UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

CLAUDEMIR FIDELES BEZERRA JUNIOR

Polinômios Centrais Graduados em Álgebras Associativas, e Mergulhos de Álgebras de Jordan

Campinas

2017

Claudemir Fideles Bezerra Junior

Polinômios Centrais Graduados em Álgebras Associativas, e Mergulhos de Álgebras de Jordan

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: Prof. Dr. Plamen Emilov Kochloukov

Coorientador: Prof. Dr. Diogo Diniz Pereira da Silva e Silva

Este exemplar corresponde à versão final da Tese defendida pelo aluno Claudemir Fideles Bezerra Junior e orientada pelo Prof. Dr. Plamen Emilov Kochloukov.

Campinas

2017

Agência(s) de fomento e nº(s) de processo(s): CAPES
ORCID: http://orcid.org/0000-0001-5107-5342

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

B469p

Bezerra Junior, Claudemir Fideles, 1987-
Polinômios centrais graduados em álgebras associativas, e mergulhos de álgebras de Jordan / Claudemir Fideles Bezerra Junior. – Campinas, SP : [s.n.], 2017.

Orientador: Plamen Emilov Kochloukov.
Coorientador: Diogo Diniz Pereira da Silva e Silva.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Álgebra não-comutativa. 2. PI-álgebras. 3. Polinômios. 4. Jordan, Álgebras de. I. Kochloukov, Plamen Emilov, 1958-. II. Silva, Diogo Diniz Pereira da Silva e. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Graded central polynomials in associative algebras, and embeddings of Jordan algebras
Palavras-chave em inglês:
Noncommutative algebras
PI-algebras
Polynomials
Jordan algebras
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Plamen Emilov Kochloukov [Orientador]
Lucio Centrone
Vyacheslav Futorny
Irina Sviridova
Victor Petrogradskiy
Data de defesa: 08-11-2017
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 08 de novembro de 2017 e aprovada pela banca examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). LUCIO CENTRONE

Prof(a). Dr(a). VYACHESLAV FUTORNY

Prof(a). Dr(a). IRINA SVIRIDOVA

Prof(a). Dr(a). VICTOR PETROGRADSKIY

As respectivas assinaturas dos membros encontram-se na Ata de defesa

À minha querida esposa Elis e a minha filha amada Laura, minha pequena guerreira.

Agradecimentos

Considerando este trabalho de tese como resultado de uma longa jornada que não começou no IMECC-UNICAMP, agradecer pode não ser tarefa fácil, nem justa. Para não correr o risco da injustiça, agradeço de antemão a todos que de alguma forma passaram pela minha vida e contribuíram para a construção de quem sou hoje. E agradeço explicitamente a alguns pela contribuição direta na construção deste trabalho:

À Deus, o que seria de mim sem a fé que eu tenho Nele.

À minha família. Em particular, a minha mãe (Dona Lia) e a meu pai (Seu Cal) que me auxiliaram na minha vida acadêmica, profissional, financeira e afetiva.

À minha querida esposa Elis, por estar sempre ao meu lado, nos momentos alegres e tristes, sempre me incentivando para a realização dos meus ideais e a minha filha amada Laura, a minha principal razão para persistir e prosseguir.

Aos amigos do IMECC pela convivência, ajudas e pelos momentos de distrações nestes três anos e meio de caminhada, em particular aos amigos Charles, Felipe, Luiz Henrique, Rondinei, Aline e Vladimir que me ajudaram a entender conceitos abstratos, me auxiliando nos estudos deste doutorado. Faço aqui um agradecimento especial ao meu irmão acadêmico e de coração Leomaques, uma das melhores pessoas que conheci nestes anos de IMECC pelas trocas de experiência na vida e pelo bom convívio e amizade. Com certeza é uma pessoa que quero ter como amigo pro resto da vida.

Aos professores do departamento de matemática da UNICAMP, aos funcionários da secretária da Pós-Graduação do IMECC, em especial ao professor Lucio Centrone pela disponibilidade de participar da composição da banca examinadora da tese, pela amizade e boa vontade de auxiliar com conversas dentro e fora do ambiente acadêmico.

Ao professor Diogo, só tenho que agradecer, por me aceitar como coorientando, por toda paciência, ajuda e disposição dedicada a mim, sempre acreditando e confiando em minhas habilidades e aptidões. Além disso, por ter sido companheiro no meu primeiro trabalho publicado como pesquisador em matemática, foi um amigo e excelente exemplo a ser admirado e seguido. Muito Obrigado!

Ao meu orientador Plamen pela excelente orientação, pelas sugestões de problemas, pelas discussões e conselhos que sempre foram muito proveitosos, além disso, não posso deixar de registrar o agradecimento pelas várias correções no texto, tudo isso foi essencial para a elaboração desta tese e para minha formação como cidadão. Professor, muito obrigado por tudo!

Aos professores que compuseram a banca examinadora da defesa de tese, professor Futorny, professor Victor e a professora Irina, pelas sugestões feitas a tese e pelas muitas correções e observações que certamente enriquecerá o nosso trabalho.

Ao departamento de matemática da UFCG por ter me acolhido e criarem um ambiente de trabalho que nos incentiva a buscar sempre a crescer, melhorar e “dar o máximo de si”. Em particular aos professores Jefferson, Marcelo e Brandão, e ao funcionário Renato por estarem sempre dispostos a ajudar na medida do possível.

E por fim, mas não menos importante, à CAPES pelo incentivo financeiro durante os dois primeiros anos de doutorado.

MUITÍSSIMO OBRIGADO A TODOS!

"Amanhã, talvez
Esse temporal saia do caminho
Dá pra escrever
O papel aceita toda qualquer coisa

Por hoje é só
Vou deixar passar a tempestade
Talvez amanhã
Água pura e toda verdade ."
(Depois da Curva - Humberto Gessinger)

Resumo

Neste trabalho apresentamos um estudo sobre identidades polinomiais e polinômios centrais graduados em álgebras associativas, bem como identidades com traço em álgebras não associativas. Mais precisamente estudamos uma propriedade de polinômios centrais graduados análoga à de $M_n(K)$, sobre um corpo infinito K de característica diferente de dois, estabelecida por Regev e determinamos em quais das graduações elementares com componente neutra comutativa e n-uplas distintas satisfazem tal propriedade, nomeando-a de graduação produto cruzado. Além disso consideremos $M_n(R)$, onde R admite uma graduação regular, de modo que $M_n(K)$ seja uma subálgebra homogênea. Fornecemos condições suficientes — satisfeitas por $M_n(E)$ com a sua graduação trivial — com o objetivo de provar que $M_n(R)$ herda a propriedade de primalidade de $M_n(K)$. Também provamos que as álgebras $M_{a,b}(E)$ satisfazem essa propriedade para polinômios centrais. Estes resultados foram publicados em [33]. Estudamos também as álgebras de divisão reais simples de dimensão finita graduadas por um grupos finito G, descrevendo uma base finita para o T_G-ideal das identidades graduadas e para o T_G-espaço dos polinômios centrais graduados para tais álgebras reais. Esses resultados estão no artigo [34] e estão aceitos para publicação. Por fim, considerando K um corpo de característica zero, provamos que uma álgebra de Jordan com traço pode ser mergulhada em uma álgebra de Jordan de um forma bilinear sobre uma álgebra comutativa e associativa C (denotada por $B_n(C)$) se, e somente se, ela satisfaz todas as identidades com traço da álgebra de Jordan $B_n(K)$. Esses resultados são novos, e serão submetidos para publicação.

Palavras-chave: álgebra verbalmente prima. polinômios centrais. identidade com traço.

Abstract

In this thesis we study graded polynomial identities and central polynomials in associative algebras, as well as trace identities for non-associative algebras. Namely we consider the primality property for $M_n(K)$, when K is an infinite field of characteristic different from 2, established by Regev. We determine, among the elementary gradings with commutative neutral component, the ones that satisfy this property, namely the crossed product gradings. Next we consider $M_n(R)$, where R admits a regular grading, equipped with a grading such that $M_n(K)$ is a homogeneous subalgebra. We provide sufficient conditions — satisfied by $M_n(E)$ with the trivial grading — to prove that $M_n(R)$ satisfies the primeness property whenever $M_n(K)$ does. We also prove that the algebras $M_{a,b}(E)$ satisfy this property for ordinary central polynomials. These results were published in [33]. We also study finite dimensional real algebras with a division grading by a finite abelian group G, and we provide finite basis for the T_G-ideal of graded identities and for the T_G-space of graded central polynomials for such real algebras. These results are contained in the article [34] and they are accepted for publication. Finally, over a field K of characteristic 0, we prove that a Jordan algebra J with trace can be realized as a Jordan algebra of a bilinear form over a commutative and associative algebra C (denoted by $B_n(C)$) if and only if it satisfies all trace identities of the Jordan algebra of a bilinear form $B_n(K)$. These results are new and will be submitted for publication.

Keywords: verbally prime algebras. central polynomials. trace identities.

Sumário

Introdução

A área da matemática na qual se insere esta tese é a álgebra, mais especificamente a teoria das Álgebras com Identidades Polinomiais, ou PI-teoria (do inglês *Polynomial Identities*) que é uma parte importante da teoria de anéis. Um polinômio $f(x_1,\ldots,x_n)$, nas variáveis não comutativas $x_1,\ldots,x_n$ e com coeficientes num corpo K, é uma identidade para a K-álgebra A se para quaisquer $a_1,\ldots,a_n \in A$ tem-se $f(a_1,\ldots,a_n) = 0$ em A. Se existir um polinômio $f \neq 0$ com esta propriedade para a álgebra A então A é chamada PI-álgebra, e f é uma identidade polinomial para A. A classe das PI-álgebras é ampla e engloba as álgebras comutativas, as de dimensão finita, as álgebras nil e as nilpotentes, entre outras. Além disso, o produto tensorial entre duas PI-álgebras, as subálgebras, as imagens homomórficas e o produto direto finito entre PI-álgebras são também álgebras com identidades polinomiais.

Atualmente esta teoria é uma área da álgebra bem desenvolvida e em expansão rápida. São três as principais linhas de pesquisa sobre PI-álgebras. A primeira (e a mais clássica) estuda as propriedades de uma álgebra (ou um anel) sabendo-se que ela satisfaz alguma identidade polinomial. Em outras palavras, "o que podemos dizer sobre a estrutura de PI-álgebra?". A segunda linha representa-se por pesquisas sobre as classes de álgebras que satisfazem um dado sistema de identidades polinomiais (essas classes são chamadas de variedades de álgebras). A terceira estuda as identidades polinomiais satisfeitas por uma álgebra "interessante". Gostaríamos de deixar claro que tal divisão não é única e definitiva, e que os problemas na PI-teoria, na maioria das vezes, estão interligados. Ainda mais, pesquisas em PI-teoria utilizam métodos e técnicas provenientes de outras áreas da Álgebra (estrutura de anéis, representações de álgebras, álgebras graduadas, ações de grupos, para citar algumas), da Combinatória, da teoria de representações de grupos (especialmente dos grupos simétrico e geral linear), da álgebra linear, da teoria de invariantes, e outras áreas da Matemática. Uma discussão mais detalhada sobre o desenvolvimento da PI-teoria pode ser encontrada, por exemplo, em [36, 39, 43, 82, 97].

O início do estudo dessa teoria deu-se por volta de 1930, com os trabalhos de Dehn [26] e Wagner [95]. Nesses trabalhos pioneiros aparecem, embora implícito, algumas identidades polinomiais para a álgebra das matrizes de ordem 2. De forma explicita, podemos destacar o trabalho de Kaplansky em 1948 no artigo [55] no qual demonstrou que qualquer PI-álgebra primitiva é central simples e de dimensão finita sobre seu centro; o resultado ficou conhecido como "O Teorema de Kaplansky". Naquele trabalho o autor introduziu o termo identidade polinomial. Dois anos mais tarde, em [6], Amitsur e Levitzki provaram, usando métodos puramente combinatórios, que o polinômio standard de grau $2k$ é uma identidade de grau mínimo para a álgebra das matrizes $k \times k$, um resultado clássico e de grande importância para o desenvolvimento da teoria das PI-álgebras. No mesmo ano Specht, em [89], levantou um problema que viria a ser conhecido como “O problema de Specht”, questionando se toda álgebra associativa, sobre um corpo de característica zero, possui base finita para o ideal de suas identidades polinomiais. Este passou a ser um problema central na teoria, motivando boa parte do seu desenvolvimento. O problema de Specht pode ser enunciado de outras maneiras equivalentes. Uma delas é se todo ideal de identidades polinomiais na álgebra associativa livre é finitamente gerado como ideal de identidades. Observamos que tal forma do problema de Specht se assemelha à propriedade Noetheriana da álgebra dos polinômios comutativos nas variáveis x_1, ..., x_n. Outra forma do problema de Specht é se toda cadeia ascendente de ideais de identidades estabiliza.

Em [57, 58], Kemer apresentou uma solução positiva para o problema proposto por Specht para as álgebras associativas em característica 0. Contudo não foi mostrado como determinar tal base finita para cada PI álgebra, e portanto o problema da descrição das identidades de uma dada álgebra associativa sobre um corpo de característica zero ainda está em aberto. Este último problema tem sido resolvido apenas para alguns casos particulares até o momento. Com a finalidade de resolver o problema de Specht, Kemer desenvolveu a estrutura dos ideais de identidades de álgebras associativas (chamados de T-ideais ou ideais verbais), em característica 0. Kemer relacionou o T-ideal de uma álgebra associativa com os T-ideais que satisfazem a condição: sempre que $f(x_1, \ldots, x_r)$ e $g(x_{r+1}, \ldots, x_s)$ são polinômios em conjuntos disjuntos de variáveis tais que $f \cdot g$ está no T-ideal então f ou g também está no T-ideal. Tais T-ideais são chamados de verbalmente primos (ou T-primos). Kemer mostrou ainda que os T-ideais T-primos não triviais são apenas os ideais de identidades das álgebras matriciais $M_n(K)$, e das álgebras $M_n(E)$ e $M_{a,b}(E)$. Esta última e uma subálgebra de $M_{a+b}(E)$ composta pelas matrizes em blocos $a \times a$ e $b \times b$ na diagonal, cujas entradas estão no centro de E, e as demais entradas estão na parte “anticomutativa” de E, aqui E é a álgebra de Grassmann de um espaço vetorial de dimensão infinita. Recordamos aqui que essas álgebras são obtidas, como sendo os respectivos envelopes de Grassmann, a partir da classificação das álgebras graduadas simples, graduadas pelo grupo cíclico de ordem 2. Tal classificação foi dada por C. T. C. Wall [96]. Recordamos ainda que o termo T-ideal *verbalmente primo* indica que os respectivos T-ideais são “primos” mas apenas dentro da classe dos T-ideais. É conhecido, que entre os T-ideais verbalmente primos apenas os T-ideais das álgebras $M_n(K)$ são primos.

Outro conceito que merece destaque na PI-teoria por sua estreita relação com as identidades polinomiais é o de polinômios centrais. Um polinômio $f(x_1, \ldots, x_n)$ é dito central para uma álgebra A se resulta em elemento do centro de A quando avaliado em quaisquer elementos dessa álgebra. Observe que as identidades polinomiais aparecem, junto com os polinômios constantes, como exemplos mais simples, e são chamados polinômios centrais triviais. Um dos problemas mais conhecidos da PI-teoria foi proposto por

Kaplansky em [56] e perguntava se existiam polinômios centrais não triviais (isto é, não identidades e sem termos constantes) para as álgebras matriciais $M_n(K)$. Recordamos que ainda na década de 30, foi observado que o polinômio $[x,y]^2$ sempre assume valores do centro da álgebra $M_2(K)$. O problema de Kaplansky foi resolvido de maneira afirmativa simultaneamente por Formanek [42] e Razmyslov [73], por volta de 1972–1973. A existência de polinômios centrais para $M_n(K)$ tornou-se um fator decisivo para o desenvolvimento da PI-teoria. Possibilitou ainda o uso de métodos da álgebra comutativa e da teoria de invariantes para a resolução de problemas de importância. A existência de polinômios centrais para as álgebras $M_n(E)$ e $M_{a,b}(E)$ foi demonstrada por Razmyslov em [76].

Os resultados de Formanek e de Razmyslov são construtivos. Eles exibiram polinômios centrais concretos para a álgebra $M_n(K)$. Por outro lado, pouco é conhecido sobre o conjunto dos polinômios centrais para as álgebras citadas acima. Claramente os polinômios centrais para alguma álgebra A, junto com as suas identidades polinomiais, formam um espaço vetorial, denotado por $C(A)$, na álgebra livre que chamaremos de espaço dos polinômios centrais. Este espaço vetorial é fechado por endomorfismos sendo chamados de T-espaços. A bem de verdade, $C(A)$ é fechado por produto, e deveríamos chamá-lo de T-subálgebra. Recordamos aqui que há exemplos de T-espaços que não formam conjunto dos polinômios centrais para nenhuma álgebra (basta escolher um espaço vetorial que é fechado por endomorfismos mas que não seja uma subálgebra).

Voltando aos T-espaços dos polinômios centrais para as álgebras T-primas, conhecem-se geradores desses em casos particulares. Em 2010, Brandão Jr., Koshlukov, Krasilnikov e Silva [21] explicitaram tais geradores para o caso da álgebra de Grassmann E quando o corpo base é infinito e de característica diferente de 2, e no caso de $M_2(K)$, Okhitin [67] exibiu o conjunto de geradores quando $char K = 0$; posteriormente Koshlukov e Colombo [23] generalizaram tal descrição para o caso do corpo ser infinito e de característica diferente de 2. Nos dois últimos casos, os resultados foram baseados no fato que são conhecidos geradores dos T-ideais das respectivas álgebras, ver [64] para a álgebra E, e [77, Seção 41, Capítulo V] para $M_2(K)$ sobre o corpo de característica zero e mais tarde, em [62], o resultado foi estendido para corpo infinito e de característica diferente de 2. Recordamos aqui que bases das identidades das álgebras T-primas, exceto as triviais e as mencionadas acima, são conhecidas apenas para $M_{1,1}(E)$ (em característica 0 somente, ver [69]), portanto não há grande expectativa de podermos encontrar descrições completas para os polinômios centrais das demais álgebras T-primas. Não é conhecido nem o grau mínimo de polinômios centrais para as álgebras $M_n(K)$ em característica 0, se $n \geqslant 4$.

Nas últimas décadas várias generalizações do conceito de identidade polinomial têm sido estudadas tais como: identidades polinomiais graduadas, identidade polinomiais com traço e identidades polinomiais com involução (ou $*$-identidades), sendo as duas primeiras objetos de estudo desta tese. Kemer utilizou identidades graduadas na sua teoria dos ideais de identidades em álgebras associativas (indicamos [59] para mais detalhes). As identidades com traço foram estudadas com detalhes por Procesi em [71], e por Razmyslov em [74]; como consequência dos resultados obtidos Razmyslov deu uma nova demonstração do Teorema de Amitsur e Levitzki. Já as identidades polinomiais com involução têm relação com as identidades polinomiais (ordinárias). Em [7], Amitsur demonstrou que uma álgebra satisfazendo uma identidade com involução é uma PI-álgebra.

