. Digamos que $a_s \in B$ seja esse elemento minimal. Assim, $a_s = a_{s+1} = \cdots$, ou seja, a sequência é finita. Seja $B \subseteq A$ um conjunto formado por elementos mutuamente incomparáveis. Cada elemento incomparável é um minimal, mas estes existem em quantidade finita. Isso mostra que vale (e). Vejamos a recíproca. Seja $B \neq \varnothing$ e B_0 o conjunto formado pelos elementos minimais de B. Os elementos de B_0 são incomparáveis entre si, mas estes existem em número finito por (e), ou seja, B_0 é finito. Suponha que B é finito. Dado $b \in B$, se b é minimal temos $B_0 \neq \varnothing$. Caso contrário, existe $b_1 \in B$ tal que $b_1 < b$. Repetimos o argumento com b_1 no lugar de b, obtendo $b_2 \in B$ tal que $b_2 < b_1 < b$. Como B é finito, esse processo deve terminar e quando isso acontecer teremos encontrado um elemento minimal $b_s \in B$, ou seja, $B_0 \neq \varnothing$. Agora, se B é infinito e $B_0 = \varnothing$, então tome $a_1 \in B$. Como a_1 não é minimal (pois $B_0 = \varnothing$) existe $a_2 \in B$ tal que $a_1 > a_2$. Da mesma forma a_2 não é minimal, e, portanto, existe $a_3 \in B$ tal que $a_1 > a_2 > a_3$. Continuando com esse procedimento, obtemos uma sequência infinita estritamente decrescente em B, mas isso não é possível. Isso mostra que $B_0 \neq \varnothing$.

Lema 2.24 (G. Higman [22])**.** *Seja Φ o conjunto de todas as funções $\phi\colon \mathbb{N} \to \mathbb{N}$ estritamente crescentes e $(A, \leqslant)$ um conjunto parcialmente ordenado, com elemento distinguido $0 \in A$. Considere $V(A) = V(A, 0)$ o conjunto de todas as sequências quase nulas de elementos de A. Defina a relação $\leqslant_\Phi$ em $V(A)$ por $\{u_i\} \leqslant_\Phi \{v_i\}$ se, e somente se, existe $\phi \in \Phi$ tal que $u_i \leqslant v_{\phi(i)}$, $\forall i \in \mathbb{N}$. Nestas condições $(V(A), \leqslant_\Phi)$ é parcialmente bem ordenado.*

Lema 2.25 (G. Higman [22])**.** *Sejam $(A_1, \leqslant_1)$ e $(A_2, \leqslant_2)$ conjuntos parcialmente ordenados. Considere a relação $\leqslant$ em $A_1 \times A_2$ dada por $(a_1, a_2) \leqslant (b_1, b_2)$ se, e somente se, $a_1 \leqslant_1 b_1$ e $a_2 \leqslant_2 b_2$. Se A_1 e A_2 são parcialmente bem ordenados, então $(A_1 \times A_2, \leqslant)$ é parcialmente bem ordenado.*

Sejam $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ e $Q_n = \mathbb{N}_0^n$. Considere em $\mathbb{N}_0$ a ordem natural $\leqslant$. Pelo Lema 2.25 o conjunto $(Q_n, \leqslant)$ é um conjunto parcialmente bem ordenado, onde $\leqslant$ é a ordem termo a termo. Considere o conjunto $V(Q_n)$ formado por todas as sequências quase nulas. Defina a relação de ordem $\leqslant_\Phi$ em $V(Q_n)$ pela regra $\{u_i\} \leqslant_\Phi \{v_i\}$ se, e somente se, existe $\phi \in \Phi$ tal que $u_i \leqslant v_{\phi(i)}, \forall i \geqslant 1$. As demonstrações dos lemas a seguir podem ser vistas em [46].

Lema 2.26. *$(V(Q_n), \leqslant_\Phi)$ é um conjunto parcialmente bem ordenado.*

Definição 2.27. *Defina em $V(Q_1)$ a relação $\leqslant$ por $\{u_i\} \leqslant \{v_i\}$ se, e somente se, $\{u_i\} = \{v_i\}$ ou existe $k > 0$ tal que $u_k < v_k$ e $u_j = v_j$ se $j > k$.*

Observe que $V(Q_1)$ está em bijeção com o conjunto $Y = \{y_1^{u_1} \cdots y_n^{u_n} \mid n \geqslant 1\}$ e que a relação em $V(Q_1)$ acima é a ordem lexicográfica induzida de Y. Assim,

Lema 2.28. *A relação $\leqslant$ é uma boa ordem linear em $V(Q_1)$.*

Observe que existe uma bijeção natural entre $V(Q_n)$ e $V(Q_1)^n$ dada por

$$\{(u_i^{(1)}, u_i^{(2)}, \ldots, u_i^{(n)})\} \mapsto (\{u_i^{(1)}\}, \{u_i^{(2)}\}, \ldots, \{u_i^{(n)}\}).$$

Em $V(Q_n)$ defina a seguinte função $\partial\colon V(Q_n) \to \mathbb{N}$ por

$$\partial(u) = \partial(\{u_i^{(1)}\}, \{u_i^{(2)}\}, \ldots, \{u_i^{(n)}\}) = \sum_{i,j} u_i^{(j)}.$$

Sejam $u = (\{u_i^{(1)}\}, \{u_i^{(2)}\})$ e $v = (\{v_i^{(1)}\}, \{v_i^{(2)}\}) \in V(Q_2)$. Defina a relação $\leqslant$ em $V(Q_2)$ por: $u \leqslant v$ se, e somente se, $\partial(u) < \partial(v)$ ou $\partial(u) = \partial(v)$ e $\{u_i^{(2)}\} < \{v_i^{(2)}\}$ ou $\partial(u) = \partial(v)$, $\{u_i^{(2)}\} = \{v_i^{(2)}\}$ e $\{u_i^{(1)}\} < \{v_i^{(1)}\}$ (ordem de $V(Q_1)$).

Lema 2.29. *A relação $\leqslant$ é uma boa ordem linear em $V(Q_2)$.*

Definamos agora uma boa ordem linear $\leqslant$ em $V(Q_n)$ para $n \geqslant 3$. Sejam

$$u = (\{u_i^{(1)}\}, \{u_i^{(2)}\}, \ldots, \{u_i^{(n)}\}) \text{ e } v = (\{v_i^{(1)}\}, \{v_i^{(2)}\}, \ldots, \{v_i^{(n)}\})$$

elementos de $V(Q_n)$. Defina $u < v$ se, e somente se, $(\{u_i^{(n-1)}\}, \{u_i^{(n)}\}) < (\{v_i^{(n-1)}\}, \{v_i^{(n)}\})$ em $V(Q_2)$ ou existe $t_0 > 0$ tal que $\{u_i^{(t_0)}\} < \{v_i^{(t_0)}\}$ em $V(Q_1)$ e $\{u_i^{(t)}\} = \{v_i^{(t)}\}, \forall t > t_0$.

Lema 2.30. *A relação acima é uma boa ordem linear em $V(Q_n)$.*

Sejam

$V_1 = V(Q_1)$
$V_2 = \{u \in V(Q_3) \mid \partial(u_i^{(2)}) > 0,\ \partial(u_i^{(2)}) - \partial(u_i^{(3)}) = 0 \text{ ou } 1\}$
$V = V_1 \cup V_2$

Cada conjunto V_i herda a boa ordem de $V(Q_n)$. Defina em V a seguinte relação:

i) Para cada i, se $u, v \in V_i$ e $u < v$ em V_i, então $u < v$ em V.

ii) Se $u \in V_1$ e $v \in V_2$, então $u < v$ em V.

Como $(V(Q_n), \leqslant)$ é totalmente ordenado, segue que $\leqslant$ é uma ordem linear em V.

Lema 2.31. *A relação $\leqslant$ é uma boa ordem linear em V.*

Demonstração. Seja $W \neq \varnothing$ um subconjunto de V. Então $W = (W \cap V_1) \cup (W \cap V_2)$. Se $W_1 = W \cap V_1$ é não vazio, então W tem um único elemento minimal e este pertence a W_1, pois V_1 é bem ordenado e por ii). Por outro lado, se W_1 é vazio, temos $W = W \cap V_2 \subseteq V_2$ não vazio, e como V_2 é bem ordenado, existe (único) elemento minimal em W. Portanto, $(V, \leqslant)$ é bem ordenado. $\square$

Defina em V a relação $\leqslant'$ da seguinte forma: dados u, $v \in V$, $u \leqslant' v$ se, e somente se, existe $i \in \{1, 2\}$ tal que u, $v \in V_i$ e $u \leqslant_\Phi v$.

Lema 2.32. *$(V, \leqslant')$ é um conjunto parcialmente bem ordenado.*

Demonstração. Seja $u = \{u_i\}$ uma sequência infinita de elementos de V. Então existe uma subsequência contida em V_1 ou em V_2. Como $V_1 \subseteq V(Q_1)$ e $V_2 \subseteq V(Q_3)$ são parcialmente bem ordenados existe uma subsequência infinita não-decrescente de u contida em V_1 (ou V_2). O resultado segue do Lema 2.22. $\square$

Seja ϕ uma função de $\mathbb{N}$ em $\mathbb{N}$ estritamente crescente. Defina $\phi\colon V(Q_n) \to V(Q_n)$ por $\phi(\{u_i\}) = \{v_i\}$, com

$$v_j = \begin{cases} u_i, & j = \phi(i) \\ 0, & j \notin \phi(\mathbb{N}) \end{cases}$$

Denote por Φ_1 a família de funções $\phi_1\colon V(Q_n) \to V(Q_n)$ dadas por $\phi_1 = \phi$ se $n = 1, 2$ e $\phi_1(u, v) = (\phi(u), v)$ com $u \in V(Q_{n-2})$ e $v \in V(Q_2)$ se $n > 2$. Analogamente denote por Φ_2 a família de funções $\phi_2\colon V(Q_n) \to V(Q_n)$ tais que ϕ_2 é a identidade se $n = 1, 2$ e $\phi_2(u, v) = (u, \phi(v))$, com $u \in V(Q_{n-2})$ e $v \in V(Q_{n-2})$ para $n > 2$.

Considere a família $\widetilde{\Phi}$ de todos os endomorfismos de $D\langle X\rangle/I$ dados por

$$\widetilde{\phi}(x_i + I) = x_{\phi(i),} + I$$

com $\phi\colon \mathbb{N} \to \mathbb{N}$ é estritamente crescente e $x_i \in \{y_i, z_i \mid i \geqslant 1\}$. Sejam ainda $\widetilde{\Phi}_1$ o conjunto formado por todos os endomorfismos de $D\langle X\rangle/I$ dados por $\widetilde{\phi}_1(y_i + I) = y_{\phi(i)} + I$ e $\widetilde{\phi}_1(z_i + I) = z_i + I$ e $\widetilde{\Phi}_2$ o conjunto dos endomorfismos de $D\langle X\rangle/I$ dados por $\widetilde{\phi}_2(z_i + I) = z_{\phi(i)} + I$ e $\widetilde{\phi}_2(y_i + I) = y_i + I$. Considere a função $\xi\colon \widetilde{M} \to V$ dada por

- $\xi(y_{a_1} y_{a_2} \cdots y_{a_k} + I) = \{u_i^{(1)}\}$

- $\xi(y_{a_1}y_{a_2}\cdots y_{a_k}z_{c_1}z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}+I)=\{(u_i^{(1)},u_i^{(2)},u_i^{(3)})\}$,

com $u_i^{(1)}=\sum_{a_j;a_j=i}1$, $u_i^{(2)}=\sum_{c_j;c_j=i}1$ e $u_i^{(3)}=\sum_{d_j;d_j=i}1$.
A função ξ é uma bijeção e portanto podemos induzir em $\widetilde{M}$ as relações de ordem $\leqslant$ e $\leqslant'$ de V. De agora em diante, omitiremos o ideal I na escrita dos elementos de $\widetilde{M}$.

Lema 2.33. *Suponha que $x\in\widetilde{M}$, $\widetilde{\phi}\in\widetilde{\Phi}$, $\widetilde{\phi}_i\in\widetilde{\Phi}_i$, $i=1,\,2$. Então $\xi(\widetilde{\phi}(x))=\phi(\xi(x))$ e $\xi(\widetilde{\phi}_i(x))=\phi_i(\xi(x))$.*

Demonstração. Observe que $\widetilde{\phi}=\widetilde{\phi}_1\circ\widetilde{\phi}_2=\widetilde{\phi}_2\circ\widetilde{\phi}_1$ e, portanto, só precisamos verificar que $\xi(\widetilde{\phi}_i(x))=\phi_i(\xi(x))$. Suponha que $x\in\widetilde{M}_1$ e, portanto, $x=y_{a_1}\cdots y_{a_k}=y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}}$, com $u_i^{(1)}=\sum_{a_j;a_j=i}1$. Temos

$$\phi_1(\xi(y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}}))=\phi_1(\{u_i^{(1)}\})=\phi(\{u_i^{(1)}\})=\{v_i\},$$

com $v_j=u_i^{(1)}$ se $j=\phi(i)$ e $v_j=0$ se $j\notin\phi(\mathbb{N})$. Por outro lado,

$$\begin{aligned}\xi(\widetilde{\phi}_1(x))&=\xi(\widetilde{\phi}_1(y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}}))\\&=\xi(y_{\phi(1)}^{u_1^{(1)}}\cdots y_{\phi(n)}^{u_n^{(1)}})\\&=\{v_i\}\end{aligned}$$

com $v_j=u_i^{(1)}$ se $j=\phi(i)$ e $v_j=0$ se $j\notin\phi(\mathbb{N})$. Suponha agora que $x\in\widetilde{M}_2$. Então podemos escrever $x=y_{a_1}y_{a_2}\cdots y_{a_k}z_{c_1}z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}=y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}}z_{c_1}z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}$. Temos

$$\begin{aligned}\phi_1(\xi(x))&=\phi_1(\{u_i^{(1)},u_i^{(2)},u_i^{(3)}\})\\&=(\phi(\{u_i^{(1)}\}),\{(u_i^2,u_i^{(3)})\})\\&=\{(v_i,u_i^{(2)},u_i^{(3)})\}\end{aligned}$$

com $v_j=u_i^{(1)}$ se $j=\phi(i)$ e $v_j=0$ se $j\notin\phi(\mathbb{N})$ $u_i^{(2)}=\sum_{c_j;c_j=i}1$ e $u_i^{(3)}=\sum_{d_j;d_j=i}1$. Calculando $\xi(\widetilde{\phi}_1(x))$ obtém-se:

$$\begin{aligned}\xi(\widetilde{\phi}_1(x))&=\xi(\widetilde{\phi}_1(y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}}z_{c_1}z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}))\\&=\{(v_i,u_i^{(2)},u_i^{(3)})\}\end{aligned}$$

com $v_i=u_j^{(1)}$ se $j=\phi(i)$ e $v_j=0$ se $j\notin\phi(\mathbb{N})$, $u_i^{(2)}=\sum_{c_j;c_j=i}1$ e $u_i^{(3)}=\sum_{d_j;d_j=i}1$. Vejamos o que ocorre com $\widetilde{\phi}_2$. Para $x\in\widetilde{M}_1$

$$\begin{aligned}\xi(\widetilde{\phi}_2(x))&=\xi(\widetilde{\phi}_2(y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}}))\\&=\xi(y_1^{u_1^{(1)}}\cdots y_n^{u_n^{(1)}})\\&=\{u_i^{(1)}\}.\end{aligned}$$

Além disso,

$$\begin{aligned}\phi_2(\xi(x)) &= \phi_2(\xi(y_1^{u_1^{(1)}} \cdots y_n^{u_n^{(1)}}))\\ &= \phi_2(\{u_i^{(1)}\})\\ &= \{u_i^{(1)}\}.\end{aligned}$$

Considere novamente $x = y_1^{u_1^{(1)}} \cdots y_n^{u_n^{(1)}} z_{c_1} z_{d_1} \cdots z_{c_m} \widehat{z_{d_m}} \in \widetilde{M}_2$. Nestas condições

$$\begin{aligned}\xi(\widetilde{\phi}_2(x)) &= \xi(\widetilde{\phi}_2(y_1^{u_1^{(1)}} \cdots y_n^{u_n^{(1)}} z_{c_1} z_{d_1} \cdots z_{c_m} \widehat{z_{d_m}}))\\ &= \xi(y_1^{u_1^{(1)}} \cdots y_n^{u_n^{(1)}} z_{\phi(c_1)} z_{\phi(d_1)} \cdots z_{\phi(c_m)} \widehat{z_{\phi(d_m)}}))\\ &= \{u_i^{(1)}, u_i^{(2)}, u_i^{(3)}\}\end{aligned}$$

com $u_i^{(2)} = \sum_{\phi(c_j);\phi(c_j)=i} 1$ e $u_i^{(3)} = \sum_{\phi(d_j);\phi(d_j)=i} 1$ e $u_i^{(k)} = 0$ se $i \notin \phi(\mathbb{N})$. Por fim,

$$\begin{aligned}\phi_2(\xi(x)) &= \phi_2(\{u_i^{(1)}, v_i^{(2)}, v_i^{(3)}\})\\ &= \{u_i^{(1)}, \phi(\{v_i^{(2)}, v_i^{(3)}\})\}\\ &= \{u_i^{(1)}, w_i^{(2)}, w_i^{(3)}\}\end{aligned}$$

com $v_i^{(2)} = \sum_{c_r;c_r=i} 1$, $v_i^{(3)} = \sum_{d_r;d_r=i} 1$ e

$$w_j^{(k)} = \begin{cases} v_i^{(k)}, & \text{se } j = \phi(i)\\ 0, & \text{se } j \notin \phi(\mathbb{N})\end{cases}.$$

Suponha que $j = \phi(i)$. Vendo ϕ como uma bijeção sobre sua imagem podemos escrever $w_j^{(2)} = v_{\phi^{-1}(j)}^{(2)} = \sum_{c_r;c_r=\phi^{-1}(j)} 1 = \sum_{c_r;\phi(c_r)=j} 1 = \sum_{\phi(c_r);\phi(c_r)=j} 1 = u_j^{(2)}$ e $w_j^{(2)} = u_j^{(2)} = 0$ se $j \notin \phi(\mathbb{N})$ e, de modo análogo, para $w_j^{(3)}$, ou seja, $w_j^{(k)} = u_j^{(k)}$. Logo $\phi_1(\xi(x)) = \xi(\widetilde{\phi}_1(x))$ e $\phi_2(\xi(x)) = \xi(\widetilde{\phi}_2(x))$. □

Observe que em geral não podemos multiplicar duas desigualdades membro a membro. Por exemplo, se $z = z_3z_4$, $z' = z_1z_5$, $x = z_2$ e $x' = x$, então $z \leqslant z'$, contudo, $x'z' < xz$. De qualquer forma, ainda existem algumas boas operações que preservam a relação de ordem conforme veremos a seguir. Antes de continuarmos note que, na demonstração do Lema 2.20 (ou Lema 2.17), mostramos que, para cada monômio $m \in D\langle X\rangle/I$, existe um único monômio $\delta(m) \in M$ satisfazendo $\delta(m) = \delta_m m$ (módulo I), com $\delta_m = \pm 1$. Em particular, se $y \in \widetilde{M}_1$ e $m \in \widetilde{M}_i$, vale a igualdade $\delta(ym) = ym \in \widetilde{M}_i$, $i = 1, 2$.