Em [75], Razmyslov relacionou os polinômios centrais para as álgebras matriciais com as chamadas identidades fracas. Essas últimas são polinômios associativos que se anulam quando avaliados sobre o subespaço sl_n das matrizes de traço 0. As identidades fracas são ferramentas de importância no estudo das identidades em álgebras matriciais bem como em álgebras não associativas mas ainda não muito longe das associativas: álgebras de Lie, de Jordan, alternativas, entre outras. Ressaltamos que no mesmo trabalho Razmyslov determinou bases finitas para a álgebra de Lie $sl_2(K)$, bem como das identidades fracas do par $(M_2(K), sl_2(K))$ (tudo isso em característica 0). Podemos ainda citar a utilização das identidades fracas em álgebras matriciais para a construção de polinômios centrais nessas álgebras, veja [77, Seção 31, pág. 143]. Mais tarde, identidades fracas foram empregadas no estudo das identidades em álgebras não associativas. Em 1985, Iltyakov [45] estabeleceu a propriedade de base finita para a álgebra de Jordan de uma forma bilinear não degenerada simétrica num espaço vetorial de dimensão finita (em característica 0), denotado por $B_n(K) = K \oplus V_n$. Em 1989, Vasilovsky [92] determinou uma base para as identidades de $sl_2(K)$ no caso em que K é um corpo infinito qualquer de característica diferente de 2, e em 1991, de novo Vasilovsky [93] determinou bases explícitas para as identidades da álgebra de Jordan $B_n(K)$ (com algumas restrições sobre a característica do corpo). Em 1987-1991, Drensky e Koshlukov [37,38] e Koshlukov [61] estudaram a álgebra relativamente livre dessa álgebra de Jordan. Além disso, em 2011, Koshlukov e Diniz [63] descreveram uma base para as identidades polinomiais graduadas, por um grupo cíclico de ordem 2, novamente para a álgebra $B_n(K)$. Todos esses trabalhos fizeram uso sistemático de identidades fracas. Nos trabalhos de Vasilovsky foi utilizada a teoria de invariantes do grupo ortogonal. Mais tarde essas ideias foram desenvolvidas para a descrição de uma base finita das identidades de $M_2(K)$, sendo K um corpo infinito qualquer de característica diferente de 2, ver [62].

Podemos observar que descrições das identidades polinomiais satisfeitas por álgebras de importância são conhecidas em poucos casos. Já foi comentado que as identidades de álgebras (associativas) simples são conhecidas somente para as matrizes de ordem 2 (e ainda com restrições sobre a característica do corpo). Portanto estudam-se outros tipos de identidades polinomiais. Assim, as identidades com traço nas álgebras matriciais foram estudadas e descritas independentemente por Procesi (veja [71]) e Razmyslov (veja [74]). Esses estudos foram marcantes pois os métodos desenvolvidos por Procesi e por Razmyslov em suas abordagens ao problema, são de grande importância na teoria de anéis. Assim, Procesi começou o uso sistemático da teoria de invariantes em PI-álgebras, enquanto

Razmyslov utilizou o conceito de identidades fracas, bem como aprofundou as várias aplicações das representações do grupo simétrico. Posteriormente, em 1991, Vasilovisky [94] utilizou a teoria de invariantes do grupo ortogonal para descrever uma base para o T-ideal das identidades com traço nas álgebras de Jordan de uma forma bilinear.

Nesta tese trataremos, entre outras coisas, de invariantes, bem como propriedade dos polinômios centrais em álgebras T-primas, identidades com traço de álgebras não-associativas e descrição de base do T-espaço dos polinômios centrais graduados de algumas álgebras interessantes. A tese está organizada em quatro capítulos.

No primeiro capítulo serão introduzidos vários conceitos fundamentais para o desenvolvimento do trabalho. Decidimos incluir as principais definições e noções da PI-teoria para tornar a tese mais independente de outras fontes, mas para não exagerar muito no volume do trabalho, optamos por omitir várias demonstrações "canônicas" na PI-teoria. O leitor pode encontrar essas demonstrações nos livros [36, 39, 43, 50, 97]. Assim, introduzimos os conceitos de identidade polinomial, identidades multihomogêneas e multilineares, discutimos a questão da estrutura das álgebras de Jordan centrais simples de dimensão finita, bem como dos grupos algébricos lineares.

Já no segundo capítulo, faremos uso da propriedade de primalidade para polinômios centrais de $M_n(K)$ estabelecida por Regev [78] em 1979, ou seja, se o produto de dois polinômios em conjuntos disjuntos de variáveis é central, então cada um dos fatores é também central. Em 2015, Diniz [31] estabeleceu um resultado análogo ao Teorema de Regev, mas para as álgebras $M_n(E)$ e $M_{a,a}(E)$. Os resultados demonstrados aqui exigem que a característica do corpo seja zero. Um ano depois, Samoilov [83] provou a propriedade para o caso de álgebras verbalmente primas, porém os polinômios deveriam ser multilineares. A combinação desses resultados estabeleceu que, sobre um corpo de característica zero, toda álgebra T-prima satisfaz a propriedade de primalidade para polinômios centrais.

Considerando K um corpo infinito de característica diferente de 2, a Seção 2.2 do capítulo 2 dedica-se a estudar uma propriedade análoga à $M_n(K)$, mas agora para polinômios graduados. Determinaremos, dentro das classificações das graduações elementares com componente neutra comutativa e n-uplas distintas, as que satisfazem esta propriedade. Mais precisamente, no Teorema 2.2.10 nós provaremos que a álgebra $M_n(K)$ munida de tal graduação satisfaz a propriedade de primalidade para polinômios centrais graduados se, e somente se, a graduação é a graduação produto cruzado (ou seja, G tem ordem n) e existe um homomorfismo não trivial $G \to K^{\times}$; tal graduação foi introduzida por Aljadeff e Karasik em [3].

Além disso, os Teoremas 2.3.15 e 2.4.3, ambas no capítulo 2, estendem o Teorema de Regev para as álgebras $M_n(E)$ e $M_{a,b}(E)$. No caso de $M_n(E)$ mostramos um fato mais forte. Seja R uma álgebra graduada por um grupo abeliano H de modo que a graduação seja regular e considerando uma G-graduação de $M_n(R)$ de forma que $M_n(K)$ e R sejam subálgebras homogêneas com $R \subseteq (M_n(R))_\epsilon$, provaremos que a propriedade de primalidade transfere de $M_n(K)$ para $M_n(R)$. Como a álgebra de Grassmann E possui uma graduação regular temos que $M_n(E)$, munida da graduação trivial, satisfaz a propriedade de primalidade. Já no caso de $M_{a,b}(E)$ admitimos a sua graduação natural pelo grupo cíclico de ordem 2. A prova de que $M_{a,b}(E)$ admite a propriedade (ver Teorema 2.4.3) segue do fato de que se o produto de dois polinômios, f e g, em conjuntos disjuntos de variáveis é central para $M_{a,b}(E)$ então f sempre assume valores em $(M_{a,b}(E))_i$, para um i fixo entre 0 ou 1, ver Lema 2.4.2. Observamos que as álgebras $M_{a,b}(E)$ nem sempre satisfazem a propriedade de primalidade para polinômios centrais graduados. Em característica positiva, a descrição das álgebras verbalmente primas não é conhecida. Porém, sobre um corpo de característica zero, nossos resultados junto com o Teorema de Regev, mostram de modo alternativo ao que foi feito nos resultados anteriormente citados, que toda álgebra verbalmente prima satisfaz a primalidade para os seus polinômios centrais.

Em 2016, considerando R uma álgebra munida de uma graduação regular por um grupo abeliano finito H e o corpo base tendo característica zero, Diniz e de Melo [32] conseguiram extrair informações sobre o $T_{G\times H}$-ideal das identidades graduadas da álgebra $A \otimes_K R$, conhecendo as identidades G-graduados de A. No Capítulo 3, conseguirmos extrair informações análogas para o $T_{G\times H}$-espaço dos polinômios centrais graduadas de tais álgebras, veja Teorema 3.2.7.

Ainda no mesmo capítulo, conseguimos descrever bases para o espaço das identidades e polinômios centrais graduados para as álgebras de divisão graduadas simples e de dimensão finita sobre o corpo dos números reais. Em 2016, Bahturin e Zaicev [16], bem como Rodrigo–Escudero [81], classificaram tais álgebras. Mais geralmente, as álgebras de divisão graduadas reais de dimensão finita estão sendo atualmente estudadas e classificadas por Bahturin e Zaicev [17]. Considerando a relação estabelecida por Bahturin e Diniz em [14] entre algumas dessas álgebras graduadas com as álgebras regulares, temos como objetivo principal deste capítulo determinar uma base finita para o T_G-ideal das identidades graduadas e para o T_G-espaço dos polinômios centrais graduados para as álgebras de divisão graduadas classificadas em [16, 17, 81]. Para obter êxito, devemos aplicar o resultado principal para estas álgebras. Por outro lado, uma base para as álgebras com graduação de Pauli regular é conhecida (basta observar o trabalho de Aljadeff, Haile e Natapov [1]), porém nada é conhecido para as álgebras com graduações não regulares. Nosso Teorema 3.2.30 determina uma base para as identidades e polinômios centrais graduados nos casos da graduação de Pauli não regular e para a álgebra real $\mathcal{E}(\epsilon, 2^k)$ obteremos tal base no Corolário 3.3.4. Podemos observar que tais resultados são independentes da demonstração do resultado principal.

Por fim, é natural tentar estudar mergulhos de álgebra em algumas variedades.

Sabe-se há muito tempo que as PI-álgebras não precisam ser imersos em $M_n(C)$, a álgebra das matrizes de ordem n sobre um anel comutativo C, para algum n. No entanto, surgiram várias questões sobre se certas classes especiais de álgebras poderiam ser mergulhadas em álgebras de Matrizes. Uma condição óbvia é que tais álgebras precisam satisfazer todas as identidades de $M_n(K)$, mas esta condição não é suficiente. Em 1970–1971, Amitsur [8] e Small [88] produziram contra-exemplos para a última afirmação. Uma resposta completa para o problema de mergulho anterior não é conhecida, porém Procesi [72] demonstrou que o mergulho é válido na variedade das álgebras com traço que satisfazem a identidade de Cayley-Hamilton de grau n. Em 1990, Berele [19] obteve um resultado análogo para o caso das álgebras das matrizes com involução do primeiro tipo, ou seja, se uma álgebra com traço e involução satisfaz as mesmas $*$-identidades com traço das álgebras das matrizes de ordem n com involução (simplética ou transposta), então existe um mergulho preservando a aplicação traço e involução sobre a álgebra das matrizes com entradas em uma álgebra comutativa. Ambos os resultados estão relacionados à teoria dos grupos algébricos lineares e portanto considerar o corpo base sendo de característica zero é essencial.

Nosso objetivo principal no quarto capítulo é provar um resultado análogo ao demonstrado por Procesi e por Berele, mas para a álgebra de Jordan $B_n(K)$. Para este fim nós consideraremos uma álgebra central simples de dimensão finita, denotada por A, na classe das álgebras de Jordan com traço e o conjunto $Id_{Tr}(A)$ de todas as identidades com traço para a álgebra A. Tal conjunto é um T-ideal invariante por endomorfismo com traço sobre a álgebra livre com traço. Seja R uma álgebra de Jordan munida de um traço, dedicaremos a Seção 4.2 para demonstrar a existência de uma A-aplicação universal de R, tal resultado é similar ao demonstrado por Amitsur [9]. Considerando uma conjectura análoga à proposta por Iltyakov [46], alguns resultados conhecidos na teoria de álgebra de Jordan e grupos algébricos semissimples, obtemos o seguinte resultado: Se R satisfaz todas as identidades com traço de A, então existe uma álgebra comutativa e associativa S de modo que R possa ser mergulhada em $A \otimes_K S$ como K-álgebra. Como consequência da teoria dos invariantes ortogonais (ver [25, Teorema 5.6]) e do resultado principal do capítulo obtemos o seguinte teorema: Toda algebra que satisfaz as identidades com traço de $B_n(K)$ pode ser mergulhada em $B_n(C) = B_n(K) \otimes C$, para alguma álgebra comutativa e associativa C, ver Teorema 4.4.3.

Os principais resultados desta tese podem ser encontrados nos artigos [33] e [34] (o primeiro já publicado na revista **Journal of Pure and Applied Algebra** e o segundo aceito para publicação na revista **International Journal of Algebra and Computation**), esses resultados estão no Capítulo 2 e no Capítulo 3, respectivamente. Já os resultados no Capítulo 4 são novos, e serão submetidos para publicação. Os resultados desta tese foram obtidos em colaboração com os professores Plamen Koshlukov (UNICAMP), Diogo Diniz (UFCG) e Sergio Mota (UESC).

1 Preliminares

Neste primeiro capítulo, temos como objetivo estabelecer notações, conceitos e resultados básicos necessários para o desenvolvimento dos estudos dos demais capítulos deste trabalho. Inicialmente falaremos sobre PI-álgebras, que é o nosso objeto fundamental. Em todo o capítulo, K é um corpo qualquer, $charK$ denotará a característica do corpo K e, a menos que se diga o contrário, todas as álgebras e espaços vetoriais serão sobre K.

1.1 Álgebras

Definição 1.1.1. *Define-se uma K-álgebra, ou simplesmente álgebra, como sendo um par $(A, \circledast)$, onde A é um K-espaço vetorial e "$\circledast$" é uma operação em A que é uma aplicação bilinear, ou seja, $\circledast\colon A \times A \to A$ satisfaz:*

(i) $a \circledast (b + c) = a \circledast b + a \circledast c$;

(ii) $(a + b) \circledast c = a \circledast c + b \circledast c$;

(iii) $(\lambda a) \circledast b = a \circledast (\lambda b) = \lambda(a \circledast b)$,

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

Na definição acima, "$\circledast$" chama-se produto ou multiplicação. Em geral, denotaremos $a \circledast b$, com a, $b \in A$, simplesmente por ab. Definimos $a_1a_2a_3$ como sendo $(a_1a_2)a_3$ e, indutivamente, $a_1a_2 \cdots a_{n-1}a_n$ como sendo $(a_1a_2 \cdots a_{n-1})a_n$, para $a_1, \ldots, a_n \in A$. Dizemos que um subconjunto $\mathcal{B}$ da álgebra A é uma **base de** A se $\mathcal{B}$ é uma base de A como espaço vetorial e definimos a **dimensão de** A como sendo a dimensão de A como espaço vetorial, denotado por $\dim_K A$.

Sejam a, b e c elementos de uma álgebra A, definimos o **comutador de** a **e** b, denotado por $[a, b]$, o **produto de Jordan de** a **e** b, $a \circ b$ e o **associador entre** a**,** b **e** c, (a, b, c), como sendo as operações

$$[a, b] = ab - ba \qquad , \qquad a \circ b = (ab + ba) \qquad \text{e} \qquad (a, b, c) = (ab)c - a(bc),$$

respectivamente. De modo geral, definimos o **comutador e produto de Jordan de comprimento** n como sendo

$$[a_1, a_2, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n] \qquad \text{e} \qquad (a_1 \circ \cdots \circ a_{n-1} \circ a_n) = (a_1 \circ \cdots \circ a_{n-1}) \circ a_n,$$

onde $a_i \in A$. Em outras palavras, a ausência de parênteses significa que esses estão colocados da esquerda à direita (os produtos são normados à esquerda).

Sendo A uma álgebra associativa, é fácil verificar que

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

Fazendo indução sobre n podemos mostrar que:

$$[a_1 a_2 \cdots a_n, c] = \sum_{i=1}^{n} a_1 \cdots a_{i-1}[a_i, c]a_{i+1} \cdots a_n, \tag{1.2}$$

para cada $a_i, c \in A$.

Observação 1.1.2. *Caso a característica do corpo seja diferente de 2, podemos definir o produto de Jordan de a e b da seguinte forma:*

$$a \circ b = (1/2)(ab + ba).$$

Tal definição do produto de Jordan tem a vantagem que se A é uma álgebra associativa, então os quadrados dos elementos (associativos e de Jordan) são os mesmos. Em outras palavras, se $a \circ b = ab + ba$ teremos $a \circ a = 2a^2$.

Definição 1.1.3. *Uma álgebra A será dita:*

(i) ***Associativa**, se $(a, b, c) = 0$ para quaisquer $a,\ b,\ c \in A$;*

(ii) ***Comutativa**, se $[a, b] = 0$, para quaisquer $a,\ b \in A$;*

(iii) ***Unitária** (ou com unidade), se existir $1_A \in A$ tal que $1_A a = a 1_A = a$, para todo $a \in A$;*

(iv) ***Álgebra de Lie** se valem $a^2 = aa = 0$ e $(ab)c + (bc)a + (ca)b = 0$ (identidade de Jacobi), para quaisquer $a,\ b,\ c \in A$. Observe que $a^2 = 0$ implica que $ab = -ba$, para quaisquer $a,\ b \in A$. Dizemos que uma álgebra de Lie é **abeliana** se $ab = 0$, para quaisquer $a,\ b \in A$.*

(v) ***Álgebra de Jordan** se for comutativa e valer $(a^2 b)a = a^2(ba)$ (identidade de Jordan), para todo $a, b \in A$, onde $a^2 = aa$. Observamos que a identidade de Jordan pode ser escrita em termos do associador como sendo $(a^2, b, a) = 0$.*

Sendo A uma álgebra unitária, identificaremos $\lambda \in K$ como sendo o elemento $\lambda 1_A$ de A e o corpo K como o subconjunto $\{\lambda 1_A \mid \lambda \in K\}$ (o subespaço de A gerado pelo elemento 1_A). Apresentaremos agora alguns exemplos importantes de álgebras.

Exemplo 1.1.4. ***(Álgebra das matrizes)*** *Sejam K um corpo e $n \in \mathbb{N}$. O espaço vetorial $M_n(K)$ munido de seu produto usual é uma álgebra associativa com unidade (a matriz identidade I_n). Destacamos nesta álgebra as matrizes elementares E_{ij}, que possuem 1 na entrada da i-ésima linha e j-ésima coluna e 0 nas demais. É fácil verificar que elas formam* *uma base para $M_n(K)$. De modo geral, se A é uma álgebra, consideramos o espaço vetorial $M_n(A)$ de todas as matrizes de ordem n com entradas em A. O produto de matrizes em $M_n(A)$ é análogo ao produto de matrizes com entradas em K. Temos então uma estrutura de álgebra em $M_n(A)$.*

Exemplo 1.1.5. ***(Álgebra de Grassmann)*** *Sejam K um corpo de característica diferente de 2, e V o espaço vetorial sobre K com base $\{e_1, e_2, e_3, \ldots\}$. Definimos a álgebra de Grassmann (ou álgebra exterior) de V, denotada por $E = E(V)$, como sendo a álgebra associativa e unitária com base*

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

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

$$E_0 = span_K\{1_E, e_{i_1}e_{i_2}\cdots e_{i_m} \mid m \text{ é par, } i_1 < i_2 < \ldots < i_m\}$$

$$e$$

$$E_1 = span_K\{e_{i_1}e_{i_2}\cdots e_{i_m} \mid m \text{ é ímpar, } i_1 < i_2 < \ldots < i_m\}.$$

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

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

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

Considere E' o subespaço de E gerado por

$$\{e_{i_1}e_{i_2}\cdots e_{i_m} \mid m \in \mathbb{N}, i_1 < i_2 < \ldots < i_m\}.$$

Temos que E', munido da operação de E, é uma álgebra chamada ***álgebra de Grassmann sem unidade****.*

Exemplo 1.1.6. *Seja A uma álgebra associativa. Para todo $a, b \in A$, podemos definir o comutador $[a, b]$ no espaço vetorial associado a A, ao substituirmos o produto original em A por essa nova multiplicação, denotaremos a nova álgebra por $A^{(-)}$. Além disso, podemos também substituir o produto original em A pelo produto de Jordan $a \circ b$, denotando a nova álgebra por $A^{(+)}$. Observa-se que $A^{(-)}$ e $A^{(+)}$ são álgebras de Lie e Jordan, respectivamente. No caso da álgebra de Jordan exigimos que a característica do corpo seja diferente de 2, iremos dedicar a Seção 1.7 para este tipo de álgebras.*

Definição 1.1.7. *Seja A uma álgebra. Dizemos que:*

(i) Um subespaço B de A é uma ***subálgebra*** *de A, se é fechado com respeito a multiplicação, isto é, $b_1 b_2 \in B$ para quaisquer b_1, $b_2 \in B$;*

(ii) Um subespaço I de A é um ***ideal*** *(bilateral) de A se $AI \subseteq I$ e $IA \subseteq I$, ou seja, se $ax, xa \in I$ para quaisquer $a \in A$ e $x \in I$.*

Podemos definir ideais unilaterais. Um subespaço I é dito ideal à direita (respectivamente à esquerda) se $IA \subseteq I$ (respectivamente $AI \subseteq I$).

Exemplo 1.1.8. *Considere a álgebra exterior E (Exemplo 1.1.5). Dado $k \in \mathbb{N}$, tomemos o subespaço E_k de E gerado por*

$$\{1, e_{i_1} e_{i_2} \cdots e_{i_l} \mid 1 \leqslant i_1 < i_2 < \cdots < i_l \leqslant k\}.$$

Temos que E_k é uma subálgebra de E de dimensão 2^k. A álgebra E_k é a ***álgebra de Grassmann do espaço vetorial com base*** *$\{e_1, e_2, \ldots, e_k\}$.*

Exemplo 1.1.9. *O subespaço $UT_n(K)$ de $M_n(K)$ formado por todas as matrizes triangulares superiores é uma subálgebra da álgebra associativa $M_n(K)$. Pode ser deduzido facilmente que este mesmo subespaço é uma subálgebra da álgebra de Lie $M_n(K)^{(-)} = gl_n(K)$, bem como uma subálgebra da álgebra de Jordan $M_n(K)^{(+)}$.*

O subespaço $sl_n(K)$ que consiste das matrizes de traço 0 em $M_n(K)$ é uma subálgebra de Lie de $M_n(K)^{(-)}$. Por outro lado $sl_n(K)$ não é subálgebra da álgebra associativa $M_n(K)$ (observe que o produto de duas matrizes de traço 0 não necessariamente terá traço 0).

Analogamente, o subespaço das matrizes simétricas é uma subálgebra de Jordan em $M_n(K)^{(+)}$ que não é subálgebra da álgebra associativa $M_n(K)$ (sabemos da álgebra linear elementar que o produto de duas matrizes simétricas é de novo uma matriz simétrica se e somente se as duas matrizes iniciais comutam).

Exemplo 1.1.10. ***(Centro de uma álgebra)*** *Seja A uma álgebra. Podemos definir o centro comutativo de A como sendo o conjunto*

$$Z(A) = \{a \in A \mid [a, x] = 0, \text{ para todo } x \in A\}$$

e seu centro associativo dado por

$$N(A) = \{a \in A \mid (a, x, y) = (x, a, y) = (x, y, a) = 0, \text{ para todo } x, y \in A\}.$$

Assim, o conjunto

$$\mathcal{Z}(A) = Z(A) \cap N(A)$$

é uma subálgebra de A chamada ***centro de*** *A. Em particular, se A for associativa então o conjunto $\mathcal{Z}(A) = Z(A)$ é o centro de A. Além disso, é fácil verificar que dado $n \in \mathbb{N}$, $\mathcal{Z}(M_n(K)) = \{\lambda I_n \mid \lambda \in K\}$ e que $\mathcal{Z}(E) = E^{(0)}$.*

O próximo resultado nos permite obter uma estrutura de álgebra a partir de um espaço vetorial.

Proposição 1.1.11. *Sejam A um espaço vetorial e $\mathcal{B}$ uma base de A. Dada uma função $f\colon \mathcal{B}\times\mathcal{B} \to A$, existe uma única aplicação bilinear $\cdot\colon A \times A \to A$ tal que $u_1 \cdot u_2 = f(u_1, u_2)$ para quaisquer u_1, $u_2 \in \mathcal{B}$.*

Demonstração. Veja a prova em [36, Observação 1.1.2]. □

Assim, para definir uma estrutura de álgebra sobre um espaço vetorial A basta definir o produto para os elementos de uma base $\mathcal{B}$ de A, uma vez que a soma e o produto por escalar estão bem definidos no espaço vetorial e são constantes de estrutura. Uma vez definido o produto, verifica-se que A é uma álgebra associativa se, e somente se, $(v_1v_2)v_3 = v_1(v_2v_3)$, para quaisquer v_1, v_2, $v_3 \in \mathcal{B}$. Similarmente para o caso comutativo ou unitário.

Exemplo 1.1.12. *Seja G um grupo. Consideraremos o conjunto KG de todas as somas formais $\sum\limits_{g\in G} \alpha_g g$, onde $\alpha_g \in K$ e o conjunto $\{g \in G \mid \alpha_g \neq 0\}$ é finito, aqui $\alpha_g g$ é um símbolo formal. Dizemos que $\sum\limits_{g\in G} \alpha_g g = \sum\limits_{g\in G} \beta_g g$ em KG se $\alpha_g = \beta_g$ para todo $g \in G$. Além disso definimos, em KG, a soma*

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

e o produto por escalar

$$\lambda \sum_{g\in G} \alpha_g g = \sum_{g\in G} (\lambda\alpha_g) g, \ \ \textit{para todo } \lambda \in K.$$

*Observe que KG munido dessas operações é um **espaço vetorial com base** G. Adotando a notação multiplicativa em G e considerando no espaço vetorial KG o produto induzido pela operação de G, pela proposição anterior, KG é uma álgebra associativa com unidade chamada de **álgebra de grupo**. Observe que KG é comutativa se, e somente se, G é abeliano.*

Exemplo 1.1.13. ***(Produto tensorial de álgebras)*** *Sejam A e B álgebras. Recordamos que o produto tensorial entre espaços vetoriais A e B, denotado por $A \otimes_K B$, é o espaço vetorial gerado por $\{a \otimes_K b \mid a \in A, b \in B\}$. Os elementos da forma $a \otimes_K b$ são chamados de **tensores** e satisfazem:*

(i) $(a_1 + a_2) \otimes_K b = (a_1 \otimes_K b) + (a_2 \otimes_K b)$;

(ii) $a \otimes_K (b_1 + b_2) = (a \otimes_K b_1) + (a \otimes_K b_2)$;

(iii) $\lambda(a \otimes_K b) = (\lambda a) \otimes_K b = a \otimes_K (\lambda b)$,

para quaisquer a_1, a_2, $a \in A$, b_1, b_2, $b \in B$ *e* $\lambda \in K$.

É um fato bastante conhecido que se $\mathcal{B}_1$ *e* $\mathcal{B}_2$ *são bases de* A *e* B*, respectivamente, então o conjunto* $\{u \otimes_K v \mid u \in \mathcal{B}_1, v \in \mathcal{B}_2\}$ *é uma base do espaço vetorial* $A \otimes_K B$ *e* $\dim_K(A \otimes_K B) = \dim_K A \cdot \dim_K B$*. Mais geralmente, sejam* $\{a_i \mid i \in I\}$ *e* $\{b_i \mid i \in I\}$ *subconjuntos de vetores linearmente independentes de* A *e* B*, respectivamente, então o conjunto* $\{a_i \otimes_K b_i \mid i \in I\}$ *é um subconjunto linearmente independente de* $A \otimes_K B$*. Além disso, se* V *é um espaço vetorial e* $f\colon A \times B \to V$ *uma aplicação bilinear, então existe uma única transformação linear* $T_f\colon A \otimes_K B \to V$ *satisfazendo* $T_f(a \otimes_K b) = f(a, b)$ *(propriedade universal do produto tensorial), para maiores detalhes ver [24, Capítulo II, Seção 12].*

Para definir uma estrutura de álgebra em $A \otimes_K B$*, fixamos bases* $\mathcal{B}_1$ *e* $\mathcal{B}_2$ *de* A *e* B*, respectivamente, e definimos o produto da forma* $(u_1 \otimes_K v_1)(u_2 \otimes_K v_2) = u_1u_2 \otimes_K v_1v_2$*, para todo* u_1, $u_2 \in \mathcal{B}_1$ *e* v_1, $v_2 \in \mathcal{B}_2$*. Da Proposição 1.1.11 temos que se* A *e* B *são álgebras associativas (comutativas) então* $A \otimes_K B$*, munido deste produto, é uma álgebra associativa (comutativa). Caso* A *e* B *tenham unidade, então* $1_A \otimes_K 1_B$ *é a unidade para a álgebra* $A \otimes_K B$.

A seguir faremos duas observações importantes sobre o exemplo anterior.

Observação 1.1.14. ***(Tensor não nulo)*** *Sejam* V *e* W *espaços vetoriais,* $v_0 \in V$ *e* $w_0 \in W$ *vetores não nulos. Então* $v_0 \otimes_K w_0$ *é um vetor não nulo em* $V \otimes_K W$.

Observação 1.1.15. ***(Centro de uma álgebra tensorial)*** *Sejam* A *e* B *álgebras unitárias, então* $\mathcal{Z}(A \otimes_K B) = \mathcal{Z}(A) \otimes_K \mathcal{Z}(B)$*. De fato, como* $\mathcal{Z}(A) \otimes_K \mathcal{Z}(B)$ *está contido em* $\mathcal{Z}(A \otimes_K B)$*, então resta mostrar a inclusão contrária. Seja* $\alpha \in \mathcal{Z}(A \otimes_K B)$ *não nulo, então existem* $a_1, \ldots, a_n \in A$ *não nulos, e* $b_1, \ldots, b_n \in B$ *linearmente independentes, tais que* $\alpha = \sum_{i=1}^{n} a_i \otimes_K b_i$*. Dados* $x, y \in A$*, temos que*

$$(\alpha, (x \otimes_K 1_B), (y \otimes_K 1_B)) = ((x \otimes_K 1_B), \alpha, (y \otimes_K 1_B)) = ((x \otimes_K 1_B), (y \otimes_K 1_B), \alpha) = 0$$

e $[\alpha, (x \otimes_K 1_B)] = 0$*. Segue que* $(a_i, x, y) = (x, a_i, y) = (x, y, a_i) = [a_i, x] = 0$*, ou seja,* $a_i \in \mathcal{Z}(A)$*, para todo* $i = 1, \ldots, n$*. Como* $\alpha \in \mathcal{Z}(A) \otimes_K B$*, existem* $z_1, \ldots, z_m \in \mathcal{Z}(A)$*, linearmente independentes, e* $b'_1, \ldots, b'_m \in B$ *não nulos tais que* $\alpha = \sum_{i=1}^{m} z_i \otimes_K b'_i$*. Fazendo procedimento análogo ao que foi feito anteriormente, concluímos que* $b'_1, \ldots, b'_m \in \mathcal{Z}(B)$*. Isto termina a demonstração.*

Definição 1.1.16. *Sejam* A *uma álgebra e* S *um subconjunto não vazio de* A*. Definimos:*

(i) ***Subálgebra de*** A ***gerada por*** S*, denotada por* $\langle S\rangle_K$*, como sendo a interseção de todas as subálgebras de* A *que contêm* S *(ou* $S \cup \{1_A\}$*, caso* A *seja unitária).*

(ii) ***Ideal de*** A ***gerado por*** S*, denotado por* (S)*, como sendo a interseção de todos os ideais de* A *que contêm* S*.*

Claramente, da definição anterior, $\langle S\rangle_K$ é a menor subálgebra de A que contém S, assim como o ideal de A gerado por S. Sendo A uma álgebra, dizemos que $S \subseteq A$ **gera** A, como álgebra, ou é **um conjunto gerador** para a álgebra A, se $\langle S\rangle_K = A$. Além disso, A é dita uma **álgebra finitamente gerada** se existe $S \subseteq A$ finito tal que $\langle S\rangle_K = A$.

Observação 1.1.17. *Sendo* A *uma álgebra associativa unitária e* S *um subconjunto não vazio de* A*, não é difícil mostrar que* $\langle S\rangle_K$ *coincide com o subespaço de* A *gerado por* $\{1, s_1s_2\cdots s_n \mid n \in \mathbb{N}, s_i \in S\}$ *e o ideal de* A *gerado por* S *coincide com o subespaço de* A *gerado por* $\{asb \mid a, b \in A, s \in S\}$*.*

Sejam A uma álgebra e I um ideal de A. Denotaremos, como usualmente, por A/I a **Álgebra Quociente de** A **por** I. Para cada $a \in A$, denotaremos o elemento correspondente em A/I por $\bar{a}$ ou $a + I$.

Definição 1.1.18. *Sejam* A *e* B *duas álgebras. Dizemos que uma transformação linear* $\varphi\colon A \to B$ *é um* ***homomorfismo de álgebras****, se* $\varphi(a_1a_2) = \varphi(a_1)\varphi(a_2)$*, para quaisquer* a_1*,* $a_2 \in A$*. Se* A *e* B *possuem unidade, exigimos que* $\varphi(1_A) = 1_B$*.*

Chamamos φ de **monomorfismo** (ou **mergulho**) se φ é um homomorfismo injetivo, de **epimorfismo** se φ é um homomorfismo sobrejetivo, e de **isomorfismo** se φ é um homomorfismo biunívoco. Dizemos que φ é um **endomorfismo** de A, se φ é um homomorfismo de A em A e um **automorfismo** de A se φ é um endomorfismo biunívoco de A. Denotamos por $End_K(A)$ e $Aut_K(A)$ o conjunto dos endomorfismos e automorfismos, respectivamente, da álgebra A. Quando existe um isomorfismo $\varphi\colon A \to B$, dizemos que as álgebras A e B são isomorfas e denotamos por $A \simeq B$.

Seja $\varphi\colon A \to B$ um homomorfismo de álgebras. Denotamos o **núcleo de** φ por $Ker\varphi = \{a \in A \mid \varphi(a) = 0\}$ e a **imagem de** φ por $Im\varphi = \{\varphi(a) \mid a \in A\}$. É de fácil verificação que $Ker\varphi$ é um ideal de A e a $Im\varphi$ é uma subálgebra de B.

Apresentaremos a seguir alguns exemplos importantes de homomorfismos.

Exemplo 1.1.19. *Sejam* A *uma álgebra e* I *um ideal de* A*. A aplicação* $\pi\colon A \to A/I$*, definida por* $\pi(a) = a + I$*, é um epimorfismo de álgebras denominada* ***projeção canônica****.*

Exemplo 1.1.20. *Seja* A *uma álgebra associativa e unitária. Dizemos que um elemento* $a \in A$ *é* ***invertível*** *se existe* $a^{-1} \in A$ *tal que* $aa^{-1} = a^{-1}a = 1$*. Vamos denotar por* $U(A)$ *o* *conjunto dos elementos invertíveis de A, então $U(A)$ é um grupo multiplicativo. Tomando $r \in U(A)$, podemos considerar a aplicação*

$$\begin{array}{rcl} Int_r\colon A & \to & A \\ x & \mapsto & Int_r(x) = rxr^{-1}. \end{array}$$

*É fácil verificar que esta aplicação é um automorfismo de A chamado de **automorfismo interno determinado por** r.*

Definição 1.1.21. *Seja A uma álgebra com unidade. Dizemos que A é uma **álgebra com divisão** se $U(A) = A \backslash \{0\}$.*

Exemplo 1.1.22. *Seja $\mathbb{R}$ o corpo dos reais, então as $\mathbb{R}$-álgebras $\mathbb{R}$, $\mathbb{C}$ (corpo dos complexos) e $\mathbb{H}$ (álgebra dos quatérnios reais) são exemplos de álgebras com divisão. A álgebra $\mathbb{R}(x)$ das funções racionais de uma variável x também é um exemplo de álgebra com divisão. Esta última é comutativa, portanto é um corpo.*

A determinação das álgebras com divisão e de dimensão finita sobre um corpo algebricamente fechado é trivial, mais precisamente observamos os dois resultados a seguir. Suas demonstrações podem ser encontradas em [53, pág. 452]

Teorema 1.1.23. *Se K é algebricamente fechado e D é uma álgebra com divisão de dimensão finita sobre K, então $D = K$*

Teorema 1.1.24 (**Teorema de Frobenius**). *As únicas álgebras associativas com divisão reais de dimensão finita são, a menos de isomorfismo, o corpo dos reais, a álgebra dos complexos e a dos quatérnios reais.*

Daremos neste momento a definição e propriedades elementares de módulos necessários para o entendimento do nosso trabalho.

Definição 1.1.25. *Sejam A uma álgebra unitária e M um espaço vetorial sobre o corpo K. Considere uma aplicação*

$$\begin{array}{rcl} \cdot\colon A \times M & \to & M \\ (a, m) & \to & a \cdot m \end{array}$$

que satisfaz as seguintes condições:

(i) $(a_1 + a_2) \cdot m = (a_1 \cdot m) + (a_2 \cdot m)$;

(ii) $a \cdot (m_1 + m_2) = (a \cdot m_1) + (a \cdot m_2)$;

(iii) $(\lambda a) \cdot m = a \cdot (\lambda m) = \lambda(a \cdot m)$;

(iv) $a_1 \cdot (a_2 \cdot m) = (a_1 a_2) \cdot m$; *e*

(v) $1_A \cdot m = m$,

para quaisquer a, a_1, $a_2 \in A$, m, m_1, $m_2 \in M$ *e* $\lambda \in K$. *Dizemos que* M, *munido dessa aplicação, é um* ***A-módulo à esquerda*** *(ou módulo à esquerda sobre* A*). De modo similar podemos definir um* A*-módulo à direita (ou módulo à direita sobre* A*).*

Notação 1.1.26. *Por simplicidade chamaremos um* A*-módulo à esquerda simplesmente de* ***A-módulo***.