Lema 2.34. *Sejam $y = y_1^{r_1} \cdots y_n^{r_n}$ e $x, \widetilde{x} \in \widetilde{M}$ tais que $x \leqslant \widetilde{x}$. Então, $yx \leqslant y\widetilde{x}$.*

Demonstração. Se $x \in \widetilde{M}_1$ e $\widetilde{x} \in \widetilde{M}_2$ (ou $x = \widetilde{x}$) nada precisa ser feito, pois $yx \in \widetilde{M}_1$ e $y\widetilde{x} \in \widetilde{M}_2$. Sejam $x = y_1^{u_1} \cdots y_k^{u_k}$ e $\widetilde{x} = y_1^{v_1} \cdots y_k^{v_k}$ com $u_kv_k \neq 0$. Então, existe $t_0 \in \mathbb{N}$ tal que $u_{t_0} < v_{t_0}$ e $u_t = v_t$ para cada $t > t_0$. Seja $m = max\{k, n\}$, então

$$\xi(yx) = \xi(y_1^{u_1+r_1} \cdots y_m^{u_m+r_m}) = \{u_i + r_i\}$$

e

$$\xi(y\widetilde{x}) = \xi(y_1^{v_1+r_1}\cdots y_m^{v_m+r_m}) = \{v_i + r_i\},$$

com $u_{t_0} + r_{t_0} < v_{t_0} + r_{t_0}$ e $u_t + r_t = v_t + r_t$, para $t > t_0$. Logo, $\xi(yx) < \xi(y\widetilde{x})$ se x, $\widetilde{x} \in \widetilde{M}_1$. Resta provar o caso x, $\widetilde{x} \in \widetilde{M}_2$. Suponha que $x = y_{a_1}\cdots y_{a_n} z_{c_1} z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}}$ e $\widetilde{x} = y_{a'_1}\cdots y_{a'_m} z_{c'_1} z_{d'_1}\cdots z_{c'_s}\widehat{z_{d'_s}}$. Observe que se $z_{c_1} z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}} \leqslant z_{c'_1} z_{d'_1}\cdots z_{c'_s}\widehat{z_{d'_s}}$, então para quaisquer y, $y' \in \widetilde{M}_1$, tem-se $y z_{c_1} z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}} \leqslant y' z_{c'_1} z_{d'_1}\cdots z_{c'_s}\widehat{z_{d'_s}}$. Assim, podemos supor que

$$z_{c_1} z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}} = z_{c'_1} z_{d'_1}\cdots z_{c'_s}\widehat{z_{d'_s}}$$

e

$$y_{a_1}\cdots y_{a_n} \leqslant y_{a'_1}\cdots y_{a'_m}.$$

Pela primeira parte da demonstração, temos $y y_{a_1}\cdots y_{a_n} \leqslant y y_{a'_1}\cdots y_{a'_m}$ e, portanto, $yx \leqslant y\widetilde{x}$. □

Lema 2.35. *Se $x = y_1^{u_1}\cdots y_n^{u_n}$ e $y = y_1^{r_1}\cdots y_k^{r_k}$, então $x \leqslant xy$.*

Demonstração. Basta notar que 1, y e $x \in \widetilde{M}_1$ e aplicar o Lema 2.34 para obter $x \cdot 1 \leqslant xy$. □

Lema 2.36. *Sejam $x = z_{a_1} z_{a_2}\cdots z_{a_k}$ e $z = z_{t_1}\cdots z_{t_k}$. Então $x \leqslant xz$.*

Demonstração. Devido à identidade (2) valem as igualdades $\delta_x = \delta_{xz} = 1$, ou seja, $x = \delta(x) \in \widetilde{M}$ e $xz = \delta(xz) \in \widetilde{M}$. Agora podemos computar a imagem destes elementos por ξ:

$$\partial(\xi(xz)) = \partial(\xi(x)) + \partial(z) \geqslant \partial(\xi(x))$$

e a igualdade ocorre apenas se z é igual a 1, portanto, $x \leqslant xz$. □

Lema 2.37. *Sejam $y = y_1^{r_1}\cdots y_n^{r_n}$, $z = z_{t_1}\cdots z_{t_k}$ e x, $\widetilde{x} \in \widetilde{M}$. Se $x \leqslant \widetilde{x}$, então:*

a) $\delta(xy) \leqslant \delta(\widetilde{x}y)$;

b) $xz \leqslant \widetilde{x}z$.

Demonstração. (a) Se x, $\widetilde{x} \in \widetilde{M}_1$, então $xy = yx$ e $\widetilde{x}y = y\widetilde{x}$. Assim, pelo Lema 2.34, obtém-se $\delta(xy) \leqslant \delta(\widetilde{x}y)$. Suponha que $x = y' z_{c_1} z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}$ e $\widetilde{x} = y'' z_{c'_1} z_{d'_1}\cdots z_{c'_l}\widehat{z_{d'_l}}$ sejam elementos de $\widetilde{M}_2$, com $y' = y_{a_1}\cdots y_{a_{m_1}}$ e $y'' = y_{a'_1}\cdots y_{a'_{l_1}}$. Caso tenhamos $z_{c_1} z_{d_1}\cdots z_{c_m}\widehat{z_{d'_m}} < z_{c'_1} z_{d'_1}\cdots z_{c'_l}\widehat{z_{d'_l}}$, então $\delta(xy) \leqslant \delta(\widetilde{x}y)$. Assim, podemos supor que $z = z_{c_1} z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}} = z_{c'_1} z_{d'_1}\cdots z_{c'_l}\widehat{z_{d'_l}}$; desta forma $y' \leqslant y''$, pois $x \leqslant \widetilde{x}$. Temos também $\delta(xy) = y' y z_{c_1} z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}$ e $\delta(\widetilde{x}y) = y'' y z_{c_1} z_{d_1}\cdots z_{c_l}\widehat{z_{d_l}}$ (identidade (3)). Segue do Lema 2.34 que $y'y < y''y$, logo $\delta(xy) \leqslant \delta(\widetilde{x}y)$. Se $x \in \widetilde{M}_1$ e $\widetilde{x} \in \widetilde{M}_2$, então segue direto da definição de $\leqslant$ que $\delta(xy) \leqslant \delta(\widetilde{x}y)$. Isso prova o ítem ($a$).

(b) Observe que $\delta(xz)$ é obtido de xz após uma reordenação das variáveis z_{t_i}, e apenas estas. Isto não produz mudanças no sinal, logo $\delta(xz) = xz$ e o mesmo para $\widetilde{x}z$. Se x, $\widetilde{x} \in \widetilde{M}_1$, então é imediato que $xz \leqslant \widetilde{x}z$. Sejam $x = yz'$ e $\widetilde{x} = y'z''$, com $z' = z_{c_1}z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}}$, $z'' = z_{c_1'}z_{d_1'}\cdots z_{c_k'}\widehat{z_{d_k'}}$ e y e y' são monômios nos y_i's. Assim, $xz = yz'z$ e $\widetilde{x}z = y'z''z$. Caso $z' = z''$, teremos $y \leqslant y'$ e, portanto, $xz \leqslant \widetilde{x}z$. Se a igualdade não ocorrer, teremos $z' \leqslant z''$ e neste caso a única coisa que precisaremos provar é que $z'z \leqslant z''z$, pois teremos $xz = yz'z \leqslant y'z''z = \widetilde{x}z$. Com isso, podemos supor que $x = z_{c_1}z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}}$ e $\widetilde{x} = z_{c_1'}z_{d_1'}\cdots z_{c_{k'}'}\widehat{z_{d_{k'}'}}$. Por hipótese $x \leqslant \widetilde{x}$, ou equivalentemente, $\xi(x) \leqslant \xi(\widetilde{x})$. Logo, $\{(r_i, s_i)\} \leqslant \{(r_i', s_i')\}$, com $r_i = \sum_{c_j;c_j=i} 1$, $s_i = \sum_{d_j;d_j=i} 1$, $r_i' = \sum_{c_j';c_j'=i} 1$ e $s_i' = \sum_{d_j';d_j'=i} 1$. Precisamos considerar os seguintes casos:

(a) $\partial(\{(r_i, s_i)\}) < \partial(\{(r_i', s_i)'\})$;

(b) $\partial(\{(r_i, s_i)\}) = \partial(\{(r_i', s_i)'\})$ e $\{s_i\} < \{s_i'\}$ ou $\{s_i\} = \{s_i'\}$ e $\{r_i\} < \{r_i'\}$.

Se vale (a), é imediato que $xz \leqslant \widetilde{x}z$, então podemos supor a igualdade $k = k'$. Para (b), apenas precisamos considerar os casos em que ambos $x = z_{c_1}z_{d_1}\cdots z_{c_k}\widehat{z_{d_k}}$ e $\widetilde{x} = z_{c_1'}z_{d_1'}\cdots z_{c_k'}\widehat{z_{d_k'}}$ possuem grau par ou ambos possuem grau ímpar. Considere que x e $\widetilde{x}$ têm grau par. Basta que provemos o resultado para $z = z_{t_1}$, o caso geral segue por indução. Por hipótese temos $\{s_i\} < \{s_i'\}$ ou $\{s_i\} = \{s_i'\}$ e $\{r_i\} < \{r_i'\}$, onde $r_i = \sum_{c_j;c_j=i} 1$, $s_i = \sum_{d_j;d_j=i} 1$, $r_i' = \sum_{c_j';c_j'=i} 1$ e $s_i' = \sum_{d_j';d_j'=i} 1$, então $\xi(xz) = \{(u_i, v_i)\}$ com $u_i = r_i$ se $i \neq t_1$, $u_{t_1} = r_{t_1} + 1$ e $v_i = s_i$, $i \geqslant 1$. Analogamente para $\widetilde{x}$ temos $\xi(\widetilde{x}z) = \{(u_i', v_i')\}$ com $u_{t_1}' = r_{t_1}' + 1$, $u_i' = r_i'$ se $i \neq t_1$ e $v_i' = s_i'$, $i \geqslant 1$. Se ocorrer $\{s_i\} < \{s_i'\}$, então $\{v_i\} < \{v_i'\}$; se por outro lado ocorrer $\{s_i\} = \{s_i'\}$ e $\{r_i\} < \{r_i'\}$, então teremos $\{v_i\} = \{v_i'\}$ e $\{u_i\} < \{u_i'\}$, logo $\{(u_i, v_i)\} \leqslant \{(u_i', v_i')\}$, ou seja, $\xi(xz) \leqslant \xi(\widetilde{x}z)$. Logo $xz \leqslant \widetilde{x}z$. O caso em que x e $\widetilde{x}$ possuem grau ímpar é análogo. $\square$

O próximo lema, mostra que $\widetilde{\phi}_1$, $\widetilde{\phi}_2$ e $\widetilde{\phi}$ preservam a relação $\leqslant$.

Lema 2.38. *Sejam $\widetilde{\phi} \in \widetilde{\Phi}$, $\widetilde{\phi}_i \in \widetilde{\Phi}_i$, $i = 1, 2$. Se $x < \widetilde{x}$, então:*

a) $\widetilde{\phi}_i(x) < \widetilde{\phi}_i(\widetilde{x})$;

b) $\widetilde{\phi}(x) < \widetilde{\phi}(\widetilde{x})$.

Demonstração. Como $\widetilde{\phi} = \widetilde{\phi}_1 \circ \widetilde{\phi}_2$, só precisamos provar o ítem (a). Suponha que $x, \widetilde{x} \in \widetilde{M}_1$. Se $x = 1$ ou $\widetilde{x} = 1$, então o resultado é imediato. Então podemos supor que $x = y_1^{r_1}\cdots y_n^{r_n}$ e $\widetilde{x} = y_1^{s_1}\cdots y_n^{s_n}$ com $s_n \neq 0$ ou $r_n \neq 0$. Temos $\xi(\widetilde{\phi}_1(x)) = \xi(y_{\phi(1)}^{r_1}\cdots y_{\phi(n)}^{r_n}) = \{r_i'\}$, onde $r_i' = r_j$ se $i = \phi(j)$ e $r_i' = 0$ se $i \notin \phi(\mathbb{N})$. Analogamente, $\xi(\widetilde{\phi}_1(\widetilde{x})) = \xi(y_{\phi(1)}^{s_1}\cdots y_{\phi(n)}^{s_n}) = \{s_i'\}$, onde $s_i' = s_j$ se $i = \phi(j)$ e $s_i' = 0$ se $i \notin \phi(\mathbb{N})$. Como $x < \widetilde{x}$, existe $t_0 \in \mathbb{N}$ tal que $r_{t_0} < s_{t_0}$ e $s_t = r_t$ se $t > t_0$. É suficiente mostrar que $r_{\phi(t_0)}' < s_{\phi(t_0)}'$ e $s_t' = r_t'$ se $t > \phi(t_0)$. Como $\phi(t_0) \in \phi(\mathbb{N})$ segue que $r_{\phi(t_0)}' = r_{t_0} < s_{t_0} = s_{\phi(t_0)}'$. Seja $t > \phi(t_0)$ e suponha que $t \in \phi(\mathbb{N})$.

Como ϕ é crescente, existe $p > t_0$ tal que $t = \phi(p)$. Logo $r'_t = r_p = s_p = s'_t$. Por outro lado, se $t \notin \phi(\mathbb{N})$, então $r'_t = s'_t = 0$. Isso mostra que $\widetilde{\phi}_1(x) < \widetilde{\phi}_1(\widetilde{x})$. Agora, sejam $x = yz$ e $\widetilde{x} = y'z' \in \widetilde{M}$, com y, $y' \in \widetilde{M}_1$ e z e z' são monômios nas variáveis z_t. Como $\widetilde{\phi}_1$ fixa as variáveis z_t, segue que $\widetilde{\phi}_1(x) = \widetilde{\phi}_1(y)z$ e $\widetilde{\phi}_1(\widetilde{x}) = \widetilde{\phi}_1(y')z'$. Se $z < z'$ o resultado é imediato. Suponha que $z = z'$. Como $x < \widetilde{x}$, temos $y < y'$ e assim $\widetilde{\phi}_1(y) < \widetilde{\phi}_1(y')$ pela primeira parte da demonstração. Logo, $\widetilde{\phi}_1(x) = \widetilde{\phi}_1(y)z < \widetilde{\phi}_1(y')z' = \widetilde{\phi}_1(\widetilde{x})$.

Vejamos como comporta-se a função $\widetilde{\phi}_2$. Suponha inicialmente que

$$x = z_{c_1} z_{d_1} \cdots z_{c_m} \widehat{z_{d_m}}, \quad \widetilde{x} = z_{c'_1} z_{d'_1} \cdots z_{c'_l} \widehat{z_{d'_l}}.$$

Por definição, temos $\xi(x) = \{(0, r_i, s_i)\}$ e $\xi(\widetilde{x}) = \{(0, r'_i, s'_i)\}$, com $r_i = \sum_{c_j; c_j = i} 1$, $s_i = \sum_{d_j; d_j = i} 1$, $r'_i = \sum_{c'_j; c'_j = 1} 1$ e $s'_i = \sum_{d'_j; d'_j = 1} 1$. Além disso, $\xi(\widetilde{\phi}_2(x)) = \{(0, u_i, v_i)\}$ e $\xi(\widetilde{\phi}_2(\widetilde{x})) = \{(0, u'_i, v'_i)\}$, com $(u_i, v_i) = (r_j, s_j)$, $(u'_i, v'_i) = (r'_j, s'_j)$ se $i = \phi(j)$ e $(u_i, v_i) = (u'_i, v'_i) = (0, 0)$ se $i \notin \phi(\mathbb{N})$. Note que x, $\widetilde{x} \in \widetilde{M}_2$ e, por hipótese, $x < \widetilde{x}$. Por isso, temos apenas duas possibilidades:

(a) $\partial(\{(r_j, s_j)\}) < \partial(\{(r'_j, s'_j)\})$;

(b) $\partial(\{(r_j, s_j)\}) = \partial(\{(r'_j, s'_j)\})$ e $\{s_i\} < \{s'_i\}$ ou $\{s_i\} = \{s'_i\}$ e $\{r_i\} < \{r'_i\}$.