Exemplo 1.1.27. *Sendo* A *uma álgebra unitária, pela definição de* A*-módulo temos que* A *é um* A*-módulo, cuja a aplicação considerada é a sua própria multiplicação.*

Exemplo 1.1.28. *Sejam* G *um grupo,* V *um espaço vetorial e* $\varphi\colon G \to GL(V)$ *um homomorfismo de grupos, onde* $\varphi(g) = \varphi_g$. *Considere o seguinte aplicação*

$$\begin{array}{rcl} \cdot\colon KG \times V & \to & V \\ (\sum_{g\in G} \lambda_g g, v) & \to & \sum_{g\in G} \lambda_g g \cdot v = \sum_{g\in G} \lambda_g \varphi_g(v). \end{array}$$

Note que V, *munido dessa aplicação, é um* KG*-módulo (ou simplesmente,* ***G-módulo****), onde as condições da Definição 1.1.25 seguem do fato de que* φ *é um homomorfismo de grupos e* φ_g *é linear, para cada* $g \in G$.

Definição 1.1.29. *Sejam* A *uma álgebra e* M *um* A*-módulo. Definimos um* ***submódulo*** *(ou* A*-submódulo)* N *de* M *como sendo um subespaço de* M *tal que* $a \cdot n \in N$ *para quaisquer* $a \in A$ *e* $n \in N$.

Exemplo 1.1.30. *Seja* A *uma álgebra. Considerando* A *como* A*-módulo; segue diretamente da definição que os seus submódulos são exatamente os ideais à esquerda da álgebra* A.

Definição 1.1.31. *Sejam* M_1 *e* M_2 *módulos sobre uma álgebra* A. *Definimos um* ***homomorfismo de A-módulos*** *como sendo uma transformação linear* $\varphi\colon M_1 \to M_2$ *tal que* $\varphi(a \cdot m) = a \cdot \varphi(m)$ *para quaisquer* $a \in A$ *e* $m \in M_1$. *Se* φ *é biunívoca, dizemos que* φ *é um* ***isomorfismo de A-módulos***.

Definição 1.1.32. *Sejam* A *uma álgebra e* M *um* A*-módulo.*

(i) Dizemos que M *é* ***simples*** *(ou* ***irredutível****), como* A*-módulo, se seus únicos submódulos são* $\{0\}$ *e* M.

(ii) Dizemos que M *é* ***completamente redutível*** *(****semissimples****) como* A*-módulo, se* M *pode ser decomposto como uma soma direta de submódulos irredutível.*

Da definição acima, temos que todo módulo irredutível é completamente redutível. A unicidade, a menos de isomorfismo e ordenação, das componentes irredutíveis de um módulo completamente redutível M é um resultado muito importante para alguns dos exemplos apresentados no Capítulo 2 (ver Observação 2.2.11), mais precisamente temos o seguinte resultado. Sua demonstração pode ser encontrada em [54, Seção, 3.4, pág. 115].

Teorema 1.1.33 (**Teorema de Krull-Schmidt**). *Seja M um A-módulo de dimensão finita tal que*

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n = N_1 \oplus N_2 \oplus \cdots \oplus N_m,$$

para M_1, $M_2, \ldots$, M_n, N_1, N_2, $\ldots$, N_m submódulos irredutíveis de M. Então $n = m$ e M_i e N_i são isomorfos para todo $i = 1, 2, \ldots, n$ (reordenando os N_i's, se necessário).

Observamos que ele é válido numa situação mais geral que a enunciada aqui. Uma afirmação equivalente à definição de módulo completamente redutível que utilizaremos aqui será enunciada a seguinte.

Teorema 1.1.34. *M é um A-módulo completamente redutível se, e somente se, para todo submódulo N de M existir N' submódulo de M tal que $M = N \oplus N'$.*

Demonstração. Ver [54, Seção 3.5, Theorem 3.10, pág. 121]. □

Seja A uma álgebra (não necessariamente associativa) sobre um corpo K. Dado $a \in A$, podemos considerar a multiplicação à direita D_a (resp., à esquerda E_a) como sendo a aplicação linear $x \to xa$ (resp., $x \to ax$). Assim, podemos associa-lá a duas álgebras associativas de transformações lineares:

(1) A **álgebra das multiplicações** $M = M(A)$ definida como sendo a subálgebra de $End_K(A)$ gerada por 1 e todos os D_a e E_a, com $a \in A$.

(2) O **Centroide** $\Gamma = \Gamma(A)$ de A como sendo o centralizador de M em $End_K(A)$, ou seja, $\gamma \in End_K(A)$ tal que $\gamma m = m\gamma$, para todo $m \in M$.

Evidentemente, para todo $\gamma \in \Gamma$, tem-se $[\gamma, D_a] = [\gamma, E_a] = 0$, para todo $a \in A$, e vice-versa, logo

$$(ab)\gamma = a(\gamma b) = (a\gamma)b, \tag{1.3}$$

para todo a, $b \in A$.

Lema 1.1.35. *Se $A^2 = A$, então Γ é comutativo.*

Demonstração. Para todo γ, $\delta \in \Gamma$ e todo a, $b \in A$ tem-se

$$\begin{aligned} (ab)\gamma\delta &= (a(b\gamma))\delta = (a\delta)(b\gamma) \text{ e} \\ (ab)\delta\gamma &= ((a\delta)b)\gamma = (a\delta)(b\gamma) \end{aligned}$$

Consequentemente, $ab(\delta\gamma-\gamma\delta)=0$. Como $A^2=A$, então todo $c\in A$ é da forma $c=\sum_i a_ib_i$. Segue que $c(\delta\gamma-\gamma\delta)=0$, para todo $c\in A$ não nulo, e portanto, $\delta\gamma=\gamma\delta$, para todo γ, $\delta\in\Gamma$. Concluímos que Γ é comutativo. □

Definição 1.1.36. *Uma álgebra A é chamada de **simples** se 0 e A são os únicos ideais de A e $A^2\neq 0$.*

Observe que os ideais de uma álgebra A são exatamente os subespaços invariantes pela multiplicação à esquerda e à direita. Assim, A é simples se, e somente se, M é uma álgebra irredutível de transformações lineares, irredutível no sentido que não há subespaço não trivial m-invariante para todo $m\in M$. Se $x\in A$, então o menor subespaço M-invariante contendo x é Mx. Portanto,

Lema 1.1.37. *A é uma álgebra simples (não necessariamente associativa) se, e somente se, $A^2\neq 0$ e $Mx=A$ para todo $x\neq 0$.*

Lema 1.1.38 (**Lema de Schur**)**.** *Seja R uma álgebra. Se N é um R-módulo irredutível, então $End_R(N)$ é um anel de divisão.*

Assim, considerando a álgebra A simples e M a álgebra irredutível de transformação lineares, podemos ver A como M-módulo irredutível (pela multiplicação $m\cdot a=m(a)$, para todo $m\in M$ e todo $a\in A$). Do Lema de Schur temos que

$$End_M(A)=\{\gamma\in End_K A\mid \gamma m=m\gamma,\ \text{para todo } m\in M\}=\Gamma,$$

ou seja, Γ é um **anel de divisão**. Como consequência temos o seguinte resultado.

Teorema 1.1.39. *O centroide Γ de uma álgebra simples é um corpo.*

Definição 1.1.40. *Uma álgebra A é dita **central**, se seu centroide Γ coincide com o corpo base.*

Dadas uma álgebra A sobre K e uma extensão qualquer F do corpo K, escreveremos $A_F=A\otimes_K F$ para indicar **a F-álgebra obtida de A por extensão de escalares para F**. Claramente, se A é simples com centroide Γ, então A_Γ é central simples sobre o corpo Γ. Consideraremos a questão de extensão do corpo base de uma álgebra não-associativa simples. A seguir enunciaremos um resultado fundamental desta conexão de definições cuja demonstração pode ser encontrada em [51, Teorema 3, pag. 292].

Teorema 1.1.41. *Seja A uma álgebra (não necessariamente associativa) sobre um corpo K e F uma extensão qualquer do corpo K. Então A é central simples se, e somente se, A_F é simples, para toda extensão F de K.*

Enunciaremos um importante resultado provado por Weedderburn para o caso de álgebras simples de dimensão finita. Posteriormente Artin estendeu o mesmo para anéis artinianos simples e assim o resultado ficou conhecido como o “Teorema de Wedderburn e Artin”.

Teorema 1.1.42 (**Wedderburn**). *Seja A um álgebra simples de dimensão finita. Então A é isomorfa a $M_n(D)$, onde D é um anel de divisão. Caso o corpo base K seja algebricamente fechado, então A é isomorfa à álgebra de matrizes $M_n(K)$ para algum n.*

Demonstração. Ver por exemplo [85, Corolário 1.6, pág. 282]. □

Por fim, o resultado final desta seção é uma consequência imediata do Teorema de Skolem-Noether, cuja demonstração pode ser encontrada em [85, Teorema 4.2, pág 291].

Proposição 1.1.43. *Se A é uma álgebra associativa central simples de dimensão finita, então todo automorfismo de A é interno.*

1.2 Álgebras Graduadas

Nesta seção apresentaremos os conceitos de álgebras graduadas que serão fundamentais para nossos estudos nos Capítulos 2 e 3. Em todo texto G denotará um grupo abeliano com elemento neutro ϵ.

Definição 1.2.1. *Dizemos que uma álgebra A é G-graduada se existe uma família de subespaços $\{A_g \mid g \in G\}$ de A tais que*

$$A = \bigoplus_{g\in G} A_g \quad e \quad A_g A_h \subseteq A_{gh},$$

para quaisquer $g, h \in G$.

Na definição anterior, o subespaço A_g é chamado de **componente homogênea de grau** g e os seus elementos de **elementos homogêneos de grau** g. Um subespaço V de A é **homogêneo** (ou **graduado**) se

$$V = \bigoplus_{g\in G}(V \cap A_g).$$

Em particular, podemos considerar subálgebra homogênea e ideal homogêneo. Além disso, o **suporte** de uma álgebra G-graduada, denotado por $\mathrm{supp}_G\, A$ (ou simplesmente por $\mathrm{supp}\, A$), é definido como sendo o conjunto $\{g \in G \mid A_g \neq 0\}$. Similarmente, podemos definir o suporte de qualquer subespaço homogêneo em A.

Exemplo 1.2.2. *Toda álgebra A admite uma G-graduação, basta considerar $A_\epsilon = A$ e $A_g = \{0\}$ para todo $g \in G\backslash\{\epsilon\}$. Esta graduação é chamada **trivial**.*

Exemplo 1.2.3. *A álgebra de Grassmann E possui uma $\mathbb{Z}_2$-graduação natural definida por $E = E_0 \bigoplus E_1$, onde E_0 e E_1 são os subespaços do Exemplo 1.1.5. Além disso, a álgebra de Grassmann E_k de dimensão 2^k (veja exemplo 1.1.8) também possui uma $\mathbb{Z}_2$-graduação natural induzida por E de maneira que $(E_k)_0 = E_k \cap E_0$ e $(E_k)_1 = E_k \cap E_1$.*

Observamos aqui que a álgebra de Grassmann possui outras graduações com o grupo $\mathbb{Z}_2$. As graduações onde o espaço V gerado pelos vetores e_1, e_2, $\ldots$, é homogêneo, são bem conhecidas (ver, por exemplo, [29]). Mas no caso geral não se tem ainda uma descrição, exceto quando $\dim V < \infty$ (ver [65]).

Exemplo 1.2.4. *Sejam $A = \oplus_{g\in G} A_g$ e $B = \oplus_{h\in H} B_h$ álgebras graduadas pelos grupos G e H, respectivamente. O produto tensorial $A \otimes_K B$ possui uma $G \times H$-graduação natural $A \otimes_K B = \oplus_{(g,h)\in G\times H}(A \otimes_K B)_{(g,h)}$ cujo os seus componentes homogêneos são dados por $(A \otimes_K B)_{(g,h)} = A_g \otimes_K B_h$. Em geral, dados grupos $G_1, G_2, \ldots, G_m$ e uma álgebra G_k-graduada R_k, para cada $k = 1, \ldots, m$, podemos definir o produto tensorial de álgebras $R_1 \otimes_K R_2 \otimes_K \cdots \otimes_K R_m$ graduado pelo grupo $G = G_1 \times G_2 \times \cdots \times G_m$, chamado de **graduação produto tensorial**, cujos componentes homogêneos são dados pelos conjuntos*

$$R_{(g_1,g_2,\ldots,g_m)} = (R_1)_{g_1} \otimes_K (R_2)_{g_2} \otimes_K \cdots \otimes_K (R_m)_{g_m},$$

onde $g_k \in G_k$, para cada $k = 1, 2, \ldots, m$.

Exemplo 1.2.5. *Introduzimos no Exemplo 1.1.4 a notação da álgebra das matrizes de ordem n sobre um corpo K, denotado por $M = M_n(K)$. Assim, para cada $\gamma \in \mathbb{Z}_n$ tomemos o subespaço $M_\gamma = \langle E_{ij} \mid \overline{j - i} = \gamma \rangle$. Além disso, para cada $k \in \mathbb{Z}$, tomemos*

$$M_k = \begin{cases} \{0\} & , \text{ se } |k| \geqslant n \\ \langle E_{ij} \mid j - i = k \rangle & , \text{ se } |k| < n \end{cases}.$$

É fácil observar que $M_{\bar{0}} = M_0$ é exatamente o conjunto das matrizes diagonais e do fato que o conjunto $\{E_{ij} \mid 1 \leqslant i, j \leqslant n\}$ forma uma base para M, temos que as decomposições

$$M = \bigoplus_{\gamma\in\mathbb{Z}_n} M_\gamma = \bigoplus_{k\in\mathbb{Z}} M_k$$

definem uma $\mathbb{Z}_n$-graduação e uma $\mathbb{Z}$-graduação, respectivamente, em $M_n(K)$. Ademais, sejam a, $b \in \mathbb{Z}$ tais que $a + b = n$, podemos considerar uma $\mathbb{Z}_2$-graduação em $M_n(K)$ dada por

$$M_0 = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \quad e \quad M_1 = \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}.$$

Aqui $A \in M_a(K)$, $D \in M_b(K)$ e B, C são blocos de matrizes $a \times b$ e $b \times a$, respectivamente, com entradas em K.

A Z_n-graduação sobre $M_n(K)$ no exemplo anterior é chamada de **Graduação de Vasilovsky** de $M_n(K)$, esse é um exemplo particular de uma graduação chamada de **elementar** sobre as álgebras das matrizes que definiremos a seguir. Tal graduação, no caso das matrizes de ordem 2, foi introduzida por Di Vincenzo [27].

Definição 1.2.6. *Seja $\boldsymbol{g} = (g_1, \ldots, g_n)$ uma n-upla de elementos em G. A decomposição*

$$M_n(K) = \oplus_{g \in G}(M_n(K))_g, \tag{1.4}$$

*onde $(M_n(K))_g$ é o subespaço gerado pelas matrizes elementares E_{ij} tais que $g_i^{-1}g_j = g$, é uma graduação por G de $M_n(K)$ chamada **graduação elementar induzida pela n-upla $\boldsymbol{g}$**.*

Observação 1.2.7. *É óbvio que a n-upla $(g_1, \ldots, g_n)$ para uma dada graduação elementar não é única. Por exemplo a n-upla $(gg_1, \ldots, gg_n)$ define a mesma graduação, para todo $g \in G$.*

Exemplo 1.2.8. *Seja K um corpo contendo uma n-ésima raiz primitiva da unidade, denotada por ε. Considere as duas matrizes de ordem n*

$$A = \begin{pmatrix} \varepsilon^{n-1} & 0 & \ldots & 0 \\ 0 & \varepsilon^{n-2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \quad e \quad B = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Então A e B satisfazem as relações

$$AB = \varepsilon BA, A^n = B^n = I_n, \tag{1.5}$$

onde I_n é a matriz identidade de ordem n. É de fácil verificação que as matrizes A^iB^j, $1 \leqslant i, j \leqslant n$, são linearmente independentes sobre K. Como são n^2 matrizes dessa forma, temos que elas formam uma base para $M_n(K)$. Agora considere o grupo $G = (a)_n \times (b)_n \cong \mathbb{Z}_n \times \mathbb{Z}_n$, o produto direto de dois grupos cíclicos de ordem n e para $g = a^ib^j$, denote por $(M_n(K))_g$ o espaço unidimensional $span_K\{A^iB^j\}$. Da relação (1.5) segue que

$$(A^iB^j)(A^rB^s) = \varepsilon^{is-rj}(A^rB^s)(A^iB^j),$$

então,

$$M_n(K) = \bigoplus_{g \in G}(M_n(K))_g \tag{1.6}$$

*é uma G-graduação de $M_n(K)$ chamada **graduação de Pauli**.*

Definição 1.2.9. *Seja A uma álgebra G-graduada tal que $A = \oplus_{g \in G}A_g$. A graduação é chamada de **fina** se para qualquer $g \in G$ temos $dim_K A_g \leqslant 1$.*

Observação 1.2.10. *A graduação de Pauli de $M_n(K)$ é um exemplo de graduação fina.*

Agora iremos enunciar um resultado de [15] que identifica qualquer graduação sobre uma álgebra de matrizes pelo grupo G, sobre um corpo algebricamente fechado. Mas antes disso precisaremos definir o que é um isomorfismo G-graduado.

Definição 1.2.11. *Sejam A e B álgebras G-graduadas. Uma aplicação $\varphi\colon A \to B$ é chamada **homomorfismo G-graduado**, se φ é um homomorfismo que satisfaz $\varphi(A_g) \subseteq B_g$ para todo $g \in G$. De modo análogo, definimos isomorfismo, endomorfismo e automorfismo G-graduado.*

Teorema 1.2.12. *[15, Teoremas 6 e 8] Sejam K um corpo algebricamente fechado e $M_n(K) = \bigoplus_{g\in G}(M_n(K))_g$ a álgebra das matrizes munida de uma graduação por um grupo abeliano G. Então existem uma decomposição $n = tq$, um subgrupo H de G, e uma q-upla $\boldsymbol{g} = (g_1, \ldots, g_q)$ de elementos de G tais que $M_n(K)$ seja isomorfa a $M_t(K) \otimes_K M_q(K)$ como álgebras G-graduadas. Aqui $M_t(K)$ é uma álgebra H-graduada com uma graduação fina e $M_q(K)$ tem uma graduação elementar induzida pela q-upla $\boldsymbol{g}$. Além disso, a escolha do subgrupo H é de tal maneira que $\dim((M_t(K))_h) = 1$ para todo $h \in H$. Então o grupo $H = H_1 \times \cdots \times H_k$, com $H_i \cong \mathbb{Z}_{t_i} \times \mathbb{Z}_{t_i}$, para $i = 1, \ldots, k$, e $M_t(K)$ é isomorfo a $M_{t_1} \otimes_K \cdots \otimes_K M_{t_k}$, onde $M_{t_j} = M_{t_j}(K)$ é uma álgebra com graduação de Pauli pelo grupo H_j.*

Corolário 1.2.13. *[15, Corolário 10] Seja $M_n(K)$ graduada por um grupo finito G cuja ordem não é divisível por um quadrado. Então qualquer graduação sobre $M_n(K)$ é elementar.*

A seguir enunciaremos dois resultados elementares porém bastantes úteis. O primeiro é uma caracterização das subálgebras homogêneas e o segundo é sobre a álgebra quociente por um ideal homogêneo, ambos de uma álgebra G-graduada. Ambos resultados são bem conhecidos, portanto omitiremos as demonstrações.

Lema 1.2.14. *Sejam A uma álgebra G-graduada e B uma subálgebra de A. As seguintes afirmações são equivalentes:*

(i) *B é subálgebra G-graduada de A;*

(ii) *As componentes homogêneas de cada elemento de B pertencem a B;*

(iii) *B é gerada por elementos homogêneos.*

Proposição 1.2.15. *Se I é um ideal homogêneo de uma álgebra G-graduada A então A/I é uma álgebra G-graduada considerando suas componentes homogêneas da forma $(A/I)_g = \{a + I \mid a \in A_g\}$, para cada $g \in G$.*

A álgebra G-graduada $A = \oplus_{g\in G} A_g$ é dita **fortemente G-graduada** se $A_g A_h = A_{gh}$, para todo $g, h \in G$. Por exemplo, a álgebra de grupo $A = K[G]$ é fortemente G-graduada. Além disso, se A é fortemente G-graduada, então A/I também o é, para todo ideal homogêneo I de A. O próximo resultado caracteriza esses tipos de graduação.

Lema 1.2.16. *R é uma álgebra fortemente G-graduada se, e somente se, $1 \in R_g R_{g^{-1}}$, para todo $g \in G$.*

Demonstração. Ver [66, Proposição 1.1.1, pag. 2] □

Definição 1.2.17. *Seja G um grupo. Uma álgebra G-graduada A é chamada **G-produto cruzado** se $U(A) \cap A_g \neq \varnothing$, para todo $g \in G$.*

Pelo Lema 1.2.16, toda álgebra G-produto cruzado é uma álgebra fortemente G-graduada. A recíproca não é verdadeira, basta considerar uma $\mathbb{Z}_2$-graduação sobre $A = M_3(K)$, definida por:

$$A_0 = \begin{pmatrix} K & K & 0 \\ K & K & 0 \\ 0 & 0 & K \end{pmatrix} \quad e \quad A_1 = \begin{pmatrix} 0 & 0 & K \\ 0 & 0 & K \\ K & K & 0 \end{pmatrix}.$$

Observe que $A_1 A_1 = A_0$, uma vez que a base de A_0 está contida em $A_1 A_1$. Então A é uma álgebra fortemente $\mathbb{Z}_2$-graduada, porém não é $\mathbb{Z}_2$-produto cruzado, já que não tem elemento invertível em A_1. Isso não contradiz o Lema 1.2.16, já que $A_g A_{g^{-1}}$ é soma de produtos entre elementos homogêneos de grau g e g^{-1}.

Definição 1.2.18. *Sejam $\Gamma\colon A = \oplus_{g\in G} A_g$ e $\Gamma'\colon A = \oplus_{h\in H} A_h$ graduações de uma álgebra A pelos grupos G e H, respectivamente. Dizemos que a graduação Γ' é um **coarsening** de Γ se para todo $g \in G$ existir $h \in H$ tal que $A_g \subseteq A_h$. Nestas condições também dizemos que Γ é um **refinamento** de Γ'.*

Observação 1.2.19. *Se, para algum $g \in \mathrm{supp}_G A$, existir $h \in H$ tal que a inclusão definida acima seja estrita, dizemos que o refinamento ou coarsening é **próprio**. Além disso, podemos definir uma ordem parcial "$\preceq$" da seguinte maneira: Dizemos que $\Gamma' \preceq \Gamma$ se, e somente se, Γ' é um coarsening de Γ. Neste caso, uma graduação que não admite refinamento próprio é chamada de fina.*

Exemplo 1.2.20. *Sejam $\Gamma\colon A = \oplus_{g\in G} A_g$ e $\Gamma'\colon A = \oplus_{h\in H} A_h$ graduações de A pelos grupos G e H, respectivamente, tais que $H = G/T$ para algum subgrupo T de G. Se $A_{\bar{g}} = \oplus_{g\in\bar{g}} A_g$, para todo $\bar{g} \in H$, então Γ' é um coarsening de Γ chamado **fator graduado**.*

A próxima definição introduz a noção de álgebras regulares, consideradas por Regev e Seeman em [79]. Tais álgebras serão utilizadas fortemente nos Capítulos 2 e 3, para maiores detalhes ver [4, 13, 79].

Definição 1.2.21. *Seja R uma álgebra e $\Gamma_R\colon R = \oplus_{h\in H} R_h$, uma graduação por um grupo abeliano H. Dizemos que Γ_R é uma graduação **regular** se existir um H-fator de comutação (ou simplesmente fator de comutação) $\beta\colon H \times H \to F^\times$ tal que*

(P1) Para todo n e toda n-upla $(h_1, \ldots, h_n)$ de elementos em H existem $r_1, \ldots, r_n$, com $r_j \in R_{h_j}$, tais que $r_1 \cdots r_n \neq 0$.

(P2) Para todos $h_1, h_2 \in H$ e todos $a_{h_1} \in A_{h_1}$, $a_{h_2} \in A_{h_2}$, temos

$$a_{h_1} a_{h_2} = \beta(h_1, h_2) a_{h_2} a_{h_1}.$$

*Neste caso, a álgebra R é dita **regular** se admitir uma graduação regular por um grupo abeliano H. A H-graduação regular sobre R é **minimal** (ou **não degenerada**) se para qualquer $h \neq \epsilon$ existir h' tal que $\beta(h, h') \neq 1$.*

Observação 1.2.22. *Na definição acima o fator de comutação $\beta\colon H \times H \to F^\times$ é um bicaracter antissimétrico (ver [4, Observação 13]), isto é, para todo $h_0 \in H$ as aplicações $h \mapsto \beta(h_0, h)$ e $h \mapsto \beta(h, h_0)$ são caracteres do grupo H e $\beta(h_2, h_1) = \beta(h_1, h_2)^{-1}$ para todos $h_1, h_2 \in H$.*

Exemplo 1.2.23. *O exemplo mais imediato de álgebra regular é o corpo K. Considerando uma $\mathbb{Z}_n$-graduação sobre o anel de polinômios em uma variável $K[x]$ dada por*

$$K[x] = \bigoplus_{i=0}^{n-1} A_i, \text{ onde } A_i = x^i K[x^n], 0 \leqslant i \leqslant n-1,$$

é exemplo de uma álgebra que possui uma graduação regular que não é minimal. Já a $\mathbb{Z}_2$-graduação natural da álgebra de Grassmann (Exemplo 1.1.5) e a graduação de Pauli de a álgebra das matrizes (Exemplo 1.2.8) são regulares e minimais. Porém, a graduação de $M_n(K)$ dada pelo grupo $\mathbb{Z}_n$ (ver Exemplo 1.2.5) não é regular.

A próxima observação dará um modo de determinar o bicaracter do produto tensorial entre duas álgebras regulares.

Observação 1.2.24. *Sejam A, B álgebras cujas graduações regulares são dadas pelos grupos abelianos G e H, respectivamente. O produto tensorial graduado de $A \otimes_K B$ é regular e o seu correspondente bicaracter $\beta_{A\otimes_K B}\colon (G \times H) \times (G \times H) \to K^\times$ é dado por*

$$\beta_{A\otimes_K B}((g_1, g_2), (h_1, h_2)) = \beta_A(g_1, g_2)\beta_B(h_1, h_2),$$

para todo g_1, $g_2 \in G$ e todo h_1, $h_2 \in H$. Além disso, se A e B são álgebras regulares minimais, então o produto tensorial $A \otimes_K B$ também será regular e minimal, para maiores detalhes ver [13, Proposição 2.1].

Exemplo 1.2.25. *Como aplicação da observação anterior, temos que as álgebras $M_n(E)$ e $E \otimes_K E$ possuem graduações regulares dadas pelos grupos $(\mathbb{Z}_n \times \mathbb{Z}_n) \times \mathbb{Z}_2$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, respectivamente.*

Seja $\beta\colon H \times H \to K^\times$ o bicaracter associado à H-graduação regular de R. Denote por

$$H' = \{h' \in H \mid \beta(h', h) = 1\ , \text{ para todo } h \in H\} \subseteq H. \tag{1.7}$$

É claro que H' é um subgrupo de H e $R_{h'} \subseteq Z(R)$ para todo $h' \in H'$. Consequentemente, o bicaracter β sobre H induzirá um bicaracter $\bar{\beta}$ sobre $\bar{H} = H/H'$. Além disso, a $\bar{H}$-graduação de R induzida pela sua H-graduação é regular e minimal.

Para finalizar está seção iremos definir o envelope de Grassmann, essa definição será utilizada como suporte para os próximos capítulos. A partir de agora uma álgebra $\mathbb{Z}_2$-graduada será chamada de **superálgebra**.

Definição 1.2.26. *Seja $A = A_0 \oplus A_1$ uma superálgebra. O* ***envelope de Grassmann de*** *A é a superálgebra*

$$E(A) = E\hat{\otimes}_K A = (E_0 \otimes_K A_0) \oplus (E_1 \otimes_K A_1).$$

Ressaltamos que no caso de álgebras não associativas a definição de superálgebra exige mais que uma $\mathbb{Z}_2$-graduação. Mais precisamente, uma álgebra $\mathbb{Z}_2$-graduada é uma superálgebra de Lie ou de Jordan, quando $E(A)$ é uma álgebra de Lie, respectivamente de Jordan.

Observação 1.2.27. *O envelope de Grassmann de uma subálgebra A é uma subálgebra do produto tensorial $E \otimes_K A$.*

Exemplo 1.2.28. *Considere a superálgebra para $M_n(K)$ dada no Exemplo 1.2.5, onde $n = a+b$. Podemos considerar o envelope de Grassmann de $M_n(K)$ como sendo a subálgebra da álgebra $M_{a+b}(E)$, denotado por $M_{a,b}(E)$, que consiste de matrizes da forma*

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

onde $A \in M_a(E_0)$, $D \in M_b(E_0)$ e B, C são blocos com entradas em E_1. Esta superálgebra possui componentes homogêneas

$$(M_{a,b}(E))_0 = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \quad e \quad (M_{a,b}(E))_1 = \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}.$$

Agora, considere a álgebra $S = M_2(K)$ e as matrizes de Sylvester abaixo:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Observe que $A^2 = B^2 = I, AB = C = -BA$, portanto uma $\mathbb{Z}_2 \times \mathbb{Z}_2$-graduação de S pode ser obtida considerando as componentes homogêneas

$$S_\epsilon = \langle I_2 \rangle,\ S_a = \langle A \rangle,\ S_b = \langle B \rangle,\ S_c = \langle C \rangle,$$

aqui $c = ab$ e I_2 é a matriz identidade, essa graduação é regular e minimal. Assim,

$$M_{1,1}(E) = E(M_2(K)) = \begin{pmatrix} E_0 & E_1 \\ E_1 & E_0 \end{pmatrix} = E_0 I_2 \oplus E_0 A \oplus E_1 B \oplus E_1 C$$

é uma graduação regular minimal para o envelope de Grassmann $E(M_2(K))$.

Exemplo 1.2.29. *Como aplicação do comentário anterior e da Observação 1.2.24, temos que a álgebra $M_{a,a}(E) \cong M_{1,1}(E) \otimes_K M_a(K)$ é regular minimal com a correspondente graduação produto tensorial.*

1.3 Álgebra Livre

Nesta seção construiremos as Álgebras Livres cuja importância está no fato de serem os ambientes onde serão introduzidos os conceitos de identidades polinomiais e de polinômios centrais utilizados em todo este trabalho. Começaremos com a definição de Álgebras Livres.

Definição 1.3.1. *Seja $\mathcal{C}$ uma classe de álgebras e $F \in \mathcal{C}$ uma álgebra gerada por um conjunto $X \subseteq F$. A álgebra F é dita **livre** na classe $\mathcal{C}$, se ela satisfaz a seguinte propriedade universal: para cada álgebra $A \in \mathcal{C}$ e cada aplicação $h\colon X \to A$ existe um único homomorfismo $F \to A$ estendendo h. Neste caso, dizemos que F é a **álgebra livre na classe $\mathcal{C}$ livremente gerada pelo conjunto** X. Além disso, a cardinalidade $|X|$ do conjunto X será chamada **posto** de F.*

Exemplo 1.3.2. *A álgebra unitária dos polinômios associativos e comutativos nas variáveis $x_1, \ldots, x_n$, denotada por $K[x_1, \ldots, x_n]$, é gerada pelo conjunto $X = \{x_1, \ldots, x_n\}$. Seja A uma álgebra associativa, comutativa e unitária. Dados $a_1, \ldots, a_n$ elementos em A considere a aplicação $\varphi\colon X \to A$ definida por $\varphi(x_i) = a_i$. O homomorfismo $\phi\colon K[x_1, \ldots, x_n] \to A$ dado por $\phi(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$ estende φ. Portanto, $K[x_1, \ldots, x_n]$ é a álgebra livre livremente gerada pelo conjunto X na classe de todas as álgebras associativas, comutativas e unitárias.*

Agora construiremos uma álgebra livre na classe de todas as álgebras unitárias. Seja $X = \{x_\alpha\}$ um conjunto enumerável arbitrário de variáveis não comutativas, adicionamos a este conjunto mais dois símbolos de parênteses "(" e ")", ou seja, parênteses à esquerda e à direita, e obtemos o conjunto $X^* = X \cup \{(\ ,\ )\}$. Considere todas as possíveis sequências finitas de elementos do conjunto X^*. Duas sequências $a_1 a_2 \cdots a_m$ e

$b_1b_2\cdots b_n$ de elementos em X^* são ditas iguais se $m = n$ e $a_i = b_i$ para $i = 1, 2, \ldots, m$. Definimos indutivamente o conjunto $V[X]$ das sequências finitas de elementos sobre o conjunto X^* que chamaremos de **palavras não associativas** de elementos do conjunto X. Primeiro, todos os elementos do conjunto X pertencem a $V[X]$. Segundo, se x_1, $x_2 \in X$ e u, $v \in V[X]\backslash X$ então as sequências x_1x_2, $x_1(u)$, $(v)x_2$ e $(u)(v)$ também pertencem a $V[X]$. Nenhuma outra sequência pertence a $V[X]$, por exemplo, a sequência $(x_1(x_2x_3))x_4$ é uma palavra não associativa de elementos do conjunto $X = \{x_1, x_2, x_3, x_4\}$, mas a sequência $(x_1(x_2x_3)x_4)$ não é. O número de elementos do conjunto X que aparece em uma palavra v é chamado o **comprimento da palavra não associativa $\boldsymbol{v}$**, e será denotado por $\deg(v)$.

Proposição 1.3.3. *Seja v uma palavra não associativa de elementos de algum conjunto. Então:*

(i) O número de parênteses à esquerda em v é igual ao número de parênteses à direita;

(ii) Em qualquer subsequência inicial de v, o número de parênteses à esquerda não é menor que o número de parênteses à direita.

Demonstração. [97, Proposição 1, pág. 2] □

Definimos no conjunto $V[X]$ uma operação binária, denotada por "$\cdot$", de acordo com as regras a seguir. Sejam $x_1, x_2 \in X$ e $u, v \in V[X]\backslash X$. Definimos: $x_1 \cdot x_2 = x_1x_2$; $x_1 \cdot v = x_1(v)$; $u \cdot x_2 = (u)x_2$; $u \cdot v = (u)(v)$.

Proposição 1.3.4. *Toda palavra não associativa v com $\deg(v) \geqslant 2$ tem uma única representação como produto de duas palavras não associativas de comprimento menor.*

Demonstração. [97, Proposição 2, pág. 2] □

Consideramos agora o espaço vetorial $K\{X\}$ cuja sua base seja o conjunto $V[X]$, estendemos a multiplicação em $V[X]$ para elementos de $K\{X\}$ através da regra

$$(\sum_i \alpha_i u_i) \cdot (\sum_j \beta_j v_j) = \sum_{i,j} \alpha_i \beta_j (u_i \cdot v_j)$$

onde α_i, $\beta_j \in K$ e $u_i, v_j \in V[X]$. Com essa multiplicação $K\{X\}$ é uma álgebra. O resultado seguinte comprovará que a álgebra $K\{X\}$ satisfaz a propriedade universal.

Teorema 1.3.5. *A álgebra $K\{X\}$ é livremente gerada pelo conjunto X na classe das álgebras unitárias.*

Demonstração. [97, Teorema 1, pág. 3] □

A álgebra $K\{X\}$ é chamada **álgebra livre com conjunto de geradores livres em** X e seus elementos são chamados **polinômios não associativos**. Um polinômio não associativo da forma αv, onde $\alpha \in K$, $v \in V[X]$, é chamado **monômio não associativo**. O comprimento de v é chamado de **grau do monômio**. O maior grau dos monômios cuja soma constitui um polinômio $f = \sum \alpha_i v_i$ é chamado **grau do polinômio**, denotado por $\deg f = \max\{\deg v_i\}$.

Proposição 1.3.6. *Duas álgebras livres $K\{X\}$ e $K\{Y\}$ são isomorfas se, e somente se, $|X| = |Y|$, isto é, se os conjuntos X e Y possuem a mesma cardinalidade.*

Demonstração. [36, pag. 10] □

Observação 1.3.7. *Uma construção análoga pode ser feita para as álgebras associativas livres, que denotaremos em todo trabalho por $K\langle X\rangle$, basta "retirar" os "(" , ")" da definição e aplicar o associador. Os elementos da álgebra $K\langle X\rangle$ são chamados simplesmente de **polinômios**, os quais são somas formais de **monômios** que por sua vez são produtos formais de um escalar por uma palavra formada por elementos de X.*

Seja G um grupo, então defina para cada g um conjunto enumerável X_g tal que os X_g sejam disjuntos. A álgebra livre $K\{X_G\}$, onde $X_G = \bigcup_{g\in G} X_g$, possui uma G-graduação natural da seguinte forma: Definimos o grau da variável $x \in X_G$ como sendo g se $x \in X_g$, denotado por $\deg_G x = g$. Além disso, definimos o grau do monômio $\alpha(u)(v)$, com $\alpha \in K$ e $u, v \in V[X_G]$, como sendo $(\deg_G u \cdot \deg_G v)$, onde $\deg_G u$ é o grau do monômio u. Da Proposição 1.3.4, o grau de qualquer monômio está bem definido. Não é difícil ver que

$$K\{X_G\} = \bigoplus_{g\in G} K\{X_G\}_g,$$

onde $K\{X_G\}_g$ é o subespaço de $K\{X_G\}$ gerado pelos monômios de grau g, define uma G-graduação para $K\{X_G\}$. Com essa graduação $K\{X_G\}$ é chamada **álgebra G-graduada livre, livremente gerada pelo conjunto** X_G.