Como $\partial(\{(0, u_i, v_i)\}) = \partial(\{(0, r_j, s_j)\})$ e $\partial(\{(0, u'_i, v'_i)\}) = \partial(\{(0, r'_j, s'_j)\})$, se ocorre (a), então $\partial(\{(0, u_i, v_i)\}) < \partial(\{(0, u'_i, v'_i)\})$. Se ocorre (b), então $\{v_i\} < \{v'_i\}$ ou $\{v_i\} = \{v'_i\}$ e $\{u_i\} < \{u'_i\}$. Isso mostra que $\xi(\widetilde{\phi}_2(x)) < \xi(\widetilde{\phi}_2(\widetilde{x}))$. Finalmente, suponha que $x = yz$ e $\widetilde{x} = y'z' \in \widetilde{M}$, com y, $y' \in \widetilde{M}_1$ e z e z' são monômios nas variáveis z_t. Se $z < z'$, então, pelo que acabamos de ver, $\widetilde{\phi}_2(z) < \widetilde{\phi}_2(z')$. Além disso, $\widetilde{\phi}_2$ fixa as variáveis y's. Logo, $\widetilde{\phi}_2(x) = y\widetilde{\phi}_2(z) < y'\widetilde{\phi}_2(z') = \widetilde{\phi}_2(y'z') = \widetilde{\phi}_2(\widetilde{x})$. Agora, se $z = z'$, então $y < y'$ e novamente obtém-se $\widetilde{\phi}_2(x) = y\widetilde{\phi}_2(z) < y'\widetilde{\phi}_2(z') = \widetilde{\phi}_2(y'z') = \widetilde{\phi}_2(\widetilde{x})$. □

Lema 2.39. *Sejam x, $\widetilde{x} \in \widetilde{M}_i$, $i = 1, 2$. Se $x \leqslant' \widetilde{x}$, então existem $\widetilde{\phi} \in \widetilde{\Phi}$, $y \in \widetilde{M}_1$ e $z = z_{t_1} \cdots z_{t_k}$, $k \geqslant 0$, tais que $y\widetilde{\phi}(x)z = \widetilde{x}$.*

Demonstração. Suponha inicialmente que $x, \widetilde{x} \in \widetilde{M}_1$, $x = y_1^{r_1} \cdots y_n^{r_n}$ e $\widetilde{x} = y_1^{s_1} \cdots y_n^{s_n}$, com $r_n \neq 0$ ou $s_n \neq 0$. Como $x \leqslant' \widetilde{x}$, existe $\phi \in \Phi$ tal que $r_j \leqslant s_{\phi(j)}$, para cada $j \geqslant 1$. Além disso, $\xi(\widetilde{\phi}(x)) = \{r'_i\}$, com $r'_i = r_j$ se $i = \phi(j)$ e $r'_i = 0$ se $i \notin \phi(\mathbb{N})$, logo $\widetilde{\phi}(x) = y_1^{r'_1} \cdots y_{\phi(n)}^{r'_{\phi(n)}}$ (lembre que ϕ é crescente). Seja, para cada $i \geqslant 1$, $l_i = s_i - r'_i$. Note que $l_i = s_i$ se $i \notin \phi(\mathbb{N})$ e que $l_i = s_{\phi(j)} - r_j > 0$ se $i = \phi(j)$. Assim, podemos considerar o elemento $y = y_1^{l_1} \cdots y_{\phi(n)}^{l_{\phi(n)}}$. Calculando $\xi(y\widetilde{\phi}(x))$, obtemos

$$\begin{aligned}
\xi(y\widetilde{\phi}(x)) &= \xi(y_1^{l_1} \cdots y_{\phi(n)}^{l_{\phi(n)}} \widetilde{\phi}(x)) \\
&= \xi(y_1^{l_1} \cdots y_{\phi(n)}^{l_{\phi(n)}} y_1^{r'_1} \cdots y_{\phi(n)}^{r'_{\phi(n)}}) \\
&= \xi(y_1^{l_1 + r'_1} \cdots y_{\phi(n)}^{l_{\phi(n)} + r'_{\phi(n)}}) \\
&= \{l_i + r'_i\} = \{s_i\} = \xi(\widetilde{x}).
\end{aligned}$$

Logo, $y\widetilde{\phi}(x)z = \widetilde{x}$, com $z = 1$. Agora, sejam $x = \overline{y}\,\overline{z}$, $\widetilde{x} = \widetilde{y}\,\widetilde{z} \in \widetilde{M}_2$, com $\overline{y} = y_{a_1}\cdots y_{a_k}$, $\widetilde{y} = y_{a'_1}\cdots y_{a'_{k'}}$, $\overline{z} = z_{c_1}z_{d_1}\cdots z_{c_m}\widehat{z_{d_m}}$ e $\widetilde{z} = z_{c'_1}z_{d'_1}\cdots z_{c'_{m'}}\widehat{z_{d'_{m'}}}$. Provaremos a existência de $\widetilde{\phi} \in \widetilde{\Phi}$ e $z = z_{t_1}\cdots z_{t_i}$ tais que:

(a) $y\widetilde{\phi}(\overline{y}) = \widetilde{y}$;

(b) $\widetilde{\phi}(\overline{z})z = \widetilde{z}$.

Como consequência teremos $y\widetilde{\phi}(x)z = y\widetilde{\phi}(\overline{y})\widetilde{\phi}(\overline{z})z = \widetilde{y}\,\widetilde{z} = \widetilde{x}$. Lembre que $\xi(x) = \{(u_i^{(1)}, u_i^{(2)}, u_i^{(3)})\}$, com $u_i^{(1)} = \sum_{a_j;a_j=i} 1$, $u_i^{(2)} = \sum_{c_j;c_j=i} 1$ e $u_i^{(3)} = \sum_{d_j;d_j=i} 1$. Analogamente, temos $\xi(\widetilde{x}) = \{(v_i^{(1)}, v_i^{(2)}, v_i^{(3)})\}$, onde $v_i^{(1)} = \sum_{a'_j;a'_j=i} 1$, $v_i^{(2)} = \sum_{c'_j;c'_j=i} 1$ e $v_i^{(3)} = \sum_{d'_j;d'_j=i} 1$. (a) Como $x \leqslant' \widetilde{x}$, existe $\phi \in \Phi$ tal que $u_j^{(i)} < v_{\phi(j)}^{(i)}$, $j \geqslant 1$ e $i \in \{1,2,3\}$. Seja $l_k^{(i)} = v_k^{(i)}$ se $k \notin \phi(\mathbb{N})$ e $l_k^{(i)} = v_{\phi(j)}^{(i)} - u_j^{(i)}$ se $k = \phi(j)$, para cada j, $k \geqslant 1$ e $i \in \{1,2,3\}$. Note que $l_k^{(i)} \geqslant 0$ e, portanto, podemos considerar um monômio y tal que $\xi(y) = \{l_j^{(1)}\}$. Temos também que $\overline{y} \leqslant' \widetilde{y}$, pois, $u_j^{(1)} < v_{\phi(j)}^{(1)}$, $j \geqslant 1$. Então pela primeira parte da demonstração obtemos $y\widetilde{\phi}(\overline{y}) = \widetilde{y}$. Para provar (b), considere o elemento $\overline{z} = z_{c_1}z_{d_1}\cdots z_{c_m}z_{d_m}$ e defina $z = z_{e_1}z_{f_1}\cdots z_{e_{m''}}z_{f_{m''}}$, com $l_i^{(2)} = \sum_{e_j;e_j=i} 1$ e $l_i^{(3)} = \sum_{f_j;f_j=i} 1$. Assim,

$$\begin{aligned}\xi(\widetilde{\phi}(\overline{z})z) &= \xi(z_{\phi(c_1)}z_{\phi(d_1)}\cdots z_{\phi(c_m)}z_{\phi(d_m)}z_{e_1}z_{f_1}\cdots z_{e_{m''}}z_{f_{m''}})\\ &= \{(0, u_i'^{(2)}, u_i'^{(3)})\}\end{aligned}$$

onde $u_i'^{(2)} = \sum_{\phi(c_j);\phi(c_j)=i} 1 + \sum_{e_j;e_j=i} 1$ e $u_i'^{(3)} = \sum_{\phi(d_j);\phi(d_j)=i} 1 + \sum_{f_j;f_j=i} 1$. Se $i = \phi(s)$, então $u_i'^{(2)} = \sum_{\phi(c_j);\phi(c_j)=\phi(s)} 1 + \sum_{e_j;e_j=\phi(s)} 1 = u_s^{(2)} + l_{\phi(s)}^{(2)} = v_i^{(2)}$. Por outro lado, se $i \notin \phi(\mathbb{N})$, então $u_i'^{(2)} = 0 + \sum_{e_j;e_j=i} 1 = l_i^{(2)} = v_i^{(2)}$. De modo análogo prova-se que $u_i'^{(3)} = v_i^{(3)}$, $i \geqslant 1$. Por fim, $\xi(\widetilde{z}) = \{(0, v_i^{(2)}, v_i^{(3)})\} = \{(0, u_i'^{(2)}, u_i'^{(3)})\} = \xi(\widetilde{\phi}(\overline{z})z)$, ou seja, $\widetilde{\phi}(\overline{z})z = \widetilde{z}$. Para o caso $\overline{z} = z_{c_1}z_{d_1}\cdots z_{c_m}$ basta definir $z = z_{f_1}z_{e_1}\cdots z_{f_{m''}}$ e repetir os argumentos anteriores. □

Definição 2.40. *Seja $f = \sum_{i=1}^{n} \alpha_i m_i$, $m_i \in \widetilde{M}$ e $\alpha_i \in D$. Se $\alpha_1 \neq 0$ e $m_1 > m_i$, para cada $i \geqslant 1$, diremos que $lm(f) = m_1$, $lc(f) = \alpha_1$ e $lt(f) = \alpha_1 m_1$ são, respectivamente, o monômio, o coeficiente e o termo líder de f.*

Lema 2.41. *Sejam f e $\widetilde{f}$ combinações lineares de elementos de $\widetilde{M}$ com $lm(f) = x$ e $lm(\widetilde{f}) = \widetilde{x}$. Se $x \leqslant' \widetilde{x}$, então existem $\widetilde{\phi} \in \widetilde{\Phi}$, $y \in \widetilde{M}_1$ e $z \in \widetilde{M}$ tais que $lm(y\widetilde{\phi}(f)z) = \widetilde{x}$.*

Demonstração. Como $x \leqslant \widetilde{x}$, então pelo Lema 2.39, existem $\widetilde{\phi} \in \widetilde{\Phi}$, $y \in \widetilde{M}_1$ e $z = z_{t_1}\cdots z_{t_k}$, $k \geqslant 0$, tais que $y\widetilde{\phi}(x)z = \widetilde{x}$. Por outro lado, a relação de ordem $\leqslant$ é preservada por $\widetilde{\phi}$ e o mesmo por multiplicações à esquerda por y e à direita por z. Logo, $lm(y\widetilde{\phi}(f)z) = y\widetilde{\phi}(x)z = \widetilde{x}$. □

Teorema 2.42. *Seja D um anel associativo, comutativo, unitário e Noetheriano. Seja I o T_2-ideal fraco gerado pelas identidades $[y_1, y_2]$, $z_1z_2z_3 - z_3z_2z_1$ e $y_1z_1 + z_1y_1$, com $y_i \in D\langle X\rangle_0$ e $z_i \in D\langle X\rangle_1$. Então, todo T_2-ideal fraco contendo I possui base finita. Em particular, munido da $\mathbb{Z}_2$-graduação natural, o par $(M_2(D), sl_2(D))$ satisfaz a propriedade de Specht.*

Demonstração. Suponha que exista um T_2-ideal fraco J contendo I que não é finitamente gerado. Então podemos escolher um elemento $g_1 \in J\backslash I$ e gerar um outro T_2-ideal fraco I_1 gerado por g_1 e I de modo que $I \subsetneq I_1 \subsetneq J$. Como J não é finitamente gerado, podemos escolher $g_2 \in J\backslash I_1$ e gerar outro T_2-ideal fraco, digamos I_2, gerado por g_2 e I_1 de modo que $I \subsetneq I_1 \subsetneq I_2 \subsetneq J$. Repetindo esse argumento, obtém-se uma cadeia estritamente ascendente de T_2-ideais fracos finitamente gerados $I \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$. Esta cadeia por sua vez, induz uma cadeia estritamente ascendente de ideais $J_1 \subsetneq J_2 \subsetneq \cdots$ de $D\langle X\rangle/I$ com $J_k = I_k/I$. Mostraremos que uma tal cadeia em $D\langle X\rangle/I$ não pode existir. Uma vez que $\widetilde{M}$ é uma base para $D\langle X\rangle/I$, podemos escrever cada elemento de $R_i = J_i\backslash J_{i-1}$ como combinação linear de elementos de $\widetilde{M}$. Seja L_i o conjunto dos monômios líderes dos elementos de R_i. Note que $L_i \neq \varnothing$, pois $R_i \neq \varnothing$. Além disso, como $\leqslant$ é uma boa ordem linear em $\widetilde{M}$, cada conjunto L_i possui um único elemento minimal x_i. A relação $\leqslant'$ é uma boa ordem parcial para $\widetilde{M}$, logo a sequência $\{x_i\}$ possui uma subsequência infinita $\{x_{i_k}\}$ não-decrescente com respeito a $\leqslant'$ (Lema 2.22). Para cada $x_{i_l} \in L_{i_l}$, seja $h_l \in R_{i_l}$ um elemento não-nulo cujo termo líder é $lt(h_l) = \alpha_l x_{i_l}$, $\alpha_l \in D$. Seja I_0 o ideal gerado por α_1, α_2, ... Como D é Noetheriano, existe k tal que I_0 é gerado por α_1, ..., α_k. Assim, $\alpha_{k+1} = \sum_l^k \beta_l\alpha_l$, com $\beta_l \in D$. Como $x_{i_l} \leqslant' x_{i_{k+1}}$, para cada $l = 1$, ..., k, existem y_l, $z_l \in \widetilde{M}$ e $\widetilde{\phi} \in \widetilde{\Phi}$ tais que $lm(y_l\widetilde{\phi}(h_l)z_l) = x_{i_{k+1}}$ (Lema 2.41). Logo, $lt(y_l\widetilde{\phi}(h_l)z_l) = \alpha_l x_{i_{k+1}}$. Considere agora $h = \sum_{l=1}^k \beta_l y_l\widetilde{\phi}(h_l)z_l$. Observe que $h = \sum_{l=1}^k \beta_l\alpha_l x_{i_{k+1}} +$ (fatores menores). Logo, $lt(h) = \sum_{l=1}^k \beta_l\alpha_l x_{i_{k+1}} = (\sum_{l=1}^k \beta_l\alpha_l)x_{i_{k+1}} = \alpha_{k+1}x_{i_{k+1}}$. Note que para cada $l = 1$, ..., k, tem-se $h_l \in R_{i_l} \subsetneq J_{i_l} \subseteq J_{i_{(k+1)}-1}$, pois $i_1 < i_2 < \cdots < i_k \leqslant i_{(k+1)} - 1$. Além disso, $\widetilde{\phi}(h_l) \in J_{i_{(k+1)}-1}$, pois I_k é um T_2-ideal fraco (na verdade porque cada ideal J_k é invariante por endomorfismos de $\widetilde{\Phi}$). Assim, $y_l\widetilde{\phi}(h_l)z_l \in J_{i_{(k+1)}-1}$ e, portanto, $h \in J_{i_{(k+1)}-1}$. Considere agora o elemento $f = h_{k+1} - h \in D\langle X\rangle/I$ e recorde que h_{k+1} possui termo líder $\alpha_{k+1}x_{i_{k+1}}$. No entanto, como mostramos anteriormente, este é o mesmo termo líder de h. Logo, f possui monômio líder menor que $x_{i_{k+1}}$. Pela escolha dos h_l's, temos $h_{k+1} \in J_{i_{(k+1)}}\backslash J_{i_{(k+1)}-1}$. Além disso, $h \in J_{i_{(k+1)}-1} \subsetneq J_{i_{(k+1)}}$ e, portanto, $f \in J_{i_{(k+1)}}\backslash J_{i_{(k+1)}-1} = R_{i_{k+1}}$. Ora, isso não é possível uma vez que o monômio líder de f está em $L_{i_{k+1}}$ (por definição) e este é menor que $x_{i_{k+1}}$, o elemento minimal de $L_{i_{k+1}}$. Isto prova o resultado. $\square$

Capítulo 3

Identidades Fracas com Ação de Grupo

Seja $G \leqslant Aut(A, L)$ um subgrupo, não necessariamente abeliano, do grupo de automorfismos do par (A, L). Dizemos neste caso que (A, L) é um G-par ou que é um par com ação de G. Considere a G-álgebra associativa $F\langle X; G\rangle$ sobre F livremente gerada por $X = \{x_i^g |\, g \in G, i \geqslant 1\}$ e $L\langle X; G\rangle \subseteq F\langle X; G\rangle^{(-)}$ a G-subálgebra de Lie gerada por X. Então o par $(F\langle X; G\rangle, L\langle X; G\rangle)$ é livre na classe dos pares (A, L) com ação de G. Em geral vale a inclusão $Aut(A, L) \subseteq Aut(A)$. Em particular, como os automorfismos de $M_n(\mathbb{C})$ são dados por conjugação (pelo teorema de Skolem e Noether) e a conjugação preserva o traço das matrizes, tem-se $Aut(M_n(\mathbb{C}), sl_n(\mathbb{C})) = Aut(M_n(\mathbb{C}))$. Segue disso que todo automorfismo de $M_n(\mathbb{C})$ preserva $sl_n(\mathbb{C})$. Observamos aqui que, se $n > 2$, os automorfismos da álgebra de Lie $sl_n(\mathbb{C})$ não se resumem apenas às conjugações. Mas como já vimos, considerando o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$, é suficiente considerar o grupo dos automorfismos da álgebra matricial.