Observação 1.3.8. *Seja G um grupo. Pode ser construída, como no caso da álgebra associativa livre, a álgebra associativa G-graduada livre que denotaremos em todo trabalho por $K\langle X_G\rangle$. Para isto basta desconsiderar os "(" , ")" da definição. Os elementos da álgebra $K\langle X_G\rangle$ são chamados simplesmente de **polinômios G-graduados**, os quais são somas formais de **monômios G-graduados** que por sua vez são produtos formais de um escalar por uma palavra formada por elementos de X_G.*

1.4 Identidade Polinomial Graduada

Seja $K\{X\}$ a álgebra livre com unidade livremente gerada por um conjunto enumerável $X = \{x_1, x_2, \ldots\}$. Dado $f \in K\{X\}$, escrevemos $f = f(x_1, \ldots, x_n)$ para indicar que $x_1, \ldots, x_n$ são elementos de X que aparecem em f. Sejam A uma álgebra e o homomorfismo $\varphi\colon K\{X\} \to A$ dado por $\varphi(x_i) = a_i$, para todo $i = 1, \ldots, n$ e $\varphi(x) = 0$ sempre que $x \in X\backslash\{x_1, \ldots, x_n\}$. Denotaremos a imagem de f por este homomorfismo por $f(a_1, \ldots, a_n)$ e diremos que este elemento é obtido pela substituição dos elementos $a_1, \ldots, a_n$ no polinômio não associativo $f(x_1, \ldots, x_n)$.

Definição 1.4.1. *Sejam A uma álgebra e $f = f(x_1, x_2, \ldots, x_n) \in K\{X\}$. Dizemos que f é uma **identidade polinomial de** A (ou identidade polinomial ordinária de A) se $f(a_1, \ldots, a_n) = 0$, para quaisquer $a_1, \ldots, a_n \in A$. Neste caso, diremos que A satisfaz a identidade $f(x_1, \ldots, x_n)$.*

É imediato que o polinômio $f = 0$ (polinômio nulo) é uma identidade polinomial para qualquer álgebra A.

Observação 1.4.2. *Considere $f(x_1, x_2, \ldots, x_n) \in K\{X\}$. Então $f = f(x_1, x_2, \ldots, x_n)$ é uma identidade polinomial de A se, e somente se, f pertence aos núcleos de todos os homomorfismos de $K\{X\}$ em A.*

Definição 1.4.3. *Dizemos que uma álgebra A é uma **PI-álgebra**, se A satisfaz uma identidade polinomial $f \neq 0$.*

Exemplo 1.4.4. *Seja A uma álgebra comutativa. Então, $[x_1, x_2] \in K\{X\}$ é uma identidade polinomial de A. Em particular, toda álgebra comutativa é uma PI-álgebra.*

Exemplo 1.4.5. *Seja A uma álgebra associativa de dimensão finita, digamos* $\dim A < n$. *Então A satisfaz a identidade standard de grau n*

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

onde S_n é o grupo simétrico das permutações de $\{1, 2, \ldots, n\}$ e $(-1)^\sigma$ é o sinal da permutação $\sigma \in S_n$. Assim, toda álgebra de dimensão finita é uma PI-álgebra. Em particular, $M_n(K)$ é uma PI-álgebra.

Exemplo 1.4.6. *(**Teorema de Amistsur e Levitzki**) A álgebra $M_n(K)$ das matrizes de ordem n satisfaz a identidade standard de grau $2n$. Para mais detalhes veja [43, Teorema 1.7.2, pág. 16].*

Seja S um subconjunto de uma álgebra A. Seja $m(x_1, \ldots x_n)$ um monômio qualquer em $K\{X\}$ e $(a_1, \ldots, a_n)$ n-upla de elementos em A tal que pelo menos um a_i pertença a S. Temos da definição de ideal gerado que (S) está contido no ideal gerado pelos elementos da forma $m(a_1, \ldots, a_n)$. O resultado a seguir demonstra a igualdade para o caso em que $A = K\{X\}$. Mais precisamente temos:

Proposição 1.4.7. *Seja $A = K\{X\}$ uma álgebra livre (não necessariamente associativa) e $I \subseteq A$. Então (I) coincide com o conjunto de todas as somas de produtos, em qualquer associação, de elementos de A desde que pelo menos um de seus elementos esteja em I.*

Demonstração. Defina P o conjunto de soma de produtos em qualquer associação de elementos de A desde que pelo menos um de seus elementos estejam em I. Sabemos que P é um ideal de A e $I \subseteq P$, logo $(I) \subseteq P$. Por outro lado, por definição

$$(I) = \bigcap_{J \lhd A; J \supseteq I} J.$$

Seja m um elemento de P, $m = \sum \alpha_i m_i(y_1^{(i)}, \ldots, y_k^{(i)})$. Aqui $\alpha_i \in K$, $m_i(x_1^{(i)}, \ldots, x_k^{(i)}) = m_i$ são monômios em $K\{X\}$, e $y_1^{(i)}, \ldots, y_k^{(i)}$ polinômios em $K\{X\}$, para cada i, onde pelo menos um dos $y_j^{(i)}$'s está em I; digamos $y_1^{(i)}$. Dessa forma todo $m_i \in J$ uma vez que $y_1^{(i)} \in J$ implicando que $m \in J$, para todo ideal J de A que contém I. Portanto $P \subseteq (I)$, ou seja, $(I) = P$. □

Um ideal I de $K\{X\}$ é um **T-ideal** se é invariante por todos os endomorfismos de $K\{X\}$, ou seja, $\varphi(I) \subseteq I$, para todo $\varphi \in End(K\{X\})$. Denotando por $Id(A)$ o conjunto de todas as identidades polinomiais de A, observa-se que $Id(A)$ é um T-ideal. Além disso, considerando A e B álgebras, dizemos que A e B são **PI-equivalentes** se $Id(A) = Id(B)$, denotado por $A \sim_{PI} B$.

A interseção de uma família qualquer de T-ideais ainda é um T-ideal. Portanto, dado um subconjunto S qualquer de $K\{X\}$, podemos definir o ***T*-ideal gerado por** S, o qual denotaremos por $\langle S \rangle_T$, como sendo a interseção de todos os T-ideias de $K\{X\}$ que contêm S. Assim, $\langle S \rangle_T$ é o menor T-ideal de $K\{X\}$ contendo S. Seja A uma álgebra, dizemos que o T-ideal $Id(A)$ é **gerado como T-ideal pelo conjunto** $\{f_i \mid i \in I\}$ se $Id(A) = \langle f_i \mid i \in I \rangle_T$, e dizemos que o conjunto $\{f_i \mid i \in I\}$ é um **base das identidades para** A. Por fim, dizemos que $g \in K\{X\}$ é **consequência das identidades polinomiais** $\{f_i \mid i \in I\}$ se $g \in \langle f_i \mid i \in I \rangle_T$.

Observação 1.4.8. *Considerando $K\langle X \rangle$ a álgebra associativa livre e S um subconjunto de $K\langle X \rangle$, obtemos que $\langle S \rangle_T$ é gerado, como subespaço, pelo conjunto*

$$\{h_1 f(g_1, \ldots, g_n) h_2 \mid h_1, h_2, g_1, \ldots g_n \in K\langle X \rangle \ e \ f \in S\}.$$

Para maiores detalhes ver [36, Observação 2.2.6, pág 23] ou demonstração da Proposição 1.4.7 para o caso associativo.

O conjunto das identidades satisfeitas por todas as álgebras de uma certa classe de álgebras $\mathcal{C}$ também é um ideal de $K\{X\}$. Não é difícil observar que tal ideal de identidades é invariante por endomorfismos de $K\{X\}$, ou seja, é T-ideias. Ele é chamado de **T-ideal da classe** $\mathcal{C}$ e é denotado por $Id(\mathcal{C})$.

Definição 1.4.9. *Seja S um subconjunto de $K\{X\}$. A classe $\mathcal{C}$ de todas as álgebras que têm todos os polinômios de S como identidades é chamada de **variedade definida pelo conjunto** S, denotado por $\mathcal{V}(S)$.*

Exemplo 1.4.10. *$\mathcal{V}(K\{X\})$ consiste da álgebra nula chamada **variedade trivial**.*

Exemplo 1.4.11. *A classe de todas as álgebras associativas é uma variedade definida pelo subconjunto $S = \{(x_1, x_2, x_3)\}$ de $K\{X\}$.*

Exemplo 1.4.12. *A classe de todas as álgebras associativas e comutativas é uma variedade definida pelo subconjunto $S = \{[x_1, x_2], (x_1, x_2, x_3)\}$ de $K\{X\}$ (ou pelo conjunto $\{[x_1, x_2]\}$ de $K\langle X\rangle$).*

Exemplo 1.4.13. *A classe de todas as álgebras de Lie é uma variedade definida pelo subconjunto $S = \{x_1^2, (x_1x_2)x_3 + (x_2x_3)x_1 + (x_3x_1)x_2\}$ de $K\{X\}$.*

Exemplo 1.4.14. *A classe de todas as álgebras de Jordan é uma variedade definida pelo subconjunto $S = \{[x_1, x_2], (x_1^2, x_2, x_1)\}$ de $K\{X\}$.*

Definição 1.4.15. *Seja $\mathcal{V}$ uma variedade de álgebras. Dizemos que uma álgebra $F \in \mathcal{V}$ é uma **álgebra relativamente livre de** $\mathcal{V}$ se existe um subconjunto Y gerador de F tal que para toda álgebra $A \in \mathcal{V}$ e toda aplicação $\rho\colon Y \to A$ existe um único homomorfismo $\varphi\colon F \to A$ que estende ρ. Nestas condições, F é dita **livremente gerada por** Y. Além disso, a cardinalidade de Y é chamada **posto de** F.*

Exemplo 1.4.16. *$K\langle X\rangle$ é relativamente livre, livremente gerada por X, na variedade $\mathcal{V} = \mathcal{V}(\{(x_1, x_2, x_3)\})$.*

Se $I \subseteq K\{X\}$ denotamos por $I(A)$ o ideal da álgebra A gerado por todos os elementos da forma $f(a_1, \ldots, a_n)$, onde $f \in I$ e $a_1, \ldots, a_n \in A$. O teorema seguinte caracteriza as álgebras relativamente livres em qualquer variedade.

Teorema 1.4.17. *Seja $\mathcal{V}$ uma variedade não trivial de álgebras determinada por um conjunto $I \subset K\{X\}$. Então para qualquer conjunto Y a restrição a Y do homomorfismo canônico $\pi\colon K\{Y\} \to K\{Y\}/I(K\{Y\})$ é injetivo e a álgebra $K_{\mathcal{V}}\{\pi(Y)\} = K\{Y\}/I(K\{Y\})$ é livre na variedade $\mathcal{V}$ com conjunto gerador $\pi(Y)$. Quaisquer duas álgebras relativamente livres em $\mathcal{V}$ com conjuntos geradores livres e de mesma cardinalidade, são isomorfas.*

Demonstração. Ver [97, Teorema 2, pág. 4] □

É fácil observar que as variedades de álgebras associativas e de Jordan são não triviais. Portanto elas possuem álgebras livres para qualquer conjunto gerador X, que denotaremos por $K\langle X\rangle$ e $J\{X\}$, respectivamente. Em geral, a álgebra livre na variedade $\mathcal{V}$ com conjunto de geradores X, será denotada por $K_{\mathcal{V}}\{X\}$.

Corolário 1.4.18. *Seja $\mathcal{V} = \mathcal{V}(I)$ uma variedade determinada por um conjunto $I \subset K\{X\}$, então $Id(\mathcal{V}) = I(K\{X\})$.*

Demonstração. Ver [97, pág. 6] □

Observação 1.4.19. *Ao estudar álgebras em uma variedade $\mathcal{V}$ iremos chamar um elemento $f \in K_{\mathcal{V}}\{X\}$ de identidade para a álgebra A se alguma imagem inversa de f pelo homomorfismo canônico (e consequentemente todas as imagens inversas de f) em $K\{X\}$ forem identidade para A.*

Seja f um polinômio não associativo arbitrário em $K\{X\}$. Podemos representar $f = f(x_1, \ldots, x_n)$ na forma $f = \sum_{i=0}^{k_1} f_1^{(i)}$, onde $f_1^{(i)}$ é a soma de todos os monômios do polinômio f que têm grau i na variável x_1. Continuando esse processo, podemos agrupar os monômios que possuem o mesmo multigrau $(\alpha_1, \ldots, \alpha_n)$ nas variáveis $x_1, \ldots, x_n$. Esses polinômios serão chamados **componentes homogêneas** do polinômio f.

Definição 1.4.20. *Sejam $m \in K\{X\}$ um monômio e $x_i \in X$. Definimos o grau de m em x_i, denotado por $\deg_i m$, como sendo o número de ocorrências de x_i em m. Um polinômio $f \in K\{X\}$ é dito **homogêneo** em x_i, se todos os seus monômios têm o mesmo grau em x_i. Em particular, um polinômio em $K\{X\}$ é dito **multihomogêneo** quando é homogêneo em todas as variáveis.*

Dado $m = m(x_1, \ldots, x_k)$ um monômio em $K\{X\}$ e se para todo $\lambda_1, \ldots, \lambda_k \in K$, temos

$$m(\lambda_1 x_1, \ldots, \lambda_k x_k) = \lambda_1^{\alpha_1} \cdots \lambda_k^{\alpha_k}(x_1, \ldots, x_k)$$

definiremos o **multigrau** de m como sendo a k-upla $(\alpha_1, \ldots, \alpha_k)$. Sendo $f \in K\{X\}$ a soma de todos os monômios de f com um dado multigrau é chamado de **componente multihomogênea** de f. Quando $f \in K\{X\}$ possui uma única componente multihomogênea, dizemos que f é **multihomogêneo**. Por fim, $f \in K\{X\}$ é **multilinear** se é multihomogêneo de multigrau $(1, 1, \ldots, 1)$.

Exemplo 1.4.21. *O polinômio $f(x_1, x_2, x_3) = x_1 x_2^2 + x_2 x_1 x_3^2$ em $K\langle X\rangle$ é homogêneo em x_1, mas não é multihomogêneo.*

Prosseguiremos com a definição de identidade polinomial graduada. Consideremos G um grupo cujo elemento neutro será denotado por ϵ e $K\{X_G\}$ a álgebra livre G-graduada. Dado $f \in K\{X_G\}$, escrevemos $f = f(x_{1,g_1}, \ldots, x_{n,g_n})$ para indicar que $x_{1,g_1}, \ldots, x_{n,g_n}$ são elementos de X_G que aparecem em f onde $\deg_G x_i = g_i$. Sejam A uma álgebra graduada pelo grupo G e $\varphi\colon K\{X_G\} \to A$ o homomorfismo G-graduado dado por $\varphi(x_{i,g_i}) = a_i$, para todo $i = 1, \ldots, n$ e $\varphi(x) = 0$ sempre que $x \in X_G \backslash \{x_{1,g_1}, \ldots, x_{1,g_1}\}$. Denotaremos a imagem de f por este homomorfismo por $f(a_1, \ldots, a_n)$ e diremos que este elemento é obtido pela **substituição f-admissível** $(a_1, \ldots, a_n)$ no polinômio G-graduado não associativo $f(x_{1,g_1}, \ldots, x_{n,g_n})$.

Definição 1.4.22. *Seja $A = \bigoplus_{g \in G} A_g$ uma álgebra G-graduada. Diremos que o polinômio $f(x_{1,g_1}, \ldots, x_{n,g_n}) \in K\{X_G\}$ é uma **identidade polinomial G-graduada** de A se $f(a_1, \ldots, a_n) = 0$ para toda substituição f-admissível de elementos em A.*

Se A é uma álgebra G-graduada, denotaremos por $Id_G(A) \subset K\{X_G\}$ o conjunto das identidades graduadas satisfeitas pela álgebra A. Não é difícil observar que tal conjunto é um ideal homogêneo de $K\{X_G\}$ invariante por endomorfismos graduados, ou seja, $Id_G(A)$ é um T_G-ideal. Ainda consideraremos uma definição análoga à de PI-equivalência da seguinte forma: Sejam A e B álgebras G-graduadas, dizemos que A e B são **G-PI-equivalentes** se $Id_G(A) = Id_G(B)$, denotado por $A \sim_{PI}^{G} B$. A proposição seguinte é um resultado clássico da PI-teoria. Por tal motivo decidimos omitir sua demonstração. O resultado relaciona as álgebra G-PI-equivalentes com as PI-equivalentes.

Proposição 1.4.23. *Sejam A e B duas álgebras. Se A e B possuem G-graduações tais que $Id_G(A) \subseteq Id_G(B)$, então $Id(A) \subseteq Id(B)$. Além disso, se $A \sim_{PI}^{G} B$, então $A \sim_{PI} B$.*

Observação 1.4.24. *Observa-se que a recíproca do resultado anterior é **falsa**. Basta observar que $[x_{1,\bar{0}}, x_{2,\bar{0}}]$ é identidade $\mathbb{Z}_2$-graduada para $E = E_0 \oplus E_1$, mas não é para a graduação trivial de E.*

Proposição 1.4.25. *Seja A uma álgebra. Então,*

(i) Se o corpo K é infinito, todas identidades polinomiais graduadas de A seguem de suas identidades graduadas multihomogêneas;

(ii) Se o corpo K tem característica zero, todas as identidades polinomiais graduadas de A seguem de suas identidades multilineares graduadas.

Demonstração. Podemos observar que o resultado de (i) segue de uma pequena "adaptação" na demonstração do [97, Corolário 1, pág. 8] e o item (ii) segue de [97, Proposição 4, pág. 15] e aplicando indução. Tal resultado pode ser demonstrado usando ideia análoga ao que foi feito em [43, Corolário 1.3.9, pág. 9], indicamos também [30, Corolário 1.39, pág. 16]. □

Observação 1.4.26. *O último resultado é válido para álgebras cuja graduação é dada pelo grupo trivial, ou seja, para o caso do T-ideal das identidades ordinárias.*

1.5 Polinômios Centrais Graduados

Definição 1.5.1. *Seja A uma álgebra com unidade, consideramos $\mathcal{Z}(A)$, o centro de A. Dizemos que $f = f(x_1, \ldots, x_n) \in K\{X\}$ é um* ***polinômio central*** *para A se f tem termo constante nulo e $f(a_1, \ldots, a_n) \in \mathcal{Z}(A)$, para quaisquer $a_1, \ldots, a_n \in A$. Denotaremos por $C(A) \subseteq K\{X\}$ o conjunto de todos os polinômios centrais de A. Além disso, dizemos que f é um* ***polinômio central próprio*** *para A se $f \in C(A) \backslash Id(A)$, ou seja, f é um polinômio central para A que não é identidade.*

Consideraremos nesta seção que A será uma álgebra associativa com unidade. Assim, o centro será denotado por $Z(A)$ e de acordo com esta definição, dizer que f é um polinômio central para A significa dizer que $[f, g]$ é uma identidade polinomial para A, para todo polinômio $g \in K\langle X\rangle$. Segue que se duas álgebras são PI-equivalentes, então elas têm exatamente os mesmos polinômios centrais.

Vejamos alguns exemplos:

Exemplo 1.5.2. *As identidades polinomiais de A são claramente polinômios centrais. Chamamos esses polinômios de* ***polinômios centrais triviais****.*

Exemplo 1.5.3. *Seja $A = M_2(K)$. Então $f(x_1, x_2) = [x_1, x_2]^2$ é um polinômio central não trivial de A.*

Exemplo 1.5.4. *Sejam K um corpo qualquer e E a álgebra de Grassmann sobre K. Temos que $f(x_1, x_2) = [x_1, x_2]$ é um polinômio central para E. Se $charK = p > 0$, temos que $g(x) = x^p$ também é um polinômio central para E.*

Como no caso das identidades, a definição seguinte é um análogo para polinômios centrais.

Definição 1.5.5. *Seja A uma álgebra com unidade, graduada por um grupo G. Dizemos que $f = f(x_{1g_1}, \ldots, x_{ng_n}) \in K\langle X_G\rangle$ é um* ***polinômio central G-graduado*** *para A se f tem termo constante nulo e $f(a_1, \ldots, a_n) \in Z(A)$ para toda substituição f-admissível de elementos em A. Denotaremos por $C_G(A) \subseteq K\langle X_G\rangle$ o conjunto de todos os polinômios centrais G-graduados de A. Dizemos que f é um* ***polinômio central G-graduado próprio*** *para A se $f \in C_G(A) \backslash Id_G(A)$.*

Definição 1.5.6. *Um subespaço V de $K\langle X_G\rangle$ é dito ser um* ***T_G-espaço*** *se $\varphi(V) \subseteq V$, para todo $\varphi \in End(K\langle X_G\rangle)$.*

É fato conhecido que dado um subconjunto $\{h_i \mid i \in \mathbb{N}\}$ de $K\langle X_G\rangle$, existe um único endomorfismo φ de $K\langle X_G\rangle$ tal que $\varphi(x_i) = h_i$, para todo $i \in \mathbb{N}$. Assim, dizer que V é um T_G-espaço de $K\langle X_G\rangle$ significa dizer que V é um subespaço de $K\langle X_G\rangle$ tal que $f(h_1, \ldots, h_n) \in V$, para quaisquer $f(x_{1g_1}, \ldots, x_{ng_n}) \in V$ e substituição f-admissível $(h_1, \ldots, h_n)$ de elementos em $K\langle X_G \rangle$.

Exemplo 1.5.7. *Todo T_G-ideal de $K\langle X_G \rangle$ é um T_G-espaço. O corpo K é também um exemplo de T_G-espaço de $K\langle X_G \rangle$.*

Podemos verificar que a interseção de uma família qualquer de T_G-espaços ainda é um T_G-espaço. Assim, dado um subconjunto S de $K\langle X_G \rangle$ podemos definir $\langle S \rangle^{T_G}$ o **T_G-espaço de $K\langle X \rangle$ gerado por** S, como sendo a interseção de todos os T_G-espaços que contêm S, ou seja, $\langle S \rangle^{T_G}$ é o menor T_G-espaço que contém S. O próximo resultado nos dará uma caracterização do T_G-espaço gerado por um conjunto e omitiremos sua demonstração.

Proposição 1.5.8. *Se $S \subseteq K\langle X_G \rangle$ e $V = \langle S \rangle^{T_G}$, então V é o subespaço de $K\langle X_G \rangle$ gerado por*

$$\{f(h_1, \ldots, h_n) \,|\, f \in S, (h_1, \ldots, h_n) \text{ substituições } f\text{-admissíveis por elementos de } K\langle X_G \rangle\}.$$

Segue da Observação 1.4.8 e da proposição anterior que a partir de uma base de um T-ideal é possível construir um conjunto capaz de gerá-lo como **T-espaço**.

1.6 Polinômio Mínimo Genérico

Uma álgebra A (não necessariamente associativa) é chamada **associativa nas potências** se as subálgebras geradas por um único elemento são associativas e A é chamada **fortemente associativa nas potências** se A_F, a álgebra obtida estendendo o corpo base K de A a um corpo F, é associativa nas potências para todo F.

Seja A uma álgebra associativa nas potências de dimensão finita e $\{u_1, \ldots, u_n\}$ uma base de A sobre K. Fixando um elemento a qualquer em A, é claro que o conjunto $\{1, a, a^2, \ldots, a^{n-1}, a^n\}$ é linearmente dependente sobre K. Logo existem α_0, α_1, $\ldots$, α_{n-1}, escalares em K, tais que

$$a^n + \alpha_{n-1} \cdot a^{n-1} + \cdots + \alpha_1 \cdot a + \alpha_0 \cdot 1 = 0.$$

Seja λ uma variável e considerando $f_a(\lambda) = \lambda^n + \alpha_{n-1} \cdot \lambda^{n-1} + \cdots + \alpha_1 \cdot \lambda + \alpha_0$ o polinômio mônico em $K[\lambda]$, temos que $f_a(a) = 0$. Assim, para cada $a \in A$, podemos definir um polinômio mônico $\mu_a(\lambda)$ em $K[\lambda]$ de grau mínimo, tal que $\mu_a(a) = 0$. Agora, consideremos indeterminadas ξ_1, $\ldots$, ξ_n e $P = K(\xi_1, \ldots, \xi_n)$ o corpo de frações do anel de polinômios nas indeterminadas ξ_i's (variáveis comutativas, associativas e algebricamente independentes sobre K) com coeficientes em K. Formamos então a álgebra A_P e consideramos o elemento

$$x = \sum_{i=1}^{n} \xi_i u_i \tag{1.8}$$

da álgebra A_P. Chamaremos o elemento (1.8) de **elemento genérico da álgebra** A **sobre** K. Como $\dim_P A_P = \dim_K A$ então podemos considerar

$$m_{x,P}(\lambda) = \lambda^s - \sigma_1(x)\lambda^{s-1} + \cdots + (-1)^s\sigma_s(x) \tag{1.9}$$

o polinômio minimal mônico de x como elemento da álgebra $P[\lambda]$, onde $\sigma_i(x) \in P$ para cada $i = 1, 2, \ldots, s$. Assim, para todo $a = \sum_{i=1}^{n} \alpha_i u_i$ em A, com $\alpha_i \in K$, podemos definir uma especialização substituindo ξ_i por α_i em (1.9). Essa relação implica que se colocarmos

$$m_{a,P}(\lambda) = \lambda^s - \sigma_1(a)\lambda^{s-1} + \cdots + (-1)^s\sigma_s(a),$$

então teremos $m_{a,P}(a) = 0$ em A. Estes coeficientes independem da escolha da base de A sobre K e da extensão do corpo base. Denotaremos o coeficiente $\sigma_1(a)$ por $Trd(a)$, então $m_{a,P}(\lambda)$ e $Trd(a)$ serão chamados o **polinômio mínimo genérico** e **traço genérico**, respectivamente, de $a \in A$. Claramente o grau s de $m_{x,P}(\lambda)$ será menor ou igual do que n e o chamaremos de **o grau da álgebra** A. Para maiores detalhes ver [50, Capítulo VI, Seção 3].

Teorema 1.6.1. *[50, Capítulo VI, Teorema 1] Seja A uma álgebra fortemente associativa nas potências de dimensão finita com unidade e de grau s, e sejam $m_a(\lambda)$, $Trd(a)$ o polinômio mínimo genérico e o traço genérico de $a \in A$, respectivamente. Então:*

(a) Trd é K-linear;

(b) $Trd(1) = s$;

(c) Se η é um isomorfismo ou anti-isomorfismo de A em A' então $m_{\eta(a)}(\lambda) = m_a(\lambda)$.

Corolário 1.6.2. *Seja A uma álgebra fortemente associativa nas potências de dimensão finita com unidade e de grau s. Então os coeficientes do polinômio mínimo genérico são invariantes pela ação do grupo dos automorfismos de A.*

Definição 1.6.3. *Uma álgebra A de dimensão finita é chamada **separável** se A_F é uma soma direta de ideais simples para toda extensão de corpos F do corpo base K.*

Podemos definir, a partir da aplicação linear $Trd\colon A \to K$, uma aplicação bilinear $Trd\colon A \times A \to K$ dada por $Trd(a, b) = Trd(ab)$. O seguinte critério nos ajudará a determinar se esta aplicação é não degenerada em álgebras associativas ou de Jordan.

Teorema 1.6.4. *[50, Teorema 5, Pag. 240] Seja A uma álgebra com unidade de dimensão finita que seja associativa ou de Jordan. Então A é separável se, e somente se, a forma bilinear traço genérico Trd for não degenerada.*

Consideramos A uma álgebra que seja associativa ou de Jordan. É bem conhecido que se A for central simples, então A_F é simples para qualquer extensão F do corpo base K. Portanto, toda álgebra central simples de dimensão finita que seja associativa ou de Jordan é separável. Logo, se A for central simples de dimensão finita com unidade, então A possui traço genérico Trd não degenerado. Por fim, um resultado importante é a propriedade cíclica e associativa do traço, que iremos enunciar a seguir.

Proposição 1.6.5. *[50, Corolário 4, pág. 227] Seja A uma álgebra que seja associativa ou de Jordan. Então o traço genérico de A é simétrico e associativo, isto é, para todos elementos a, b e c em A temos $Trd([a,b]) = Trd((a,b,c)) = 0$.*

1.7 Álgebras de Jordan

Nesta seção temos a finalidade de fixar notação apresentando conceitos e resultados básicos da teoria estrutural das álgebras de Jordan, assim como os teoremas de classificação das álgebras de Jordan simples de dimensão finita sobre um corpo algebricamente fechado. Estabelecemos na Definição 1.1.3 o que é uma álgebra de Jordan e lembramos que as álgebras consideradas nesta seção serão definidas sobre um corpo arbitrário de característica diferente de 2, reservando o símbolo K para denotar tal corpo. Utilizamos como referência principal desta seção o livro [50]. Antes de cumprir com este objetivo iremos nos familiarizar com algumas definições e exemplos a respeito das álgebras com involução, uma vez que tais álgebras possuem uma estreita relação com as álgebras de Jordan simples.

Definição 1.7.1. *Seja A uma álgebra associativa. Dizemos que um automorfismo de grupos abelianos aditivos $*\colon A \to A$ é uma **involução** de A, se*

$$a^{**} = a \qquad e \qquad (ab)^* = b^* a^*,$$

para quaisquer $a, b \in A$. Uma álgebra A com involução $*$ é denotada por $(A, *)$.

Seja $(A, *)$ uma álgebra associativa unitária com involução, e seja $Z(A)$ o centro da álgebra A. Denotamos $Z(A, *) = \{a \in Z(A) \mid a^* = a\}$ o centro de $(A, *)$.

Definição 1.7.2. *Diremos que a involução $(*)$ sobre a álgebra A é do **primeiro tipo** se $Z(A) = Z(A, *)$. Caso contrário, dizemos que $(*)$ é do **segundo tipo**.*

Definição 1.7.3. *Seja $(A, *)$ uma álgebra com involução. Dizemos que um ideal I de A é um **$*$-ideal de** A (ou ideal com involução) se $I^* \subseteq I$, onde $I^* = \{a^* \mid a \in I\}$.*

Vejamos alguns exemplos de involuções.

Exemplo 1.7.4. *A aplicação $t\colon M_n(K) \to M_n(K)$, definida por A^t = transposta de A, é uma involução do* ***primeiro tipo*** *em $M_n(K)$, chamada de* ***involução transposta****.*

Exemplo 1.7.5. *A aplicação $s\colon M_{2n}(K) \to M_{2n}(K)$, definida por*

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^s = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix}$$

onde A, B, C, $D \in M_n(K)$, é uma involução do ***primeiro tipo*** *em $M_{2n}(K)$, chamada de* ***involução simplética****.*

Exemplo 1.7.6. *Considerarmos $A = A_1 \oplus A_2$, onde $A_i = M_n(K)$ e $\vartheta(x, y) = (y^t, x^t)$, temos que (A, ϑ) é uma álgebra com involução do* ***segundo tipo****.*

Exemplo 1.7.7. *A aplicação $h\colon M_n(\mathbb{C}) \to M_n(\mathbb{C})$ dada por $A \mapsto (\overline{A})^t$, a transposta e conjugada da matriz A, é uma involução do segundo tipo. Esta é a involução* ***transposta hermitiana****.*

Definição 1.7.8. *Seja $(A, *)$ uma álgebra com involução. Os elementos a de A tais que $a^* = a$ são chamados* ***$*$-simétricos****. Seja (J) uma involução sobre A do mesmo tipo que $(*)$ dizemos que $(*)$ e (J) são* ***involuções equivalentes*** *se $* = J \circ Int_a$, para algum elemento $*$-simétrico $a \in U(A)$. Aqui Int_a é o automorfismo interno definido pelo elemento $a \in U(A)$.*

Definição 1.7.9. *Sejam $(A, *)$ e (B, η) álgebras com involução. Dizemos que uma aplicação $\psi\colon (A, *) \to (B, \eta)$ é um* ***homomorfismo com involução*** *se $\psi\colon A \to B$ é um homomorfismo de álgebras tal que $\psi(a^*) = \psi(a)^\eta$, para todo $a \in A$. O conjunto dos elementos em $Aut_K(A)$ que são homomorfismos com involução será denotado por $Aut_K(A, *)$.*

Estamos interessados em descrever o grupo de automorfismos das álgebras associativas simples com involução de dimensão finita com grau maior ou igual do que 3 sobre um corpo algebricamente fechado. Argumentaremos que tais grupos serão os denominados “grupos unitários”.

Seja (A, ζ) uma álgebra simples de dimensão finita com involução e com grau maior ou igual do que 3, Z o centro de (A, ζ) que contém K e F um corpo algebricamente fechado que contém Z. Observe que a restrição de ζ é um automorfismo sobre Z de ordem 2. Além disso, tome σ uma involução sobre A que coincida com ζ sobre o centro Z, então $\varphi = \sigma\zeta^{-1}$ é um automorfismo sobre A fixando o corpo Z. Da Proposição 1.1.43 temos que φ é interno, ou seja, $\varphi = Int_a$, para algum $a \in U(A)$. Consequentemente, por $\sigma(x) = a\zeta(x)a^{-1}$ e $\sigma^2 = id$ temos

$$x = \sigma^2(x) = a\zeta(\sigma(x))a^{-1} = a\zeta(a)^{-1}x\zeta(a)a^{-1}, \text{ para todo } x \in A,$$

implicando que $\zeta(a)a^{-1} \in Z$.

Se ζ é uma involução do primeiro tipo, então do Teorema 1.1.42 temos que A_F é isomorfa a $M_n(F)$, para algum n. Concluímos que ζ é equivalente a uma das involuções transposta ou simplética, este último caso acontecendo só se n for par. Para maiores detalhes ver [82, Corolário 3.1.58, pág. 168].

Caso ζ seja uma involução do segundo tipo com $[Z\colon K] = 2$, aplicando novamente o Teorema 1.1.42 temos que

$$A_F \simeq (A_Z)_F = (A \otimes_K Z) \otimes_Z F \simeq M_n(F) \otimes_K Z \simeq M_n(F) \oplus M_n(F).$$

Concluímos que ζ é equivalente à involução dada no Exemplo 1.7.11, para maiores detalhes ver [50, Seção V.7, pág. 206] ou [68, Seção 2.3.3, pág. 83].

Consideremos A a álgebra das matrizes de ordem n sobre F, então dado $\varphi \in Aut_K(A, *)$, para alguma involução, pela Proposição 1.1.43, existe $g \in GL_n(F)$ tal que $\varphi(x) = g^{-1}xg$. Por outro lado, a hipótese implica que $\varphi(x^*) = \varphi(x)^*$, portanto $g \cdot x^* \cdot g^{-1} = (g \cdot x \cdot g^{-1})^*$. Isto implica a existência de $z \in Z$ tal que $g^* \cdot g = z$. Consequentemente, podemos definir o grupo

$$G = U_n(K) = \{X \in GL_n(K) \mid X^*X \in Z\}$$

chamado de **grupo unitário associado a involução** $(*)$, observe que $g \in G$. Por fim, podemos afirmar que $Aut_K(A, *) = G/Z(G)$.

Estamos prontos para dar continuidade aos estudos sobre álgebras de Jordan.

Definição 1.7.10. *Uma* ***álgebra de Jordan especial*** *é um subespaço vetorial de uma álgebra associativa A fechado em relação ao produto de Jordan. As álgebras de Jordan que não são especiais são chamadas de* ***excepcionais****.*

Exemplo 1.7.11. *Seja $(A, *)$ uma álgebra associativa com involução. O conjunto*

$$H(A, *) = \{u \in A \mid u^* = u\} \subset A^{(+)}$$

é fechado com relação ao produto de Jordan e involução $(*)$, portanto $(H(A, *), \circ)$ é uma álgebra de Jordan especial. Por simplicidade de notação denotaremos tal álgebra por $H(A, *)$.

É claro que qualquer subespaço vetorial de A fechado em relação ao produto de Jordan é uma subálgebra de $A^{(+)}$ e, por consequência, uma álgebra de Jordan especial. Além disso, se J é uma álgebra de Jordan e $\iota\colon J \to A^{(+)}$ é um homomorfismo entre álgebras de Jordan, então $e = \iota(1)$ é um elemento idempotente de A e

$$\iota(x) = \iota(1x) = \frac{e\iota(x) + \iota(x)e}{2},$$

para todo $x \in J$. Portanto, $e\iota(x) = (e\iota(x) + e\iota(x)e)/2$, e consequentemente, $e\iota(x) = e\iota(x)e$ (analogamente, $\iota(x)e = e\iota(x)e$). Assim,

$$e\iota(x) = e\iota(x)e = \iota(x)e = \frac{(e\iota(x) + \iota(x)e)e}{2} = \frac{e\iota(x) + \iota(x)e}{2} = \iota(x),$$

implicando que $\iota(J)$ está contido na subálgebra unitária eAe, cuja unidade é o elemento e. Isto motiva a seguinte definição.