Definição 3.1. *Dizemos que um G-polinômio $f(x_1^{g_1}, \ldots, x_n^{g_n}) \in \mathbb{C}\langle X; G\rangle$ é uma G-identidade fraca para o par (A, L) se $f(a_1^{g_1}, \ldots, a_n^{g_n}) = 0$, para cada $a_i \in L$.*

Definição 3.2. *Sejam (A_1, L_1) e (A_2, L_2) dois G-pares. Um homomorfismo de pares $f\colon (A_1, L_1) \to (A_2, L_2)$ é dito um homomorfismo de G-pares se para cada $g \in G$ e $a \in A_1$ tem-se $f(a^g) = f(a)^g$.*

Como no caso de identidades polinomiais, o conjunto $Id^G(A, L)$ de todas as G-identidades fracas do par (A, L) forma um G-ideal fraco, ou seja, um ideal invariante por endomorfismos do G-par $(F\langle X; G\rangle, L\langle X; G\rangle)$. Seja agora $A = \mathbb{C}[a_i, b_i, c_i |\, i \geqslant 1]$ a álgebra associativa e comutativa livremente gerada por $X = \{a_i, b_i, c_i |\, i \geqslant 1\}$ e $G \subseteq Aut(M_2(\mathbb{C}))$ um grupo finito de automorfismos agindo fielmente em $M_2(\mathbb{C})$. Então $G \subseteq PGL_2(\mathbb{C})$ age em $M_2(A)$ por meio de conjugações. Considere as G-álgebras associativa e de Lie, respectivamente, $R^G, S^G \subseteq M_2(A)$ geradas sobre $\mathbb{C}$ por

$$s_i = \begin{pmatrix} a_i & b_i \\ c_i & -a_i \end{pmatrix},\ i \geqslant 1.$$

De modo análogo ao que foi feito para o caso graduado podemos verificar que o par (R^G, S^G) é o G-par associativo-Lie relativamente livre na variedade $\mathcal{V}(I)$ determinada pelo G-ideal de identidades fracas $I = Id^G(M_2(\mathbb{C}), sl_2(\mathbb{C}))$. De agora em diante admitiremos sempre que $G \subseteq Aut(M_2(\mathbb{C}), sl_2(\mathbb{C})) = Aut(M_2(\mathbb{C}))$ é um grupo finito agindo fielmente no par

$$Aut(M_2(\mathbb{C}), sl_2(\mathbb{C})),$$

ou seja, G é um dos grupos $\mathbb{Z}_n$, D_n, S_4, A_4 ou A_5. Estes são os subgrupos finitos $PGL_2(\mathbb{C})$ e sua descrição remonta ao Teorema de Platão sobre os poliedros regulares. A demonstração formal foi dada por F. Klein em [27], em 1884. O lema seguinte é demonstrado do mesmo modo que o Lema 2 de [6].

Lema 3.3. *Sejam $\phi\colon G \to PGL_2(\mathbb{C})$ e $\psi\colon G \to PGL_2(\mathbb{C})$ duas ações de um grupo G no G-par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$ tais que $\phi(g) = B\psi(g)B^{-1}$. Então $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$ tem as mesmas G-identidades nas duas ações.*

3.1 Identidades fracas com ação de $\mathbb{Z}_n$

Como $Aut(A, L) \subseteq Aut(A)$ e $L\langle X; G\rangle$ herda a $\widehat{G}$-graduação da álgebra livre $\mathbb{C}\langle X; G\rangle = \oplus_{\chi\in\widehat{G}}\mathbb{C}\langle X; G\rangle^{(\chi)}$, a dualidade entre G-ação de grupo abeliano finito e G-graduação continua válida se considerarmos pares (A, L) no lugar de álgebras e a demonstração da proposição a seguir repete palavra por palavra a demonstração da Proposição 1.45.

Proposição 3.4. *Seja $G \subseteq Aut(A, L)$ um grupo abeliano finito e considere o G-par livre $(\mathbb{C}\langle X; G\rangle, L\langle X; G\rangle)$. Então $(\mathbb{C}\langle X; G\rangle, L\langle X; G\rangle)$ é o par livre $\widehat{G}$-graduado de posto enumerável e $id^G(A, L) = id^{gr}(A, L)$.*

Suponha que $G = \mathbb{Z}_n$ é gerado por g. Como g tem ordem n, segue que g age por meio de conjugação por uma matriz diagonalizável $\phi(g)$. Assim, pelo Lema 3.3, podemos supor que $\phi(g) = \alpha e_{11} + \beta e_{22}$, com $\alpha, \beta \neq 0$. Porém multiplicar $\phi(g)$ por escalares não-nulos não altera a ação e, então, multiplicando esta matriz por $1/\alpha$, podemos supor que g age por conjugação através de uma matriz da forma $\phi(g) = e_{11} + \omega e_{22}$, sendo ω é uma raíz n-ésima primitiva da unidade. Dito isso, g age assim em $sl_2(\mathbb{C})$:

$$g\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a & \omega^{-1}b \\ \omega c & -a \end{pmatrix}$$

No caso particular em que $n = 2$, a ação ocorre da seguinte forma:

$$e\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}, \qquad g\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a & -b \\ -c & -a \end{pmatrix}.$$

Sejam $\pi_0(x) = e(x) + g(x)$ e $\pi_1(x) = e(x) - g(x)$. Então, pela Proposição 2.19, e, pela Proposição 3.4, obtemos:

Proposição 3.5. *Os $\mathbb{Z}_2$-polinômios a seguir formam uma base de $\mathbb{Z}_2$-identidades fracas para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$:*

1. $[\pi_0(x_1), \pi_0(x_2)]$,
2. $\pi_1(x_1)\pi_1(x_2)\pi_1(x_3) - \pi_1(x_3)\pi_1(x_2)\pi_1(x_1)$,
3. $\pi_0(x_1)\pi_1(x_2) + \pi_1(x_2)\pi_0(x_1)$.

Suponha que $G = \mathbb{Z}_n$, $n \geqslant 3$. Como G é abeliano a álgebra de grupo $\mathbb{C}G$ tem decomposição em soma direta de ideais minimais $\mathbb{C}G = \bigoplus \mathbb{C}e_i$, com $e_i = 1/|G| \sum \omega^{-ij} g^j$. Note que

$$e_0\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \quad e_1\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix},$$

$$e_{n-1}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}.$$

Em geral temos o seguinte:

$$e_i\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} \sum \omega^{-ij} a & \sum \omega^{-(i+1)j} b \\ \sum \omega^{-(i-1)j} c & -\sum \omega^{-ij} a \end{pmatrix}.$$

Mas, $\omega^{-i} = 1$ se, e somente se, $i = 0$. Por outro lado, $w^{-(i+1)} = 1$ apenas quando $i = n-1$. Por fim, $\omega^{-(i-1)} = 1$ equivale a termos $i = 1$. Portanto, como cada potência ω^j é igual a 1 ou é uma raíz do polinômio $f(x) = 1 + x + \cdots + x^{n-1}$, pois ω é uma raíz primitiva da unidade, isso mostra que e_i aniquila $sl_2(\mathbb{C})$ se $i \neq 0$, 1, $n-1$. Escreveremos e_{-1} no lugar de e_{n-1}.

Lema 3.6. *Sejam $G = \mathbb{Z}_n$, $n \geqslant 3$ e $\alpha = \pm 1$. As seguintes relações são G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$:*

1. $e_0(x) + e_1(x) + e_{-1}(x) = x$,
2. $e_\alpha(x_1)e_\alpha(x_2) = 0$,
3. $[e_0(x_1), e_0(x_2)] = 0$,

4. $e_\alpha(x_1)e_{-\alpha}(x_2)e_\alpha(x_3) = e_\alpha(x_3)e_{-\alpha}(x_2)e_\alpha(x_1)$,

5. $e_0(x_1)e_\alpha(x_2) + e_\alpha(x_2)e_0(x_1) = 0$.

Demonstração. De verificação imediata. □

Seja B o conjunto de todos os monômios da forma

$$e_0(x)^{\underline{n}}e_\alpha(x_{i_1})e_{-\alpha}(x_{j_1})\cdots e_\alpha(x_{i_k})\widehat{e_{-\alpha}(x_{j_k})},$$

com $\alpha = \pm 1$, $e_0(x)^{\underline{n}} = e_0(x_1)^{n_1}\cdots e_0(x_r)^{n_r}$, $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_k$, $j_1 \leqslant j_2 \leqslant \cdots \leqslant j_k$ e $\widehat{e_{-\alpha}(x_{j_k})}$ significa que a parcela $e_{-\alpha}(x_{j_k})$ pode não ocorrer. Denote por I o G-ideal de identidades fracas gerado pelas identidades do Lema 3.6.

Lema 3.7. *Seja B como acima. Então*

$$\mathbb{C}\langle X; G\rangle / I = \langle \{m + I \,|\, m \in B\}\rangle.$$

Demonstração. Primeiramente observe que a identidade $x = e_0(x) + e_1(x) + e_{-1}(x)$ ou, de modo mais geral, $g^j x = e_0(x) + \omega^j e_1(x) + \omega^{-j}e_{-1}(x)$ (ver Observação 1.38), nos mostra que um monômio

$$m = m(x_1^{g_1}, \ldots, x_n^{g_n})$$

pode ser escrito como uma combinação linear de monômios em $e_0(x_i)$, $e_1(x_i)$ e $e_{-1}(x_i)$ módulo I. Sem perda de generalidade, podemos supor que m é apenas um monômio em $e_0(x_i)$, $e_1(x_i)$ e $e_{-1}(x_i)$. Pela identidade 5 do Lema 3.6, podemos reescrever cada um desses monômios deixando todos os $e_0(x_i)$ à esquerda dos demais elementos. Além disso, usando a identidade 3 do mesmo lema podemos escrever $m = e_0(x)^{\underline{n}}e_{\alpha_1}(x_{r_1})\cdots e_{\alpha_s}(x_{r_s})$ módulo I, com $\alpha_i = \pm 1$. Observe que devido à identidade 2 do Lema 3.6 podemos supor que os elementos da forma $e_{\alpha_p}(x_i)$ e $e_{\alpha_p}(x_j)$ não são adjacentes. Por fim, a identidade 4 permite reescrevermos

$$m = e_0(x)^{\underline{n}}e_\alpha(x_{i_1})e_{-\alpha}(x_{j_1})\cdots(x_{i_k})\widehat{e_{-\alpha}(x_{j_k})}$$

módulo I com $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_k$ e $j_1 \leqslant j_2 \leqslant \cdots \leqslant j_k$. □

Lema 3.8. *Nenhuma combinação linear não trivial dos elementos de B é uma G-identidade para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

Demonstração. Observe que se avaliarmos um elemento de B nas matrizes genéricas

$$X_i = \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} = e_0\begin{pmatrix} a_i & b_i \\ c_i & -a_i \end{pmatrix} \in S^G$$

e este monômio apresentar algum fator da forma $e_1(x_i)$ ou $e_{-1}(x_i)$, então este monômio será aniquilado. Consequentemente, em uma combinação linear de tais monômios, os únicos fatores que sobram após estes serem avaliados nas matrizes X_i são aqueles da forma $e_0(x)^{\underline{n}} = e_0(x_1)^{n_1}\cdots e_0(x_k)^{n_k}$ e estas avaliações resultam em $a_1^{n_1}\cdots a_k^{n_k}e_{11} + (-1)^{n_1+\cdots+n_k}a_1^{n_1}\cdots a_k^{n_k}e_{22}$. Observando que os $a_i's$ são algebricamente independentes, podemos recuperar cada $e_0(x)^{\underline{n}}$ de sua avaliação. Então uma combinação linear nula de monômios de B só ocorre se todos os coeficientes dos fatores $e_0(x)^{\underline{n}}$ forem iguais a zero e, assim, podemos supor que em uma tal combinação linear não aparecem elementos da forma $e_0(x)$. Considere os monômios dos tipos m_1, m_2, m_3 e m_4 a seguir:

1. $m_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_1(x_{i_k})e_{-1}(x_{j_k})$,
2. $m_2 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_1(x_{i_k})$,
3. $m_3 = e_{-1}(x_{i_1})e_1(x_{j_1})\cdots e_{-1}(x_{i_k})e_1(x_{j_k})$,
4. $m_4 = e_{-1}(x_{i_1})e_1(x_{j_1})\cdots e_{-1}(x_{i_k})$.

Seja, para cada $i \geqslant 1$,

$$X_i = \begin{pmatrix} a_i & b_i \\ c_i & -a_i \end{pmatrix}.$$

Avaliando cada um dos monônios acima em $X_{i_1}, X_{j_1}, \ldots, X_{j_k}$, obteremos como resultado, respectivamente, as matrizes

1. $M_1 = c_{i_1}\cdots c_{i_k}b_{j_1}\cdots b_{j_k}e_{22}$,
2. $M_2 = c_{i_1}\cdots c_{i_k}b_{j_1}\cdots b_{j_{k-1}}e_{21}$,
3. $M_3 = b_{i_1}\cdots b_{i_k}c_{j_1}\cdots c_{j_k}e_{11}$,
4. $M_4 = b_{i_1}\cdots b_{i_k}c_{j_1}\cdots c_{j_{k-1}}e_{12}$.

Logo, basta considerarmos combinações lineares onde os monômios são do mesmo tipo m_i, $i \in \{1,2,3,4\}$. Agora é só proceder como na demonstração do Lema 2.18 para ver que $m_r(X_{i_1}, X_{j_1}, \ldots, \widehat{X_{j_k}}) = m'_r(X_{i_1}, X_{j_1}, \ldots, \widehat{X_{j_k}})$ se e somente se $m_r = m'_r$. Desta forma se $f = \sum \alpha_{ij}m_i^j$ ($\alpha_{ij} \in \mathbb{C}$ e $m_i^j \in B$ é do tipo m_i) aniquila o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$, então $\sum \alpha_{i1}M_1^j = \sum \alpha_{i2}M_2^j = \sum \alpha_{i3}M_3^j = \sum \alpha_{i4}M_4^j = 0$, com M_i^j é a avaliação de m_i^j nas matrizes X_i. Como as variáveis são algebricamente independentes, segue que $\alpha_{ij} = 0$ para quaisquer i, j. □

Teorema 3.9. *Seja $G = \mathbb{Z}_n$, $n \geqslant 3$. As identidades do Lema 3.6 formam uma base de G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

Demonstração. Consequência imediata dos Lemas 3.7 e 3.8. □

3.2 Identidades fracas com ação de D_n

Suponha agora que $G = D_n = \langle g, h |\, g^n = h^2 = 1, hgh = g^{-1}\rangle$, $n \geqslant 3$. Analogamente ao que foi feito para o grupo cíclico, recorrendo ao Lema 3.3 (ou Lema 9 de [6]), podemos supor que g e h agem assim:

$$g\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a & \omega^{-1}b \\ \omega c & -a \end{pmatrix}, \quad h\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} -a & c \\ b & a \end{pmatrix}.$$

É bem conhecido, ver [48], que neste caso o grupo possui apenas representações irredutíveis de grau 1 e 2, mais precisamente se $n = 2m$ e e_i é como antes, então a álgebra de grupo $\mathbb{C}[G]$ decompõe-se em uma soma direta de cópias de $\mathbb{C}$ e $M_2(\mathbb{C})$ da seguinte maneira:

- 4 cópias de $\mathbb{C}$, cada uma gerada por:
  (a) $(1/2)(1+h)e_0$,
  (b) $(1/2)(1-h)e_0$,
  (c) $(1/2)(1-h)(1+e_0)$,
  (d) $(1/2)(1+h)(1-e_0)$,
- $m-1$ cópias de $M_2(\mathbb{C})$ geradas por: $e_{\pm i}$, $he_{\pm i}$, $i \geqslant 1$.

Por outro lado se $n = 2m+1$, então $\mathbb{C}[G]$ possui:

- 2 cópias de $\mathbb{C}$ geradas por:
  (a) $(1/2)(1+h)e_0$,
  (b) $(1/2)(1-h)e_0$,
- m cópias de $M_2(\mathbb{C})$ geradas por: $e_{\pm i}$, $he_{\pm i}$, $i \geqslant 1$.

Um cálculo direto mostra que e_i (e portanto he_i) aniquilam $sl_2(\mathbb{C})$ se $i \neq 0$, 1, $n-1$. Como no caso do grupo cíclico, escreveremos e_{-1} no lugar de e_{n-1}.

Lema 3.10. *Seja $G = D_n$, $n \geqslant 3$ e $\alpha = \pm 1$. As seguintes relações são G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$:*

1. $(1+h)e_0(x) = 0$,
2. $e_0(x_1)f(x_2) + f(x_2)e_0(x_1) = 0$, *com* $f \in \{e_\alpha, he_\alpha\}$,
3. $e_0(x) + e_1(x) + e_{-1}(x) = x$,
4. $[e_0(x_1), e_0(x_2)] = 0$,

5. $f(x_1)f(x_2) = 0$, *onde* $f \in \{e_\alpha, he_\alpha\}$,

6. $f(x_1)g(x_2) = 0$, *onde o par* $(f, g) \in \{(e_\alpha, he_{-\alpha}), (he_\alpha, e_{-\alpha})\}$,

7. $f(x_1)x_2g(x_3) = f(x_3)x_2g(x_1)$, *onde* $f, g \in \{e_\alpha, he_\alpha\}$,

8. $e_\alpha(x_1)x_2he_{-\alpha}(x_3) = he_{-\alpha}(x_3)x_2e_\alpha(x_1)$,

9. $e_\alpha(x_1)e_{-\alpha}(x_2) = he_{-\alpha}(x_2)he_\alpha(x_1)$,

10. $e_\alpha(x_1)he_\alpha(x_2) = e_\alpha(x_2)he_\alpha(x_1)$.

Demonstração. A demonstração é imediata e consiste de avaliação direta. □

Veremos que estas identidades formam uma base de G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$ no caso em que $G = D_n$. Observe que esta não é uma base minimal, por exemplo, as identidades (9) e (10) são equivalentes; (7) e (8) o são, bem como (5) e (6). Resolvemos manter as identidades 6, 8 e 10 apenas para que os argumentos do Lema 3.11 fiquem mais transparentes.

Sejam I o G-ideal de identidades fracas gerado pelas identidades do Lema 3.10 e B o conjunto formado por todos os monômios do tipo $e_0(x)^{\underline{n}}\hat{u}$, onde $u = 1$ ou é um monômio em $\{e_{\pm 1}, he_{\pm 1}\}$ tal que:

($\mathcal{B}_1$) he_1 e he_{-1} não ocorrem simultaneamente,

($\mathcal{B}_2$) Cada he_α aparece apenas após os $e_{-\alpha}$,

($\mathcal{B}_3$) Cada e_α (respectivamente he_α) pode ser seguido imediatamente apenas por $e_{-\alpha}$ e he_α (respectivamente por e_α),

($\mathcal{B}_4$) Se $i \leqslant j$ e $f \in \{e_\alpha, he_\alpha\}$, então $f(x_i)$ vem antes de $f(x_j)$,

($\mathcal{B}_5$) Se $i < j$, então u não contém fatores do tipo $f(x_j)g(x_i)$ com $f, g \in \{e_\alpha, he_\alpha\}$.

Dadas as condições ($\mathcal{B}_1$)–($\mathcal{B}_5$), as únicas possibilidades para os monômios u (além de $u = 1$) são $u = u_1u_2$, com (u_1 e/ou u_2 podem ser iguais a 1):

- $u_1 = e_\alpha(x_{i_1})e_{-\alpha}(x_{j_1}) \cdots e_\alpha(x_{i_k})\widehat{e_{-\alpha}(x_{j_k})}$,
- $u_2 = he_\beta(x_{l_1})e_\beta(x_{l_2}) \cdots he_\beta(x_{l_{r-1}})\widehat{e_\beta(x_{l_r})}$.

Aqui $\beta = \alpha$ e $l_s = i_{k+s}$ se u_1 termina em $e_\alpha(x_{i_k})$, por outro lado $\beta = -\alpha$ e $l_s = j_{k+s}$ caso u_1 termine em $e_{-\alpha}(x_{j_k})$. Em qualquer caso tem-se também $i_1 \leqslant i_2 \leqslant \cdots$, $j_1 \leqslant j_2 \leqslant \cdots$.

Lema 3.11. *Seja B como acima. Então*

$$\mathbb{C}\langle X; G\rangle / I = \langle \{m + I | \, m \in B\} \rangle$$

Demonstração. Por analogia com o que foi feito no caso do grupo cíclico, temos $x^{g^j} = e_0(x) + \omega^j e_1(x) + \omega^{-j} e_{-1}(x)$. Além disso $e_0(x) = -he_0(x)$ módulo I o que nos dá a identidade

$$x^h = he_0(x) + he_1(x) + he_{-1}(x) = -e_0(x) + he_1(x) + he_{-1}(x).$$

Desta forma cada G-monômio pode ser escrito como uma combinação linear de monômios em $e_0(x_j)$, $e_\alpha(x_j)$ e $he_\alpha(x_j)$, módulo I. Agora, seja $m = m' he_\alpha(x_1) Y he_{-\alpha}(x_2) m'' \notin I$ de modo que na escrita de Y não ocorrem he_1 e nem he_{-1}. Se Y é uma expressão vazia, usando a identidade (9) do Lema 3.10, podemos escrever m na forma $m = m' e_{-\alpha}(x_2) e_\alpha(x_1) m''$. Caso contrário, pelas identidades (5) e (6), Y deve ter a forma $Y = e_\alpha(y_1) e_{-\alpha}(y_2) \cdots e_\alpha(y_{k-1}) e_{-\alpha}(y_k)$. Usando as identidades (8) e (9) sucessivamente obtemos

$$\begin{aligned} m &= m' he_\alpha(x_1)(e_\alpha(y_1) e_{-\alpha}(y_2) \cdots e_\alpha(y_{k-1}) e_{-\alpha}(y_k)) he_{-\alpha}(x_2) m'' \\ &\overset{(8)}{=} m' he_\alpha(x_1) he_{-\alpha}(x_2) Y' m'' \\ &\overset{(9)}{=} m' e_{-\alpha}(x_2) e_\alpha(x_1) Y' m'', \end{aligned}$$

módulo I, sendo Y' um monômio em $e_{\pm 1}$. Continuando com esse procedimento obteremos $(\mathcal{B}_1)$. Suponha que m tenha a forma

$$m = m_1' he_\alpha(x_1) Y e_{-\alpha}(x_2) m_2''$$

com he_α o mais próximo possível de $e_{-\alpha}(x_2)$ (e que satisfaça $\mathcal{B}_1$), ou seja, que tenhamos na escrita de m algum elemento $e_{-\alpha}$ à direita de algum he_α. Das identidades (6) e (8) e do fato que $m \notin I$, obtemos que $Y e_{-\alpha}(x_2) = e_\alpha(y_1) e_{-\alpha}(y_2) \cdots e_{-\alpha}(y_{k-1}) e_\alpha(y_k) e_{-\alpha}(x_2)$, e

$$m = m_1' Y' e_{-\alpha}(x_2) e_\alpha(y_k) he_\alpha(x_1) m_2''$$

módulo I. Aqui Y' é um monômio nos $e_{\pm 1}$. Isso nos permite supor, sem interferirmos em $\mathcal{B}_1$, que na escrita de m cada he_α ocorre apenas após todos os $e_{-\alpha}$. Com isso, btemos $(\mathcal{B}_1)$–$(\mathcal{B}_2)$. Pelas identidades (5) e (6) já temos:

$$\begin{aligned} e_\alpha(x_1) e_\alpha(x_2) &= 0, \\ e_\alpha(x_1) he_{-\alpha}(x_2) &= 0, \\ he_\alpha(x_1) he_\alpha(x_2) &= 0, \\ he_\alpha(x_1) e_{-\alpha}(x_2) &= 0, \end{aligned}$$

e, pela primeira parte da demonstração, eliminamos ocorrências da forma $he_\alpha(x_1)he_{-\alpha}(x_2)$. Logo, cada monômio $m \notin I$ pode ser escrito módulo I como um produto de $e_0(x_i)$, $e_\alpha(x_i)$ e $he_\alpha(x_i)$ onde cada e_α é seguido imediatamente apenas por $e_{-\alpha}$ ou he_α, enquanto que he_α é seguido imediatamente apenas por e_α. Além disso, he_1 e he_{-1} não ocorrem simultaneamente. Com isso, as condições $(\mathcal{B}_1)$–$(\mathcal{B}_3)$ estão mantidas. Sejam $f, g \in \{e_\alpha, he_\alpha\}$ e suponha que em m aparecem elementos do mesmo tipo (e_α ou he_α). Assim, m tem a forma $m = m_2' f(x_i) m_2'' f(x_j) m_3$. Escolha $f(x_i)$ e $f(x_j)$ de modo que em m_2'' não ocorra elemento do tipo f. Se $f = e_\alpha$, então das propriedades $(\mathcal{B}_1)$–$(\mathcal{B}_3)$ e da identidade (6) segue que $m_2'' \in \{e_{-\alpha}(y_1), he_\alpha(y_1)\}$. Por outro lado se $f = he_\alpha$, novamente de $(\mathcal{B}_1)$–$(\mathcal{B}_3)$ e (6) obteremos $m_2'' = e_\alpha(y_1)$. Em qualquer caso $m = m_2' f(x_j) m_2'' f(x_i) m_3$ módulo I (identidade (7)), e isso nos dá $(\mathcal{B}_1)$-$(\mathcal{B}_4)$. Se $m = m_3' f(x_j) g(x_i) m_3''$, a identidade (10) nos permite escrever $m = m_3' f(x_i) g(x_j) m_3''$ módulo I, portanto as condições $(\mathcal{B}_1)$–$(\mathcal{B}_5)$ são satisfeitas. Por fim, todos os e_0 podem ser colocados à esquerda de cada monônio devido à identidade (2) e as variáves x_i dos elementos da forma $e_0(x_i)$ podem ser colocadas em ordem crescente (identidade (4)). Isso conclui a prova. $\square$

Lema 3.12. *Nenhuma combinação linear não trivial dos elementos de B é uma G-identidade para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

Demonstração. Considere matrizes genéricas $X_i = a_i(e_{11} - e_{22}) + b_i e_{12} + c_i e_{21}$ e uma combinação linear f de elementos de B, digamos $f = \sum_{\underline{n}} e_0(x)^{\underline{n}} u_{\underline{n}}$, sendo $e_0(x)^{\underline{n}}$ dois a dois distintos. Então, cada $u_{\underline{n}}$ tem a forma

$$u_{\underline{n}} = \sum_{i,j=1}^{2} \sum_k \alpha_{ij}^k(\underline{n}) u(\underline{n})_{ij}^k,$$

com $u(\underline{n})_{ij}^k \in B$, $\alpha(\underline{n})_{ij}^k \in \mathbb{C}$, $u(\underline{n})_{ij}^k(X_1, \ldots, X_m) = g(\underline{n})_{ij}^k e_{ij}$ com $g(\underline{n})_{ij}^k \in \mathbb{C}[b_i, c_i | i \geqslant 1]$. A avaliação de $e_0(x)^{\underline{n}}$ nas matrizes $X_1, \ldots, X_m$ resulta em uma matriz da forma $m(\underline{n})(e_{11} \pm e_{22})$, com $m(\underline{n}) = a_1^{n_1} \cdots a_k^{n_k}$. Assim,

$$\begin{aligned} f(X_1, \ldots, X_m) &= \sum_{\underline{n}} m(\underline{n})(e_{11} \pm e_{22})\Big(\sum_{i,j=1}^{2} \sum_k \alpha_{ij}^k(\underline{n}) u(\underline{n})_{ij}^k(X_1, \ldots, X_m)\Big) \\ &= \sum_{\underline{n}} m(\underline{n}) \begin{pmatrix} \sum_k \alpha_{11}^k(\underline{n}) g(\underline{n})_{11}^k & \sum_k \alpha_{12}^k(\underline{n}) g(\underline{n})_{12}^k \\ \pm \sum_k \alpha_{21}^k(\underline{n}) g(\underline{n})_{21}^k & \pm \sum_k \alpha_{22}^k(\underline{n}) g(\underline{n})_{22}^k \end{pmatrix}. \end{aligned}$$

Devido à ordem imposta aos a_i's podemos recuperar cada $e_0(x)^{\underline{n}}$ a partir de sua avaliação nas matrizes genéricas, ou seja,

$$e_0(x)^{\underline{n}} = e_0(x)^{\underline{n'}} \Leftrightarrow m(\underline{n}) = m(\underline{n'}).$$

Como os a_i, b_i e c_i são algebricamente independentes, teremos

$$\sum_k \alpha_{ij}^k(\underline{n}) g(\underline{n})_{ij}^k = 0,$$

se $f(X_1, \ldots, X_m) = 0$. Assim tudo que precisamos fazer é verificar se são linearmente independentes os elementos $u \in B$ que avaliados nas matrizes genéricas resultam em múltiplos da mesma matriz elementar e_{ij}. Escreva $u = u_1u_2$ e denote a avaliação de u nas matrizes X_i por $\overline{u}$. Note que as únicas maneiras de se obter um múltiplo de uma matriz elementar e_{ij} são as seguintes:

(e_{11}):

a) $u_1 = 1,$
$u_2 = he_1(x_{i_1})e_1(x_{i_2}) \cdots he_1(x_{i_{r-1}})e_1(x_{i_r}),$
$\overline{u} = c_{i_1}c_{i_2} \cdots c_{i_{r-1}}c_{i_r}e_{11},$

b) $u_1 = e_{-1}(x_{i_1})e_1(x_{j_1}) \cdots e_1(x_{j_{k-1}})e_{-1}(x_{i_k}),$
$u_2 = he_{-1}(x_{i_{k+1}})e_{-1}(x_{i_{k+2}}) \cdots he_{-1}(x_{i_{k+r-1}}),$
$\overline{u} = b_{i_1}b_{i_2} \cdots b_{i_{k+r-1}}c_{j_1}c_{j_2} \cdots c_{j_{k-1}}e_{11},$

c) $u_1 = e_{-1}(x_{i_1})e_1(x_{j_1}) \cdots e_{-1}(x_{i_k})e_1(x_{j_k})$
$u_2 = 1$
$\overline{u} = b_{i_1}b_{i_2} \cdots b_{i_k}c_{j_1}c_{j_2} \cdots c_{j_k}e_{11},$

d) $u_1 = e_{-1}(x_{i_1})e_1(x_{j_1}) \cdots e_{-1}(x_{i_k})e_1(x_{j_k}),$
$u_2 = he_1(x_{j_{k+1}})e_1(x_{j_{k+2}}) \cdots he_1(x_{j_{k+r-1}})e_1(x_{j_{k+r}}),$
$\overline{u} = b_{i_1}b_{i_2} \cdots b_{i_k}c_{j_1}c_{j_2} \cdots c_{j_{k+r-1}}c_{j_{k+r}}e_{11},$

(e_{12}):

a) $u_1 = 1,$
$u_2 = he_1(x_{i_1})e_1(x_{i_2}) \cdots he_1(x_{i_r}),$
$\overline{u} = c_{i_1}c_{i_2} \cdots c_{i_r}e_{12},$

b) $u_1 = e_{-1}(x_{i_1})e_1(x_{j_1}) \cdots e_1(x_{j_{k-1}})e_{-1}(x_{i_k}),$
$u_2 = 1,$
$\overline{u} = b_{i_1}b_{i_2} \cdots b_{i_k}c_{j_1}c_{j_2} \cdots c_{j_{k-1}}e_{12},$

c) $u_1 = e_{-1}(x_{i_1})e_1(x_{j_1}) \cdots e_{-1}(x_{i_k})e_1(x_{j_k}),$
$u_2 = he_1(x_{j_{k+1}})e_1(x_{j_{k+2}}) \cdots he_1(x_{j_{k+r}}),$
$\overline{u} = b_{i_1}b_{i_2} \cdots b_{i_k}c_{j_1}c_{j_2} \cdots c_{j_{k+r}}e_{12},$

d) $u_1 = e_{-1}(x_{i_1})e_1(x_{j_1}) \cdots e_1(x_{j_{k-1}})e_{-1}(x_{i_k}),$
$u_2 = he_{-1}(x_{i_{k+1}})e_{-1}(x_{i_{k+2}}) \cdots he_{-1}(x_{i_{k+r-1}})e_{-1}(x_{i_{k+r}}),$
$\overline{u} = b_{i_1} \cdots b_{i_{k+r}}c_{j_1} \cdots c_{j_{k-1}}e_{12},$

(e_{21}):

a) $u_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_{-1}(x_{j_{k-1}})e_1(x_{i_k})$,
$u_2 = 1$,
$\overline{u} = c_{i_1}c_{i_2}\cdots c_{i_k}b_{j_1}b_{j_2}\cdots b_{j_{k-1}}e_{21}$,

b) $u_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_{-1}(x_{j_{k-1}})e_1(x_{i_k})$,
$u_2 = he_1(x_{i_{k+1}})e_1(x_{i_{k+2}})\cdots he_1(x_{i_{k+r-1}})e_1(x_{i_{k+r}})$,
$\overline{u} = c_{i_1}c_{i_2}\cdots c_{i_{k+r-1}}c_{i_{k+r}}b_{j_1}b_{j_2}\cdots b_{j_{k-1}}e_{21}$,

c) $u_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_1(x_{i_k})e_{-1}(x_{j_k})$,
$u_2 = he_{-1}(x_{j_{k+1}})e_{-1}(x_{j_{k+2}})\cdots he_{-1}(x_{j_{k+r}})$,
$\overline{u} = c_{i_1}c_{i_2}\cdots c_{i_k}b_{j_1}b_{j_2}\cdots b_{j_{k+r}}e_{21}$,

d) $u_1 = 1$,
$u_2 = he_{-1}(x_{i_1})e_{-1}(x_{i_2})\cdots he_{-1}(x_{i_r})$,
$\overline{u} = b_{i_1}b_{i_2}\cdots b_{i_r}e_{21}$,

(e_{22}):

a) $u_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_{-1}(x_{j_{k-1}})e_1(x_{i_k})$,
$u_2 = he_1(x_{i_{k+1}})e_1(x_{i_{k+2}})\cdots he_1(x_{i_{k+r-1}})$,
$\overline{u} = c_{i_1}c_{i_2}\cdots c_{i_{k+r-1}}b_{j_1}b_{j_2}\cdots b_{j_{k-1}}e_{22}$,

b) $u_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_1(x_{i_k})e_{-1}(x_{j_k})$,
$u_2 = 1$,
$\overline{u} = c_{i_1}c_{i_2}\cdots c_{i_k}b_{j_1}b_{j_2}\cdots b_{j_k}e_{22}$,

c) $u_1 = e_1(x_{i_1})e_{-1}(x_{j_1})\cdots e_1(x_{i_k})e_{-1}(x_{j_k})$,
$u_2 = he_{-1}(x_{j_{k+1}})e_{-1}(x_{j_{k+2}})\cdots he_{-1}(x_{j_{k+r-1}})e_{-1}(x_{j_{k+r}})$,
$\overline{u} = c_{i_1}c_{i_2}\cdots c_{i_k}b_{j_1}b_{j_2}\cdots b_{j_{k+r}}e_{22}$,

d) $u_1 = 1$,
$u_2 = he_{-1}(x_{i_1})e_{-1}(x_{i_2})\cdots he_{-1}(x_{i_{r-1}})e_{-1}(x_{i_r})$,
$\overline{u} = b_{i_1}b_{i_2}\cdots b_{i_r}e_{22}$,

Em cada caso e_{ij}, observe que nenhuma relação entre G-monômios em (a), (b), (c) e (d) é possível. Para exemplificar, consideremos o caso (e_{11}). Temos 4 possibilidades: na primeira o grau total das variáveis $b's$ é zero, já na segunda o grau total das variáveis do tipo b é maior que o grau das variáveis do tipo c, na terceira os graus coincidem entre as variáveis dos tipo b e c, por fim, no quarto caso o grau total das variáveis do tipo c é maior que o grau total das variáveis b. Comportamento semelhante ocorre para cada matriz elementar e_{ij}, assim apenas precisamos verificar se são linearmente independentes os G-monômios dos tipos $(a), (b), (c)$ e (d) separadamente. Como as variáveis b_i, c_i, para $i \geqslant 1$, estão em ordem crescente, os monômios podem ser recuperados unicamente a partir de sua avaliação nas matrizes genéricas. Além disso as variáveis b_j e c_k são algebricamente independentes, assim nehuma relação entre eles é possível. □

Os Lemas 3.11 e 3.12 fornecem o próximo resultado.

Teorema 3.13. *Seja $G = D_n$. As identidades do Lema 3.10 formam uma base de G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

3.3 Identidades fracas com ação de A_4, A_5 e S_4

Suponha que $G = A_4, A_5$ ou S_4 é um grupo agindo em $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$. O seguinte resultado pode ser visto em [32, Lema 14] ou [6, Lema 12].

Lema 3.14. *Suponha que G age fielmente em $sl_2(\mathbb{C})$. Então, $sl_2(\mathbb{C})$ é um $\mathbb{C}G$-módulo irredutível.*

Os três casos são semelhantes e são tratados simultaneamente. Este mesmo comportamento ocorre no cálculo de identidades com ação para $M_2(\mathbb{C})$ e $sl_2(\mathbb{C})$. Como observado em [32], podemos então decompor $\mathbb{C}G$ em uma soma direta de um ideal J_0 que aniquila $sl_2(\mathbb{C})$ e uma cópia de $M_3(\mathbb{C})$. Sejam $v_1 = e_{11} - e_{22}$, $v_2 = e_{12}$ e $v_3 = e_{21}$. Como álgebra de transfomações lineares sobre o espaço $sl_2(\mathbb{C})$ de dimensão três, $M_3(\mathbb{C})$ tem base $\{\epsilon_{ij} \mid 1 \leqslant i, j \leqslant 3\}$ (a base canônica) a qual satisfaz $\epsilon_{ij}(v_k) = \delta_{jk} v_i$. Explicitamente, esta base age em $x = a(e_{11} - e_{22}) + be_{12} + ce_{21} \in sl_2(\mathbb{C})$ assim:

$$\epsilon_{11}(x) = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \quad \epsilon_{12}(x) = \begin{pmatrix} b & 0 \\ 0 & -b \end{pmatrix}, \quad \epsilon_{13}(x) = \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix},$$

$$\epsilon_{21}(x) = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \quad \epsilon_{22}(x) = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad \epsilon_{23}(x) = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix},$$

$$\epsilon_{31}(x) = \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}, \quad \epsilon_{32}(x) = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}, \quad \epsilon_{33}(x) = \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}.$$

Lema 3.15. *Seja $G = A_4$, A_5 ou S_4. As seguintes relações são G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$:*

1. $\epsilon_{11}(x) + \epsilon_{22}(x) + \epsilon_{33}(x) = x$,
2. $[\epsilon_{1\alpha}(x_1), \epsilon_{1\beta}(x_2)] = 0$, α, $\beta \in \{1, 2, 3\}$,
3. $\epsilon_{1\alpha}(x_1)$ *anticomuta com* $\epsilon_{ij}(x_2)$, $i = 2$, 3 *e* j, $\alpha \in \{1, 2, 3\}$,

4. $\epsilon_{i\alpha}(x_1)\epsilon_{j\beta}(x_2)\epsilon_{i\gamma}(x_3) = \epsilon_{1\alpha}(x_1)\epsilon_{1\beta}(x_2)\epsilon_{i\gamma}(x_3)$, *onde* $i,\ j = 2,\ 3\ (i \neq j)$ *e* $\alpha,\ \beta,\ \gamma = 1,\ 2,\ 3$,

5. $\epsilon_{i\alpha}(x_1)\epsilon_{i\beta}(x_2) = 0$, *para* $i = 2,\ 3$ *e* $\alpha,\ \beta \in \{1, 2, 3\}$,

6. $\epsilon_{3\alpha}(x_1)\epsilon_{2\beta}(x_2) + \epsilon_{2\beta}(x_2)\epsilon_{3\alpha}(x_1) = \epsilon_{1\alpha}(x_1)\epsilon_{1\beta}(x_2)$, *onde* $\alpha,\ \beta = 1,\ 2,\ 3$,

7. $\epsilon_{1\alpha}(x_1)\epsilon_{j\beta}(x_2) = \epsilon_{1\beta}(x_2)\epsilon_{j\alpha}(x_1)$, *com* $j \in \{2, 3\}$ *e* $\alpha,\ \beta \in \{1, 2, 3\}$,

8. $\epsilon_{2\alpha}(x_1)\epsilon_{3\beta}(x_2) = \epsilon_{2\beta}(x_2)\epsilon_{3\alpha}(x_1)$, *com* $\alpha,\ \beta \in \{1, 2, 3\}$.

Demonstração. A demonstração é imediata e consiste de avaliação direta em cada caso. □

Seja B o conjunto formado por todos os monômios da forma $u = u_1u_2$ tais que:

($\mathcal{B}_1$) $u_1 = \epsilon_{11}(x_1)^{l_1} \cdots \epsilon_{11}(x_k)^{l_k}\epsilon_{12}(x_1)^{m_1} \cdots \epsilon_{12}(x_k)^{m_k}\epsilon_{13}(x_1)^{n_1} \cdots \epsilon_{13}(x_k)^{n_k}$,

($\mathcal{B}_2$) $u_2 \in \{1, \epsilon_{2i}(x_\alpha), \epsilon_{3j}(x_\alpha), \epsilon_{2i}(x_\alpha)\epsilon_{3j}(x_\beta)\}$,

($\mathcal{B}_3$) Em u_2 se ocorre $\epsilon_{ij}(x_\alpha)$, $i \in \{2, 3\}$, então para cada $\epsilon_{1s}(x_p)$ na escrita de u_1 tem-se $s < j$ ou $s = j$ e $p \leqslant \alpha$,

($\mathcal{B}_4$) Em $u_2 = \epsilon_{2i}(x_\alpha)\epsilon_{3j}(x_\beta)$, tem-se $i < j$ ou $i = j$ e $\alpha \leqslant \beta$.

Lema 3.16. *Se I é o G-ideal fraco gerado pelas identidades do Lema 3.15, então*

$$\mathbb{C}\langle X; G\rangle/I = \langle\{u + I |\, u \in B\}\rangle.$$

Demonstração. Como $x = \sum \epsilon_{ii}(x)$ e $\{\epsilon_{ij} \mid 1 \leqslant i, j \leqslant 3\}$ gera um ideal bilateral de $\mathbb{C}G$, então cada G-monômio pode ser escrito (módulo I) como uma combinação linear de monômios em $\epsilon_{ij}(x_\alpha)$. Dado um tal monômio podemos colocar todos os termos $\epsilon_{1j}(x_k)$ à esquerda (identidade (3)), então o que restará à direita será um produto de fatores dos tipos $\epsilon_{2i}(x_\alpha)$ e $\epsilon_{3j}(x_\beta)$. Por outro lado, a identidade (5) elimina as ocorrências de fatores da forma $\epsilon_{ij}(x_\alpha)\epsilon_{ik}(x_\beta)$, $i \in \{2, 3\}$, assim os termos ϵ_{2j} e ϵ_{3k} aparecem alternadamente. Agora recorrendo às identidades (2), (3) e (4) sucessivamente poderemos escrever módulo I cada monômio $m \in \mathbb{C}\langle X; G\rangle \backslash I$ na forma $m = u_1u_2$, onde

- $u_1 = \epsilon_{11}(x_1)^{l_1} \cdots \epsilon_{11}(x_k)^{l_k}\epsilon_{12}(x_1)^{m_1} \cdots \epsilon_{12}(x_k)^{m_k}\epsilon_{13}(x_1)^{n_1} \cdots \epsilon_{13}(x_k)^{n_k}$,
- $u_2 \in \{1, \epsilon_{2i}(x_\alpha), \epsilon_{3j}(x_\alpha), \epsilon_{2i}(x_\alpha)\epsilon_{3j}(x_\beta), \epsilon_{3j}(x_\beta)\epsilon_{2i}(x_\alpha)\}$.

Usando a identidade (6) podemos enviar os elementos $\epsilon_{3i}(x_\alpha)$ para a direita dos $\epsilon_{2j}(x_\beta)$. Agora se $u_2 = \epsilon_{2j}(x_\alpha)$ ou $\epsilon_{3j}(x_\alpha)$ e $\epsilon_{1s}(x_p)$ ocorre em u_1 colocamos (caso necessário) estes dois fatores lado a lado (identidade (2)), depois permutamos o segundo índice por meio da identidade (7) e novamente usamos (2) para reordenar os fatores em u_1. Por outro lado, se $u = u_1 u_2$ com $u_2 = \epsilon_{2i}(x_\alpha)\epsilon_{3j}(x_\beta)$, realizamos o procedimento anterior para arrumar a primeira parcela de u_2. Escolha $\epsilon_{1p}(x_q)$ em u_1 com p o maior possível tal que $j \leqslant p$; agora escolha dentre estes fatores $\epsilon_{1p}(x_q)$ aquele com maior valor de q. Se não existe um tal p, então acabamos. Caso contrário, teremos três situações a considerar:

a) Se $j = p$ e $q = \beta$ nada precisa ser feito.

b) Se $j = p$ e $\beta < q$, troque x_β por x_q (identidades (2), (3) e (7)), obtendo: $u = \widetilde{u_1}\epsilon_{2i}(x_\alpha)\epsilon_{3p}(x_q)$ isso conclui o argumento, pois $p < i$ ou $i = p$ e $\beta < q \leqslant \alpha$ uma vez que $\epsilon_{2i}(x_\alpha)$ satisfaz $(\mathcal{B}_3)$.

c) Suponha $j < p$. Como em (b), troque j por p e x_β por x_q obtendo: $u = \widetilde{u_1}\epsilon_{2i}(x_\alpha)\epsilon_{3p}(x_q)$, assim $j < p \leqslant i$ e $\epsilon_{2i}(x_\alpha)$ continua satisfazendo $(\mathcal{B}_3)$.

Por fim, use a identidade (8) para obter $(\mathcal{B}_4)$. □

Antes de continuarmos fixemos algumas notações:

- $\underline{n} := (l_1, \ldots, l_k, m_1, \ldots, m_k, n_1, \ldots, n_k)$, $l_i, m_i, n_i \geqslant 0$,
- $u_1(x)^{\underline{n}} := \prod_{i=1}^{k} \epsilon_{11}(x_i)^{l_i} \prod_{i=1}^{k} \epsilon_{12}(x_i)^{m_i} \prod_{i=1}^{k} \epsilon_{13}(x_i)^{n_i}$,
- $U_1^{\underline{n}} := a_1^{l_1} \cdots a_k^{l_k} b_1^{m_1} \cdots b_k^{m_k} c_1^{n_1} \cdots c_k^{n_k}$,
- $U_2 := u_2(X_1, \ldots, X_k)$ a avaliação de u_2 nas matrizes genéricas $X_i = a_i(e_{11} - e_{22}) + b_i e_{12} + c_i e_{21}$.

Lema 3.17. *Nenhuma combinação linear não trivial dos elementos de B é uma G-identidade para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

Demonstração. Se $E_j^1 = a_j$, $E_j^2 = b_j$ e $E_j^3 = c_j$, então U_2 será I, $E_\alpha^i e_{12}$, $E_\alpha^i e_{21}$ ou $E_\alpha^i E_\beta^j e_{11}$ caso u_2 seja, respectivamente, $1, \epsilon_{2i}(x_\alpha), \epsilon_{3i}(x_\alpha)$ ou $\epsilon_{2i}(x_\alpha)\epsilon_{3j}(x_\beta)$. Defina a seguinte relação de ordem: $E_p^s < E_\alpha^j$ se $s < j$ ou $s = j$ e $p \leqslant \alpha$. Esta é a relação de ordem induzida pela ordem lexicográfica no conjunto dos pares (j, α) e apenas estabelece a seguinte ordem linear no conjunto $\{a_i, b_i, c_i \mid i \geqslant 1\}$:

$$a_i < a_{i+1} < b_j < b_{j+1} < c_k < c_{k+1},\ \forall i, j, k \geqslant 1.$$

Suponha que exista uma identidade da forma

$$f = \sum_{\underline{n}} \alpha_i u_1(x)^{\underline{n}} + \sum_{j,p,q,\underline{n}} \beta_i u_1(x)^{\underline{n}} u_{pq}^j(x),$$

onde u_{pq}^j denota os elementos $u_2 \in B$ tais que U_2 é um múltiplo da matriz elementar e_{pq}. Como as variáveis em $u_1 = u_1(x)^{\underline{n}}$ estão ordenadas, u_1 fica inteiramente determinado por sua avaliação nas matrizes genéricas. Além disso, quando avaliamos $\sum_{\underline{n}} \alpha_i u_1(x)^{\underline{n}}$ obtemos

$$\begin{pmatrix} \sum_{\underline{n}} \alpha_i U_1^{\underline{n}} & 0 \\ 0 & \pm \sum_{\underline{n}} \alpha_i U_1^{\underline{n}} \end{pmatrix}.$$

A entrada e_{22} não ocorre de outra maneira na avaliação de f, logo $\alpha_i = 0$, para todo $i \geqslant 1$ e tudo que precisamos fazer é mostrar que não existem identidades $f = \sum_{i,\underline{n}} \alpha_i u_1(x)^{\underline{n}} u_{pq}^i(x)$ com $(p,q) \in \{(1,2),(2,1),(1,1)\}$. Os três casos são semelhantes. Seja $u = u_1 u_2 \in \mathcal{B}$. Se $\epsilon_{1s}(x_p)$ ocorre em u_1 e $\epsilon_{ij}(x_\alpha)$ ocorre em u_2, então por $(\mathcal{B}_3)$ temos $s < j$ ou $s = j$ e $p \leqslant \alpha$, ou seja, $E_p^s < E_\alpha^j$. Escreva $u(X_1, \ldots, X_k) = \pm m_1 m_2 \widehat{m_3} e_{pq}$, onde m_2 e m_3 são as duas maiores variáveis ocorrendo em u. Agora note que pelo argumento anterior as váriáveis que ocorrem em U_2 serão maiores que aquelas que ocorrem em $U_1^{\underline{n}}$, logo $m_2 \widehat{m_3}$ corresponde a u_2 e m_1 corresponde a u_1. Analogamente, desta vez por $(\mathcal{B}_4)$, se $m_2 < m_3$, então m_2 e m_3 correspondem, respectivamente, à primeira e à segunda variável de u_2. Isso mostra que podemos recuperar os elementos $u \in \mathcal{B}$ a partir de sua avaliação. Como os a_i, b_i e c_i são algebricamente independentes, nenhuma combinação linear não trivial entre estes pode resultar em 0. □

Para ilustrar o que ocorre na demonstração acima, considere os seguintes exemplos.

Exemplo 3.18. *Suponha que após avaliação de u em matrizes genéricas tenhamos obtido*

$$u(X_1, \ldots, X_k) = \begin{pmatrix} 0 & a_1^2 b_{10} c_2 c_7 \\ 0 & 0 \end{pmatrix}.$$

Temos $u_2 = \epsilon_{2j}(x_\alpha)$, pois obtivemos um múltiplo de e_{12} (veja o início da demonstração). Além disso, $a_1 \leqslant a_1 \leqslant b_{10} \leqslant c_2 \leqslant c_7$. Como a_1, b_{10} e c_2 são menores que c_7, estas não podem ocorrer na avaliação de u_2, por $(\mathcal{B}_3)$. Logo $u_2 = \epsilon_{23}(x_7)$ e as demais variáveis surgem da avaliação de u_1, mas já vimos que u_1 é determinado unicamente por sua avaliação e, portanto, $u_1 = \epsilon_{11}(x_1)^2 \epsilon_{12}(x_{10}) \epsilon_{13}(x_2)$.

Exemplo 3.19. *Agora suponha que após avaliação de u em matrizes genéricas tenhamos obtido*

$$u(X_1, \ldots, X_k) = \begin{pmatrix} a_1^2 b_{10} c_2 c_7 & 0 \\ 0 & 0 \end{pmatrix},$$

então $u_2 = \epsilon_{2i}(x_\alpha)\epsilon_{3j}(x_\beta)$, pois obtivemos um múltiplo de e_{11}. Ordenando as variáveis, obtemos $a_1 \leqslant a_1 \leqslant b_{10} \leqslant c_2 \leqslant c_7$. Como a_1 e b_{10} são menores que c_2 estas não podem *ocorrer na avaliação de u_2. Além disso, uma vez que u_2 possui dois fatores, as únicas possibilidades são $u_2 = \epsilon_{23}(x_2)\epsilon_{33}(x_7)$ e $u_2 = \epsilon_{23}(x_7)\epsilon_{33}(x_2)$. A segunda não ocorre, por $(\mathcal{B}_4)$. Logo $u_2 = \epsilon_{23}(x_2)\epsilon_{33}(x_7)$ e $u_1 = \epsilon_{11}(x_1)^2\epsilon_{12}(x_{10})$.*

Os Lemas 3.16 e 3.17 fornecem o próximo resultado.

Teorema 3.20. *Seja $G = A_4$, A_5 ou S_4. As identidades do Lema 3.15 formam uma base de G-identidades para o par $(M_2(\mathbb{C}), sl_2(\mathbb{C}))$.*

Capítulo 4

Identidades de Laurent

4.1 Um breve histórico

Seja F um corpo, $X = \{x_1, x_2, \ldots\}$ um conjunto de símbolos, e denote por $\langle x_1, x_2, \ldots \rangle$ o grupo livre e livremente gerado por X. Seja $\mathcal{F}_L = F\langle x_1^{\pm 1}, x_2^{\pm 1}, \ldots \rangle$ a álgebra do grupo livre gerado por X, seus elementos são chamados de polinômios de Laurent (em variáveis não comutativas). Se A é uma F-álgebra associativa unitária, denotamos por $U(A)$ seu grupo de unidades (os elementos invertíveis). A álgebra $\mathcal{F}_L$ satisfaz a seguinte propriedade universal: dada qualquer álgebra associativa unitária A e qualquer função $\alpha\colon X \to U(A)$, existe um único homomorfismo de álgebras $\widehat{\alpha}\colon \mathcal{F}_L \to A$ que estende α. Dizemos que $f(x_1^{\pm 1}, \ldots, x_n^{\pm 1}) \in \mathcal{F}_L$ é uma identidade polinomial de Laurent (LPI) para A (ou para $U(A)$), se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_1, \ldots, a_n \in U(A)$. Claramente as identidades polinomiais de Laurent de A formam um ideal de $\mathcal{F}_L$ e uma identidade de grupo $w = 1$ é equivalente a uma LPI da forma $w - 1 = 0$. A álgebra $\mathcal{F}$, gerada por y_1 e y_2 sujeita às relações $y_1^2 = y_2^2 = 0$ desempenha um importante papel na teoria de LPI's. Mais geralmente, aparece no estudo das relações entre as identidades de grupo de um dado grupo G e as identidades polinomiais satisfeitas por sua álgebra de grupo FG. Neste capítulo, relacionamos as LPI's de $\mathcal{F}$ e as LPI's da álgebra das matrizes de ordem 2, $M_2(F)$. Segue dos nossos resultados que, se o corpo base F é infinito e quadraticamente fechado, então os ideais de LPI's dessas duas álgebras coincidem.

O estudo das relações entre identidades polinomiais satisfeitas por álgebras e identidades de grupo satisfeitas por seu grupo de unidades é bastante antigo e muitos autores têm dado atenção a este objeto. Vários resultados importantes foram obtidos. Por exemplo, em [7] Y. Billig, D. Riley e V. Tasić provaram que, se A é uma álgebra unitária nil-gerada sobre corpo infinito, então seu grupo de unidades $U(A)$ satisfaz uma identidade de grupo se, e somente se, A satisfaz uma identidade polinomial não matricial, ou seja, uma identidade polinomial não satisfeita pela álgebra das matrizes de ordem 2.

B. Hartley conjecturou por volta de 1980 que se G é um grupo de torção e o grupo de unidades $U(FG)$ de FG satisfaz uma identidade de grupo, então FG satisfaz uma identidade polinomial. Este fato foi provado em 1997 por A. Giambruno, S. Sehgal e A. Valenti [19] assumindo que o corpo F é infinito. Em 1999, Chia-Hsin Liu [38] provou a conjectura sem restrições sobre F e no ano seguinte [39], provou a conjectura para álgebras algébricas sobre corpos infinitos. Dois anos mais tarde, J. Z. Gonçalves e M. A. Dokuchaev [11] obtiveram uma versão da conjectura de Hartley para álgebras algébricas com identidades polinomiais de Laurent.

O lema seguinte, uma adaptação da Proposição 1 de [17], foi usada por Liu [38] e desempenha um papel importante no estudo de LPI's. Seja F_0 o subanel de F gerado por 1.

Lema 4.1. *Seja A uma álgebra sobre o corpo F e suponha que $U(A)$ satisfaz uma identidade de grupo $w = 1$. Então, existe um polinômio não nulo $f \in F_0[t]$, o anel de polinômios em uma variável, tal que $f(ab) = 0$ para quaisquer $a, b \in A$ satisfazendo $a^2 = b^2 = 0$.*

Em 2017 O. Broche, J. Gonçalves e Á. Del Río [8] estenderam a conjectura de Hartley (para álgebras de grupo), desta vez considerando identidades polinomiais de Laurent no lugar de identidades de grupo. Devemos notar que a demonstração do lema anterior não funciona bem para a maioria dos polinômios de Laurent. Os autores de [8] encontraram um interessante critério que permite escolher as "boas" identidades e, para estas identidades, conseguiram provar a conjectura. Seja g um polinômio não nulo em $F[t]$, a álgebra de polinômios em uma variável. Dizemos que a F-álgebra A tem a propriedade $\mathcal{P}_1$ com respeito a g se $g(ab) = 0$ para qualquer par de elementos $a, b \in A$ satisfazendo $a^2 = b^2 = 0$. Dizemos que um polinômio de Laurent f tem a propriedade $\mathcal{P}$ se qualquer álgebra A, para a qual f é uma identidade para $U(A)$, tem a propriedade $\mathcal{P}_1$ com respeito a algum polinômio $g \in F[t]$. O lema seguinte foi provado em [8]:

Lema 4.2. *Sejam $\mathcal{F} = F\langle y_1, y_2 \mid y_1^2 = y_2^2 = 0\rangle$ e f um polinômio de Laurent. São equivalentes:*

1) *f não é uma LPI para $U(\mathcal{F})$;*

2) *Existe um polinômio não nulo $g \in F[t]$ tal que qualquer F-álgebra A, para a qual f é uma LPI de $U(A)$, satisfaz a propriedadade $\mathcal{P}_1$ com respeito a g.*

Como observado por O. Broche, J. Gonçalves e Á. Del Río em [8], o grupo $U(\mathcal{F})$ não satisfaz identidade de grupo (este possui subgrupo livre não abeliano). Logo, o seguinte resultado obtido por eles generaliza a conjectura.

Teorema 4.3. *Seja F um corpo e G um grupo de torção. Se $U(FG)$ satisfaz uma LPI que não é LPI de $U(\mathcal{F})$, então FG satisfaz uma identidade polinomial.*

Após a confirmação da validade da conjectura por A. Giambruno, S. Sehgal e A. Valenti [19] em 1997, a póxima etapa seria descrever os grupos de torção G para os quais $U(FG)$ satisfaz identidade de grupo. No mesmo ano, D. S. Passman [42] obteve condições necessárias e suficientes para $U(FG)$ satisfazer identidade de grupo. Mais recentemente M. Ramezan-Nassab, M. H. Bien e M. Akbari-Sehat [43], considerando grupos sem torção G, forneceram algumas condições necessárias para $U(FG)$ satisfazer uma identidade polinomial de Laurent. Estas condições geralmente são dadas em termos de propriedades satisfeitas pelo grupo G. Mais uma vez, as identidades polinomiais de Laurent de $U(\mathcal{F})$ desempenharam um papel crucial.

4.2 Identidades de Laurent para $U(\mathcal{F})$

Se A é uma álgebra sobre F, denotamos por $Id_L(A) \subseteq \mathcal{F}_L$ o ideal de identidades de Laurent de $U(A)$. Nesta seção provamos que as identidades de $U(\mathcal{F})$ são identidades matriciais desde que o corpo seja infinito e quadraticamente fechado, ou seja, a equação $x^2 - a = 0$ possui solução em F para cada $a \in F$. Recordemos que um corpo algebricamente fechado é obviamente quadraticamente fechado, enquanto a recíproca falha. O subcorpo dos números complexos consistindo de todos os números construtíveis com régua e compasso sobre os racionais é quadraticamente fechado, mas não é algebricamente fechado (ver Teorema 1.7, página 223, de [37]).

Precisaremos dos seguintes subgrupos de $GL_2(F)$:

$$\begin{aligned} G_1 &= Z(GL_2(F)), \\ G_2 &= \{\lambda I + \beta e_{12} \mid \lambda, \beta \in F, \lambda \neq 0\}, \\ G_3 &= \{g \in GL_2(F) \mid \det(g) = k^2,\ k \in F^\times\}. \end{aligned}$$

Se A é uma álgebra gerada por a, $b \in A$ tais que $a^2 = b^2 = 0$, então existe um único homomorfismo de álgebras $\mathcal{C}_1 \colon \mathcal{F} \to A$ tal que $\mathcal{C}_1(y_1) = a$ e $\mathcal{C}_1(y_2) = b$. Seja $A = F\langle xe_{12}, ye_{21}\rangle \subseteq M_2(F[x,y])$, defina o homomorfismo $\mathcal{C}_1 \colon \mathcal{F} \to A$ por $\mathcal{C}_1(y_1) = xe_{12}$ e $\mathcal{C}_1(y_2) = ye_{21}$, e seja $\mathcal{C}_2 \colon F\langle xe_{12}, ye_{21}\rangle \to M_2(F)$ o homomorfismo definido por $\mathcal{C}_2(xe_{12}) = e_{12}$ e $\mathcal{C}_2(ye_{21}) = e_{21}$.

Se

$$f = \alpha + \sum_i \alpha_i (y_1y_2)^i y_1 + \sum_j \beta_j (y_1y_2)^j + \sum_k \gamma_k (y_2y_1)^k + \sum_l \delta_l (y_2y_1)^l y_2 \in \mathcal{F},$$

então

$$\mathcal{C}_1(f) = \begin{pmatrix} \alpha + \sum \beta_j x^j y^j & \sum \alpha_i x^{i+1} y^i \\ \sum \delta_l x^l y^{l+1} & \alpha + \sum \gamma_k x^k y^k \end{pmatrix}.$$

Claramente $\mathcal{C}_1$ é um isomorfismo e $\mathcal{C}_2$ é um epimorfismo. Assim $\mathcal{C}_1(f) \in U(M_2(F[x,y]))$ se, e somente se, $\det(\mathcal{C}_1(f)) \in U(F[x,y])$. Mas $\det(\mathcal{C}_1(f)) = \alpha^2 + g(x,y)$, com g não possuindo termo constante. Portanto, $\det(\mathcal{C}_1(f))$ é uma unidade se, e somente se, $g(x,y) = 0$ e $\alpha \neq 0$. Deste modo, se $B \in \mathcal{C}_1(\mathcal{F})$ é um elemento invertível, então $B^{-1} \in \mathcal{C}_1(\mathcal{F})$. Por outro lado, expandindo o determinante de B obtemos o polinômio:

$$h(x,y) = (\alpha + \sum \beta_j x^j y^j)(\alpha + \sum \gamma_k x^k y^k) - (\sum \alpha_i x^{i+1} y^i)(\sum \delta_l x^l y^{l+1}).$$

Além disso,

$$\det(\mathcal{C}_2 \circ \mathcal{C}_1(f)) = (\alpha + \sum \beta_j)(\alpha + \sum \gamma_k) - (\sum \alpha_i)(\sum \delta_l) = h(1,1).$$

Então, $\mathcal{C}_2 \circ \mathcal{C}_1(f)$ possui determinante quadrático para cada $f \in U(\mathcal{F})$, ou seja, $\mathcal{C}_2 \circ \mathcal{C}_1(U(\mathcal{F})) \subseteq G_3$.

Sejam A_1, $A_2 \in M_2(F)$ matrizes não nulas tais que $A_1^2 = A_2^2 = 0$ e $f\colon \mathcal{F} \to M_2(F)$ definido por $f(y_i) = A_i$. Como A_1 e $A_2 \in M_2(F)$ possuem quadrado nulo, existem matrizes invertíveis P_1 e P_2 tais que $A_1 = P_1 e_{12} P_1^{-1}$ e $A_2 = P_2 e_{21} P_2^{-1}$. Considere agora o automorfismo $\lambda\colon M_2(F) \to M_2(F)$ definido por $\lambda(m) = P_1^{-1} m P_1$. Então, $\lambda \circ f$ satisfaz $\lambda \circ f(U(\mathcal{F})) = P_1^{-1} f(U(\mathcal{F})) P_1 \cong f(U(\mathcal{F}))$. Além disso, $\lambda \circ f(y_1) = e_{12}$ e $\lambda \circ f(y_2) = N^{-1} e_{21} N$ com $N = P_1^{-1} P_2$. Portanto, para classificarmos as imagens homomorfas de $U(\mathcal{F})$, a menos de conjugação, precisamos considerar apenas os seguintes casos:

- $f(y_1) = f(y_2) = 0$;
- $f(y_1) = e_{12}, f(y_2) = \alpha e_{12}$, $\alpha \neq 0$;
- $f(y_1) = e_{12}$ e $f(y_2) = 0$;
- $f(y_1) = e_{12}$ e $f(y_2) = P e_{21} P^{-1}$, com $P = \alpha e_{11} + \beta e_{12} + \gamma e_{21} + \theta e_{22}$ é invertível.

Seja $V_f = span\{I, f(y_1), f(y_2)\}$. Verificaremos que $f(U(\mathcal{F})) \cong G_i$ onde $i = \dim V_f$. Se $\dim V_f = 1$, então I é uma base para V_f e, assim, $f(y_1) = f(y_2) = 0$ e obtemos que $f(U(\mathcal{F})) = G_1$.

Temos $\dim V_f = 2$ se, e somente se, $V_f = span\{I, e_{12}\}$. Então, $f(U(\mathcal{F})) = G_2$ neste caso. Se substituirmos y_1 por y_2 ou e_{12} por e_{21} obteremos grupos conjugados. Resta verificar o que acontece quando $\dim V_f = 3$. De agora em diante denotaremos por f_1 e f_2 os homomorfismos dados por:

$$f_1(y_1) = e_{12},\ f_1(y_2) = e_{21},$$

e

$$f_2(y_1) = e_{12},\ f_2(y_2) = P e_{21} P^{-1}.$$

Lema 4.4. *As seguintes afirmações são equivalentes:*

a) $\dim V_{f_2} = 3$*;*

b) $\theta \neq 0$*;*

c) f_2 *é sobrejetor;*

d) $P,\ P^{-1} \in Im_{f_2}$*;*

e) Existem $u,\ v \in \mathcal{F}$ *tal que* $f_1(g(y_1, y_2)) = f_2(g(y_1, uy_2v))$*, para qualquer* $g \in \mathcal{F}$*.*

Demonstração. Provemos que (a) e (b) são equivalentes. Se $\theta \neq 0$, temos as relações

$$\begin{aligned} e_{11} &= \theta^{-2}(\det(P)e_{12}Pe_{21}P^{-1} + \theta\beta e_{12}) \in Im_{f_2}, \\ e_{22} &= I - e_{11} \in Im_{f_2}, \\ e_{21} &= \theta^{-2}(\det(P)Pe_{21}P^{-1}e_{11} - \beta\theta e_{11}) \in Im_{f_2}. \end{aligned}$$

Por outro lado,

$$Pe_{21}P^{-1} = \det(P)^{-1}\begin{pmatrix} \alpha & \beta \\ \gamma & \theta \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \theta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \det(P)^{-1}\begin{pmatrix} \beta\theta & -\beta^2 \\ \theta^2 & -\beta\theta \end{pmatrix}.$$

Então se $\theta = 0$, teremos $f_2(\mathcal{F}) \subseteq span\{I, e_{12}\}$ e então f_2 não é sobrejetor. Note que $\dim V_{f_2} = 3$ garante $e_{21}P^{-1} \notin span\{I, e_{12}\}$ e este por sua vez fornece que $\theta \neq 0$. As demais equivalências são demonstradas de modo similar. ☐

Lema 4.5. *Se* $\dim V_{f_2} = 3$*, então* $f_2(U(\mathcal{F})) = f_1(U(\mathcal{F}))$*.*

Demonstração. Suponha que existam elementos não nulos w_1 e w_2 em $\mathcal{F}$ tais que:

$$w_1^2 = w_2^2 = 0,\ f_1(w_1) = f_2(y_2) \text{ e } f_2(w_2) = f_1(y_2).$$

Assim, dado $g(y_1, y_2) \in \mathcal{F}$ temos para quaisquer $j,\ k \in \{1, 2\}$:

$$\begin{aligned} f_k(g(y_1, y_2)) &= g(f_k(y_1), f_k(y_2)) \\ &= g(f_j(y_1), f_j(w_j)) \\ &= f_j(g(y_1, w_j)). \end{aligned}$$

Como $w_j^2 = 0$, existe um homomorfismo $\lambda_{w_j} : \mathcal{F} \to \mathcal{F}$ dado por $\lambda_{w_j}(y_1) = y_1$ e $\lambda_{w_j}(y_2) = w_j$. As igualdades acima nos dizem que $f_k = f_j \circ \lambda_{w_j}$. Então $f_k(U(\mathcal{F})) \subseteq f_j(U(\mathcal{F}))$, para cada j e k. Agora precisamos obter os elementos w_1 e w_2 acima. Seja $\lambda = \det(P)$ e considere os seguintes elementos

$$\begin{aligned} u &= a_1y_1 + a_2y_2 + a_3y_2y_1 + a_4y_1y_2, \\ v &= -a_1y_1 - a_2y_2 + a_4y_2y_1 + a_3y_1y_2, \\ w &= uy_2v. \end{aligned}$$

Então, $w^2 = 0$. Como $\dim V_{f_2} = 3$ temos $\theta \neq 0$ e, então, para cada a'_1, a'_2, a'_3, $a'_4 \in F$ a equação $f_2(u) = a'_1 e_{12} + a'_2 e_{21} + a'_3 e_{22} + a'_4 e_{11}$ tem uma solução dada por:

$$a_2 = \frac{a'_2}{\lambda^{-1}\theta^2}, \quad a_3 = \frac{a'_3 + a_2\lambda^{-1}\beta\theta}{\lambda^{-1}\theta^2}, \quad a_4 = \frac{a'_4 - a_2\lambda^{-1}\beta\theta}{\lambda^{-1}\theta^2}, \; a_1 = -\frac{a'_2\beta^2}{\theta^2} - \frac{a'_3\beta}{\theta} + \frac{a'_4\beta}{\theta} + a'_1.$$

Mais ainda, esta solução satisfaz

$$f_2(v) = -a'_1 e_{12} - a'_2 e_{21} + a'_4 e_{22} + a'_3 e_{11}.$$

Escolhendo os $a'_i s$ de modo que $f_2(u) = P^{-1}$ temos

$$f_2(\lambda u y_2 v) = P^{-1} P e_{21} P^{-1} P = e_{21} = f_1(y_2).$$

Então tomamos $w_2 = \lambda u y_2 v$. Seja

$$w_1 = \det(P)^{-1}(-\beta^2 y_1 y_2 y_1 + \theta^2 y_2 + \beta\theta y_1 y_2 - \beta\theta y_2 y_1).$$

Note que $w_1^2 = 0$ e

$$f_1(w_1) = \det(P)^{-1}\begin{pmatrix} \beta\theta & -\beta^2 \\ \theta^2 & -\beta\theta \end{pmatrix} = P e_{21} P^{-1} = f_2(y_2).$$

Isso mostra que $f_2(U(\mathcal{F})) = f_1(U(\mathcal{F}))$. □

Lema 4.6. $f_1(U(\mathcal{F})) = G_3$.

Demonstração. Seja

$$h = 1 + \alpha_{11}y_1 + \alpha_{22}^0 y_2 + \alpha_{22}^1 y_2 y_1 y_2 + \alpha_{12} y_1 y_2 + \alpha_{21} y_2 y_1,$$

com $\alpha_{12} = \alpha - 1$, $\alpha_{11} = \beta$, $\alpha_{21} = \theta - 1$, $\alpha_{22}^0 + \alpha_{22}^1 = \gamma$ e

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \theta \end{pmatrix}$$

é uma matriz com determinante 1 com $\beta \neq 0$. Agora, observemos que

$$\det(\mathcal{C}_1(h)) = 1 + (\alpha_{21} + \alpha_{12} - \alpha_{11}\alpha_{22}^0)xy + (\alpha_{21}\alpha_{12} - \alpha_{11}\alpha_{22}^1)x^2y^2$$

e

$$\frac{\theta + \alpha - 2}{\beta} = -\frac{(\alpha - 1)(\theta - 1) - \beta\gamma}{\beta} \text{ se, e somente se, } \det(A) = 1.$$

Seja $\alpha_{22}^0 = \beta^{-1}(\theta + \alpha - 2)$. Então

$$\alpha_{21} + \alpha_{12} - \alpha_{11}\alpha_{22}^0 = \alpha_{12}\alpha_{21} - \alpha_{11}\alpha_{22}^1 = 0,$$

ou seja, $h \in U(\mathcal{F})$. Além disso, $f_1(h) = A$. Suponha que $\beta = 0$ e note que, pelo que acabamos de ver, temos

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} \gamma & \theta \\ -\alpha & 0 \end{pmatrix} \in f_1(U(\mathcal{F})),$$

então

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \gamma & \theta \\ -\alpha & 0 \end{pmatrix} \in f_1(U(\mathcal{F})).$$

Deste modo, obtemos novamente que $A \in f_1(U(\mathcal{F}))$. Seja A uma matriz invertível com determinante $\det(A) = d^2$. Então, $\det(d^{-1}A) = 1$ e então existe $h \in U(\mathcal{F})$ tal que $f_1(dh) = A$. Isso mostra que $G_3 \subseteq f_1(U(\mathcal{F}))$. Como $f_1 = \mathcal{C}_2 \circ \mathcal{C}_1$, obtemos $f_1(U(\mathcal{F})) = \mathcal{C}_2 \circ \mathcal{C}_1(U(\mathcal{F})) \subseteq G_3$. Isso completa a prova. $\square$

Segue diretamente dos lemas anteriores:

Lema 4.7. *Sejam A_1, $A_2 \in M_2(F)$ matrizes de quadrado zero e $f\colon \mathcal{F} \to M_2(F)$ o homomorfismo dado por $f(y_i) = A_i$, $i = 1, 2$. Se $V_f = span\{I, A_1, A_2\}$. Então:*

(*a*) *Existe $P_f \in GL_2(F)$ (dependendo de f) tal que $f(U(\mathcal{F})) = PG_\delta P^{-1}$, com $\delta = \dim V_f$;*

(*b*) *f é um epimorfismo se, e somente se, $f(U(\mathcal{F})) = G_3$.*

Teorema 4.8. *Seja F um corpo. Então F é quadraticamente fechado se, e somente se, existe um homomorfismo $f\colon \mathcal{F} \to M_2(F)$ tal que $f(U(\mathcal{F})) = GL_2(F)$. Neste caso $Id_L(\mathcal{F}) \subseteq Id_L(M_2(F))$. Se um tal homomorfismo existe e além disso F é infinito, então*

$$Id_L(\mathcal{F}) = Id_L(M_2(F)).$$

Demonstração. A equivalência é imediata. Sejam $B_1, \ldots, B_n \in GL_2(F)$ e $u_1, \ldots, u_n \in U(\mathcal{F})$ tais que $f(u_i) = B_i$, para cada $i \geqslant 1$. Dado qualquer $g \in Id_L(\mathcal{F})$ temos

$$g(B_1, \ldots, B_n) = g(f(u_1), \ldots, f(u_n)) = f(g(u_1, \ldots, u_n)) = 0,$$

assim $Id_L(\mathcal{F}) \subseteq Id_L(M_2(F))$. Por outro lado, se existe uma identidade de Laurent g para $GL_2(F)$ que não é uma identidade para $U(\mathcal{F})$, então existem $u_1, \ldots, u_n \in U(\mathcal{F})$ tais que $g(u_1, \ldots, u_n) \neq 0$ em $\mathcal{F}$. Multiplicando $g(u_1, \ldots, u_n)$ no lado esquerdo (ou direito) por y_1 (e/ou por y_2), obteremos um polinômio não nulo h em uma variável de modo que

$$\widehat{y_i} g(u_1, \ldots, u_n) \widehat{y_j} = h(y_i y_j).$$

Mas aplicando o homomorfismo f_2 dado por $f_2(y_i) = \lambda e_{12}$ e $f_2(y_j) = e_{21}$, com $\lambda \in F$, à última expressão, obtém-se $h(\lambda e_{11}) = h(\lambda e_{12} e_{21}) = 0$ e, como o corpo é infinito, por um famoso argumento do determinante de Vandermonde e_{11} deveria ser nilpotente, o que é impossível. Então $Id_L(\mathcal{F}) = Id_L(M_2(F))$. $\square$

O conteúdo deste capítulo foi enviado para publicação em Archiv der Mathematik, o qual encontra-se em análise no momento.

Referências

[1] Aljadeff, E., and Kanel-Belov, A. Representability and Specht problem for G-graded algebras. *Advances in Mathematics 225*, 5 (2010), 2391–2428. Citado na página 14.

[2] Amitsur, A. S., and Levitzki, J. Minimal identities for algebras. *Proc. Amer. Math. Soc. 1*, 4 (1950), 449–463. Citado na página 19.

[3] Amitsur, S. A. Identities in rings with involutions. *Israel Journal of Mathematics 7* (1969), 63–68. Citado 2 vezes nas páginas 10 e 15.

[4] Belov, A. Y. On non-spechtian varieties. *Fundamental'naya i Prikladnaya Matematika 5* (1999), 47–66. Citado 2 vezes nas páginas 12 e 20.

[5] Belov, A. Y. Counterexamples to the specht problem (russian, with russian summary). *Mat. Sb 191* (2000), 13–24. Citado na página 20.

[6] Berele, A. Polynomial identities for 2 x 2 matrices with finite group actions. *J. Algebra 274* (2004), 202–214. Citado 7 vezes nas páginas 7, 8, 16, 31, 51, 55 e 61.

[7] Billig, Y., Riley, D., and Tasic, V. Nonmatrix varieties and nil-generated algebras whose units satisfy a group identity. *J. Algebra 190*, 1 (1997), 241–252. Citado na página 66.

[8] Broche, O., Gonçalves, J. Z., and del Río, Á. Group algebras whose units satisfy a laurent polynomial identity. *Arch. Math. (Basel) 4* (2018), 353–367. Citado 2 vezes nas páginas 16 e 67.

[9] Dehn, M. Über die grundlagen der projektiven geometrie und allgemeine zahlsysteme. *Mathematische Annalen 85* (1922), 184–194. Citado na página 10.

[10] Di Vincenzo, O. M. On the graded identities of $M_{1,1}(E)$. *Israel J. Math. 80*, 3 (1992), 323–335. Citado 4 vezes nas páginas 13, 14, 21 e 31.

[11] Dokuchaev, M., and Gonçalves, J. Z. Identities on units of algebraic algebras. *J. Algebra 250*, 2 (2002), 638–646. Citado na página 67.

[12] Drensky, V. A minimal basis of identities for a second-order matrix algebra over a field of characteristic 0. *Algebra and Logic 20* (1981), 188–194. Citado 2 vezes nas páginas 11 e 20.

[13] Drensky, V., and Formanek, E. *Polynomial Identity Rings*. Advanced Courses in Mathematics - CRM Barcelona. Springer, 2004. Citado na página 11.

[14] Formanek, E. Central polynomials for matrix rings. *J. Algebra 23* (1972), 129–132. Citado na página 14.

[15] Genov, G. K. A basis of identities of the algebra of third-order matrices over a finite field. *Algebra and Logic 20* (1981), 241–257. Citado na página 12.

[16] Genov, G. K., and Siderov, P. N. A basis for the identities of the algebra of fourth-order matrices over a finite field. II. *Serdica 8*, 4 (1982), 351–366. Citado na página 12.

[17] Giambruno, A., Jespers, E., and Valenti, A. Group identities on units of rings. *Archiv der Mathematik 63*, 4 (1994), 291–296. Citado na página 67.

[18] Giambruno, A., and Koshlukov, P. On the identities of the grassmann algebras in characteristic p $>$ 0. *Israel J. Math 122* (2001), 305–316. Citado na página 11.

[19] Giambruno, A., Sehgal, E., and Valenti, A. Group algebras whose units satisfy a group identity. *Proc. Amer. Math. Soc. 125*, 3 (1997), 629–634. Citado 2 vezes nas páginas 67 e 68.

[20] Giambruno, A., and Zaicev, M. *Polynomial Identities and Asymptotic Methods*. Mathematical surveys and monographs. American Mathematical Society, 2005. Citado 5 vezes nas páginas 18, 19, 26, 34 e 35.

[21] Grishin, A. V. Examples of t-spaces and t-ideals over a field of characteristic 2 without the finite basis property. *Fundamentalnaya i prikladnaya matematika 5*, 1 (1999), 101–118. Citado na página 12.

[22] Higman, G. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society 3*, 1 (1952), 326–336. Citado 2 vezes nas páginas 39 e 40.

[23] Kaplansky, I. Rings with a polynomial identity. *Bull. Amer. Math. Soc. 54* (1948), 575–580. Citado 2 vezes nas páginas 10 e 11.

[24] Kaplansky, I. "Problems in the theory of rings" revisited. *Amer. Math. Monthly 77* (1970), 445–454. Citado na página 14.

[25] Kemer, A. R. Varieties and $\mathbb{Z}_2$-graded algebras. *Mathematics of The Ussr-izvestiya 25* (1985), 359–374. Citado na página 14.

[26] Kemer, A. R. Finite basis property of identities of associative algebras. *Algebra and Logic 26* (1987), 362–397. Citado 2 vezes nas páginas 12 e 20.

[27] Klein, F. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade, English Translation: Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree.* Teubner, Leipzig, 1884; Dover, New York, 1956, revised ed, 1884; 1956. Citado na página 51.

[28] Koshlukov, P. Weak polynomial identities for the matrix algebra of order two. *J. Algebra 188* (1997), 610–625. Citado na página 15.

[29] Koshlukov, P. Basis of the identities of the matrix algebra of order two over a field of characteristic p $\neq$ 2. *J. Algebra. 241*, 1 (2001), 410–434. Citado 2 vezes nas páginas 11 e 20.

[30] Koshlukov, P., and Azevedo, S. S. Graded identities for t-prime algebras over fields of positive characteristic. *Israel Journal of Mathematics 128* (2002), 157–176. Citado 3 vezes nas páginas 13, 21 e 37.

[31] Koshlukov, P., and Krasilnikov, A. A basis for the graded identities of the pair $((M_2(K), gl_2(K)))$. *Serdica Mathematical Journal 38*, 1-3 (2012), 497–506. Citado 2 vezes nas páginas 15 e 37.

[32] Koshlukov, P., and Mortari, A. D. M. G-identities for the lie algebra $sl_2(\mathbb{C})$. *Journal of Pure and Applied Algebra 219* (2015), 2381–2395. Citado 5 vezes nas páginas 7, 8, 16, 31 e 61.

[33] Kostrikin, A. I. Introduction to algebra. *American Mathematical Monthly 91* (1982), 322. Citado na página 27.

[34] Krakowski, D., and Regev, A. The polynomial identities of the grassman algebra. *Trans. Amer. Math. Soc. 181* (1973), 429–438. Citado na página 11.

[35] Kruse, R. L. Identities satisfied by a finite ring. *J. Algebra. 26* (1973), 298–318. Citado na página 12.

[36] Lam, T.-Y. *A first course in noncommutative rings*, vol. 131. Springer, 1991. Citado 3 vezes nas páginas 23, 25 e 26.

[37] Lam, T.-Y. *Introduction to quadratic forms over fields*, vol. 67. American Mathematical Society Providence, RI, 2005. Citado na página 68.

[38] Liu, C.-H. Group algebras with units satisfying a group identity. *Proc. Amer. Math. Soc. 127*, 2 (1999), 327–336. Citado na página 67.

[39] Liu, C.-H. Some properties on rings with units satisfying a group identity. *J. Algebra 232*, 1 (2000), 226–235. Citado 2 vezes nas páginas 16 e 67.

[40] L'vov, I. V. Varieties of associative rings. i. *Algebra and Logic 12* (1973), 150–167. Citado na página 12.

[41] Mal'tsev, Y. N., and Kuzmin, E. N. A basis for identities of the algebra of second-order matrices over a finite field. *Algebra i Logika 17*, 1 (1978), 28–32, 121. Citado na página 12.

[42] Passman, D. S. Group algebras whose units satisfy a group identity. II. *Proc. Amer. Math. Soc. 125*, 3 (1997), 657–662. Citado na página 68.

[43] Ramezan-Nassab, M., Bien, M. H., and Akbari-Sehat, M. Algebras whose units satisfy a *-Laurent polynomial identity. *Archiv der Mathematik 117*, 6 (2021), 617–630. Citado na página 68.

[44] Razmyslov, J. P. On a problem of kaplansky. *Izvestiya: Mathematics 7*, 3 (June 1973), 479–496. Citado na página 14.

[45] Razmyslov, Y. P. Finite basing of the identities of a matrix algebra of second order over a field of characteristic zero. *Algebra and Logic 12* (1973), 47–63. Citado 3 vezes nas páginas 11, 14 e 15.

[46] Rezende, E. P. Identidades polinomiais graduadas de algumas álgebras matriciais. Tese (Doutorado). *Universidade de Brasília, Brasília* (2010). Citado 2 vezes nas páginas 39 e 41.

[47] Sehgal, S. K., and Zaicev, M. V. Graded identities of group algebras. *Communications in Algebra 30* (2002), 489 – 505. Citado na página 21.

[48] Serre, J.-P. *Linear Representations of Finite Groups*. Springer New York, 1977. Citado 2 vezes nas páginas 26 e 55.

[49] Shchigolev, V. Examples of infinitely based T-ideals. *Fundam. Prikl. Mat. 1* (1999), 307–312. Citado na página 12.

[50] Specht, W. Gesetze in Ringen. I. *Mathematische Zeitschrift 52* (1950), 557–589. Citado na página 12.

[51] Sviridova, I. Identities of pi-algebras graded by a finite abelian group. *Comm. Algebra.*, 9 (2011). Citado na página 14.

[52] Swan, R. G. Correction to "an application of graph theory to algebra". *Proc. Amer. Math. Soc. 21*, 2 (1969), 379–380. Citado na página 19.

[53] Vasilovsky, S. Y. $\mathbf{Z}_n$-graded polynomial identities of the full matrix algebra of order n. *Proc. Amer. Math. Soc. 127*, 12 (1999), 3517–3524. Citado na página 14.

[54] Wagner, W. Über die grundlagen der projektiven geometrie und allgemeine zahlensysteme. *Math. Ann. 113* (1937), 528–567. Citado na página 10.