Definição 1.7.12. *Seja J uma álgebra de Jordan unitária sobre um corpo K. Um par $(\mathcal{U}, \iota)$, onde $\mathcal{U}$ é uma álgebra associativa sobre o mesmo corpo K e $\iota\colon J \to \mathcal{U}^{(+)}$ um homomorfismo de álgebras de Jordan unitárias, é dita ser uma **álgebra universal envolvente unitária** de J se para qualquer álgebra associativa unitária A e qualquer homomorfismo $\sigma\colon J \to A^{(+)}$ de álgebras de Jordan unitárias, existir um único homomorfismo de álgebras associativas $\bar{\sigma}\colon \mathcal{U} \to A$ tal que $\sigma = \bar{\sigma}\iota$. Denotaremos $\mathcal{U}$ por $\mathcal{U}(J)$.*

Exemplo 1.7.13. *Observa-se, por [50, Seção 3.4] que:*

(a) $\mathcal{U}(M_n(K)^{(+)}) = M_n(K) \oplus M_n(K)^{op}$, onde $M_n(K)^{op}$ é a álgebra das matrizes com a multiplicação $A_1 \cdot A_2 = A_2A_1$, $\iota(X) = (X, X)$, para $n \geqslant 3$;

(b) $\mathcal{U}(H(M_n(K), t)) = M_n(K)$, para $n \geqslant 3$ com ι a aplicação inclusão; e

(c) $\mathcal{U}(H(M_{2n}(K), s)) = M_{2n}(K)$, para $n \geqslant 3$ com ι a aplicação inclusão.

Daremos a seguir algumas propriedades dessas álgebras envolventes.

Teorema 1.7.14. *[50, Seção 2.1, Teorema 1] Sejam J uma álgebra de Jordan sobre K e $(\mathcal{U}(J), \iota)$ sua álgebra universal envolvente unitária.*

(1) Se $(\mathcal{U}(J)', \iota')$ é também uma álgebra universal envolvente unitária de J, então existe um único isomorfismo $\mu\colon \mathcal{U}(J) \to \mathcal{U}(J)'$ tal que $\iota' = \iota\mu$. Em particular, $\mathcal{U}(J)$ é única a menos de isomorfismo.

(2) ι é injetivo se, e somente se, J é especial.

(3) $\mathcal{U}(J)$ é gerada, como álgebra, por $\iota(J)$.

(4) Se F é uma extensão do corpo K, então $(\mathcal{U}(J)_F, \iota \otimes_K id)$ é a álgebra universal envolvente unitária da álgebra de Jordan J_F.

(5) Se $\dim_K J = n$, então $\dim_K \mathcal{U}(J) \leqslant 2^n$.

Exemplo 1.7.15. *Seja V um espaço vetorial de dimensão n que possui uma forma bilinear simétrica f. Consideremos o espaço vetorial $B_n(K) = K \oplus V$ munido com o produto:*

$$(\alpha \cdot 1_K + x) \diamond (\beta \cdot 1_K + y) = (\alpha\beta + f(x, y)) \cdot 1 + (\beta x + \alpha y),$$

*onde $\alpha, \beta \in K$ e $x, y \in V$. O conjunto $(B_n(K), \diamond)$ é uma álgebra de Jordan especial e sua álgebra associativa universal é a álgebra de Clifford da forma f. Além disso, se f é não degenerada e $\dim_K V > 1$ então $(B_n(K), \diamond)$ é simples. Por fim, é conhecido que, sobre um corpo algebricamente fechado, o grupo dos automorfismos de $(B_n(K), \diamond)$ é isomorfo ao grupo ortogonal que preserva a forma em V. Dizemos que $B_n(K)$ é uma **álgebra de Jordan do tipo** $\mathcal{D}$.*

Considerando as álgebras associativas centrais simples de grau maior ou igual do que 3, o resultado seguinte relaciona as álgebras associativas com involução e as álgebras de Jordan obtidas de seus elementos invariantes pela involução (elementos simétricos).

Teorema 1.7.16. *Se $(A, *)$ e $(A', *')$ são álgebras centrais simples associativas de dimensão finita com involução e de graus $\geqslant 3$, então elas são isomorfas se e somente se as álgebras de Jordan $H(A, *)$, $H(A', *')$ são isomorfas.*

Demonstração. Ver [50, Teorema 11, pag. 210] □

Pelo teorema anterior temos que o grupo dos automorfismos de $H(A, *)$ e $Aut_K(A, *)$ coincidem. Portanto, considerando K um corpo algebricamente fechado, temos os seguintes resultados.

Exemplo 1.7.17. *Seja $A = A_1 \oplus A_2$ onde $A_i = M_n(K)$ e $\vartheta(x, y) = (y^t, x^t)$ (ver Exemplo 1.7.6). A álgebra $H(A, \vartheta)$ será chamada **álgebra de Jordan do tipo** $\mathcal{A}$. Além disso, $H(A, \vartheta)$ é central simples e $Aut(H(A, \vartheta)) = Aut(A, \vartheta) = U_n(K)/Z(U_n(K)) = PU_n(K)$ é o grupo projetivo unitário.*

Exemplo 1.7.18. *Consideramos $A = M_n(K)$ munida de uma involução do primeiro tipo $(*)$. Dizemos que $H(M_n(K), t)$ é uma **álgebra de Jordan do tipo** $\mathcal{B}$ e $H(M_{2n}(K), s)$ é do **tipo** $\mathcal{C}$. Isto implica que o grupo dos automorfismos de $H(A, *)$ é isomorfo ao grupo projetivo ortogonal ou projetivo simplético, respectivamente.*

Exemplo 1.7.19. *Por fim, seja $A = H(\mathbb{O}_3)$, as matrizes simétricas de ordem 3 sobre $\mathbb{O}$, isto é, a álgebra de Albert. A álgebra A é de Jordan, excepcional, simples e de dimensão 27, ver [50]. O grupo $G = Aut_K(A)$ é simples do tipo F_4, para maiores detalhes ver [52]. Dizemos que $H(\mathbb{O}_3)$ é uma **álgebra de Jordan do tipo** $\mathcal{E}$.*

A seguir enunciaremos a classificação completa das álgebras de Jordan centrais simples de dimensão finita sobre um corpo de característica diferente de 2, tal classificação pode ser encontrada em [60, Teorema 37.2].

Teorema 1.7.20. *Uma álgebra de Jordan central simples de dimensão finita é isomorfa a uma álgebra da seguinte lista:*

(i) A álgebra de Jordan de uma forma bilinear, simétrica e não degenerada num espaço vetorial de dimensão $\geqslant 2$;

(ii) Uma álgebra de Jordan $H(A,*)$, onde A é uma álgebra associativa P-central simples munida de uma involução $(*)$, com P sendo uma extensão quadrática de K e $(*)$ uma involução do segundo tipo ou $P = K$ e $(*)$ sendo uma involução do primeiro tipo; ou

(iii) Uma álgebra de Jordan excepcional de dimensão 27.

Podemos reformular o teorema anterior, mas sob a condição do corpo base ser algebricamente fechado.

Teorema 1.7.21. *Uma álgebra de Jordan central simples sobre um corpo algebricamente fechado é, a menos de isomorfismo, igual a $\mathcal{A}$ (Exemplo 1.7.17), $\mathcal{B}$ (Exemplo 1.7.18), $\mathcal{C}$ (Exemplo 1.7.18), $\mathcal{D}$ (Exemplo 1.7.15) ou $\mathcal{E}$ (Exemplo 1.7.19) listados anteriormente.*

Observação 1.7.22. *Seja J uma álgebra de Jordan especial com unidade de dimensão finita e $(\mathcal{U},\iota)$ sua álgebra universal envolvente unitária, então J_F é uma álgebra de Jordan especial e $(\mathcal{U}_F, \iota \otimes_K id)$ é a sua álgebra universal envolvente unitária, para toda F extensão do corpo K. Como o polinômio minimal do elemento genérico x de J dado na Eq. (1.9) independe da extensão do corpo K, podemos então considerá-lo tomado na extensão F o qual denotaremos por $m_{x,J}(\lambda)$. Como $J \subseteq \mathcal{U}^{(+)} \subseteq \mathcal{U}$, nós podemos complementar a base de J para uma base de $\mathcal{U}$ e assim introduzir mais variáveis em F, digamos $F[\xi]$. Obtemos um elemento genérico $\bar{x}$ de $\mathcal{U}$ cujo polinômio minimal em $P[\xi]$ será denotado por $m_{\bar{x},\mathcal{U}}(\lambda)$. Colocando $\xi_{n+1} = \xi_{n+2} = \ldots = \xi_N = 0$ obtemos que $m_{x,\mathcal{U}}(x) = 0$ implicando que $m_{x,J}(\lambda)$ divide $m_{x,\mathcal{U}}(\lambda)$. Mas $m_{x,\mathcal{U}}(\lambda)$ e $m_{x,J}(\lambda)$ são polinômios mônicos em $F[\lambda]$ de mesmo grau. Do Lema de Gauss, $m_{x,J}(\lambda) = m_{x,\mathcal{U}}(\lambda)$. Concluímos que o traço genérico de todo elemento a em J é o mesmo traço genérico de a em $\mathcal{U}$.*

Afim de concluir a seção, considere J uma álgebra de Jordan. Definiremos as potências $J^{\cdot 2^k}$ de J por $J^{\cdot 2^0} = J$, $J^{\cdot 2^k} = (J^{\cdot 2^{k-1}})^{\cdot 2}$. Dizemos que J é **solúvel** se existir algum número natural N tal que $J^{\cdot 2^N} = 0$. Claramente qualquer subálgebra e imagem homomórfica de uma álgebra solúvel é solúvel. Além disso, dizemos que J é **nilpotente** se existir algum inteiro positivo N tal que qualquer produto (em qualquer associação) de N elementos da álgebra J é 0. Evidentemente qualquer álgebra de Jordan nilpotente é solúvel. Além disso, dizemos que J é uma **álgebra nil** se todo elemento de J é nilpotente. Essas definições servem para entender o resultado seguinte denominado como o Teorema de Albert.

Teorema 1.7.23. *Seja J uma álgebra de Jordan de dimensão finita. Então:*

(1) Se J é solúvel, então é nilpotente.

(2) Se J é nil, então é solúvel.

(3) Se J é nil, cujo nil-índice é N, então J é nilpotente e seu índice de nilpotência é menor do que 2^N.

Demonstração. Ver [50, Seção V.3, pág. 195]. □

1.8 Álgebra com Traço

Suponha que A seja uma álgebra (não necessariamente associativa) com unidade sobre o corpo K e $\mathcal{Z}(A)$ seu centro.

Definição 1.8.1. *Uma transformação K-linear $\tau\colon A \to A$ tal que*

(i) $\tau(\tau(a)b) = \tau(a)\tau(b)$;

(ii) $\tau([a,b]) = [\tau(a), b] = \tau((a,b,c)) = 0$; *e*

(iii) $(\tau(a), b, c) = (a, \tau(b), c) = (a, b, \tau(c)) = 0$,

*para quaisquer a, b, $c \in A$, será chamada de **traço sobre a álgebra** A. O par (A,τ) será denominado **álgebra com traço**.*

Segue da definição da aplicação traço que $\tau(A)$ é uma subálgebra de $\mathcal{Z}(A)$. Um ideal (resp. subálgebra) em uma álgebra com traço é um **ideal com traço** (resp. **subálgebra com traço**) se é um ideal (resp. subálgebra) τ-invariante. Considerando (A,τ) uma álgebra com traço chamaremos de **álgebra dos traços** a imagem de A por τ, denotado por $\tau(A)$. A seguir listaremos alguns exemplos de álgebras com traço que usaremos nessa tese.

Exemplo 1.8.2. *Seja $A = M_n(K)$ a álgebra das matrizes de ordem n e tome "tr" a função traço usual de matrizes, ou seja, $tr(a)$ é a soma todos os elementos da diagonal de uma matriz a. É fácil verificar que (A, tr) é uma álgebra com traço.*

Exemplo 1.8.3. *Seja $A = M_n(K)^{(+)}$ a álgebra de Jordan munida do produto de Jordan, então (A, tr) é uma álgebra com traço, onde tr é o traço usual de matrizes. Em particular, se $B = H_n(M_n(K), *)$, então (B, tr) também é uma álgebra com traço.*

Exemplo 1.8.4. *Mais geralmente, sejam A uma álgebra central com traço τ_A e B uma subálgebra de A, então (B, τ_B) é uma álgebra com traço, onde $\tau_B =^{\tau_A}|_B$.*

Exemplo 1.8.5. *Seja $A = B_n(K)$ a álgebra de Jordan de uma forma bilinear simétrica e não degenerada e defina $tr(\alpha + v_\alpha) = 2\alpha$, então (A, tr) é uma álgebra com traço.*

Definição 1.8.6. *Sejam (A, τ) e (B, θ) álgebras com traço, onde A e B são álgebras com unidades. Uma aplicação*

$$\varphi\colon A \to B$$

será chamada um ***homomorfismo entre álgebras com traço****, se φ é um homomorfismo unitário entre as álgebras A e B, e $\varphi(\tau(a)) = \theta(\varphi(a))$, para todo $a \in A$.*

As álgebras com traço formam uma categoria onde os objetos são álgebras com traços e morfismos são homomorfismos entre álgebras com traço. Então os teoremas usuais de homomorfismos são válidos.

Vale salientar que a existência de uma aplicação traço não nula em uma álgebra A, de modo geral, pode não ser trivial. Neste caso, A e o comutador $[A, A]$ não podem coincidir, pois o traço é identicamente zero no segundo e não em A. Seja A uma álgebra (de matrizes ou Jordan semissimples), temos a existência da decomposição,

$$A = \mathcal{Z}(A) \oplus W, \tag{1.10}$$

de A como soma direta do centro de A com o subespaço W gerado pelos comutadores e associadores, note que para o caso da álgebra de matrizes está decomposição é trivial e para o caso de Jordan podemos destacar [50, Teorema 3, pág. 314]. Adicionando a hipótese da existência de um traço "tr" em A e a álgebra ser central, temos que a Igualdade (1.10) é também uma decomposição de G-módulos, com G sendo grupo de automorfismos de A. Assim um traço por definição é identicamente zero em W e como todo $a \in A$ pode ser escrito da forma $a = z + w$ teremos $tr(a) = ztr(1)$, ou seja, qualquer traço é múltiplo escalar da projeção no centro. Como $g \cdot a = z + g \cdot w$ temos $tr(g \cdot a) = tr(a)$ e portanto o traço também é um invariante pelo grupo G. Em [18], Belov provou que uma PI-álgebra associativa não pode coincidir com o seu comutador. Consequentemente, se $char K$ é zero ou não dividir $tr(1)$ temos que o traço é não trivial e portanto $A = K \oplus W$.

Seja $\mathcal{V}$ a variedade de álgebras com unidade e tome $K\{X\}$ a álgebra livre na variedade $\mathcal{V}$ livremente gerada pelo conjunto enumerável X. Pode-se construir a álgebra livre com traço sobre o conjunto X, denotada por $KTR\{X\}$, em $\mathcal{V}$ da seguinte forma. Denotamos, novamente, por $V[X]$ o conjunto de todos os monômios não associativos em $K\{X\}$ (ver Seção 1.3) Então podemos definir um símbolo formal $Tr(v)$ para todo v elemento em $V[X]$. Assim, $K\{X, Tr(V[X])\}$ denotará a álgebra livre livremente gerada pelo conjunto X junto com os símbolos $Tr(v)$, para todo $v \in V[X]$. Note que a existência da álgebra relativamente livre com traço, denotado por $KTR\{X\}$, é garantida pelo Teorema 1.4.17 tomando o ideal I gerado por

(i) $Tr(\alpha a) - \alpha Tr(a)$, para todo $\alpha \in K$;

(ii) $Tr(a + b) - Tr(a) - Tr(b)$;

(iii) $Tr(aTr(b)) - Tr(a)Tr(b)$;

(iv) $(Tr(a), b, c), \quad (a, Tr(b), c), \quad (a, b, Tr(c))$;

(v) $Tr([a, b]), \quad [Tr(a), b], \quad Tr((a, b, c))$,

para todo a, b e $c \in V[X]$. O símbolo formal Tr será chamado de **traço formal sobre** $K\{X\}$.

Sejam $\mathcal{V}_{Tr}$ a variedade das álgebras unitárias com traço e $(A, \tau) \in \mathcal{V}_{Tr}$. Pela definição da álgebra livre $K\{X\}$, uma aplicação $\mu\colon X \to A$ dada por $\mu(x_i) = a_i$ pode ser estendida para um homomorfismo $\varphi\colon K\{X\} \to A$. Segue que

$$\varphi(Tr(v(x_1, \ldots, x_n))) = tr(v(\mu(x_1), \ldots, \mu(x_n)),$$

para toda palavra $v(x_1, \ldots, x_n)$ em $V[X]$. Considerando a linearidade da aplicação Tr, temos que $KTR\{X\}$ é a **álgebra livre com traço na variedade** $\mathcal{V}_{Tr}$ livremente gerada pelo conjunto enumerável X.

Em uma expressão $f(x_1, \ldots, \hat{x}_i, \ldots, x_n)$, o "chapéu" sobre a variável (ou expressão) significa a possível omissão dessa variável (ou expressão) no lugar indicado em f. A subálgebra $G\{X\}$ em $KTR\{X\}$ gerada pelo conjunto

$$\{g(x_1, \ldots, x_n), Tr(g(x_1, \ldots, x_n)) \mid g(x_1, \ldots, x_n) \in K\{X\}\}$$

é chamada **álgebra de polinômios generalizados** (da variedade $\mathcal{V}$) e seus elementos serão chamados de **polinômios com traço**. Claramente, $G\{X\}$ é gerado como espaço vetorial pelos monômios generalizados da forma

$$\widehat{a}_0 tr(a_1) \cdots tr(a_s), \tag{1.11}$$

onde os a_i's são palavras em $V[X]$ e $a_1, \ldots, a_t$ são não vazias. Note que a representação de elementos da forma (1.11) não é única, mas é fácil contornar esse problema, basta tomar como representante de uma classe de elementos congruentes da forma (1.11) o elemento tal que a palavra $a_0 a_1 \cdots a_t$ é máxima no sentido de uma ordem dada.

Definição 1.8.7. *Seja (A, τ) uma álgebra com traço em $\mathcal{V}$. Dizemos que um polinômio com traço $f(x_1, \ldots, x_n) \in G\{X\}$ é uma* ***identidade com traço*** *para (A, τ), se substituindo Tr por τ, obteremos $f(a_1, \ldots, a_n) = 0$ para qualquer $a_1, \ldots, a_n \in A$.*

Definição 1.8.8. *Um ideal I da álgebra $G\{X\}$ é denominado* ***T_{Tr}-ideal*** *(ou T-ideal com traço) se, para qualquer polinômio com traço $f(x_1, \ldots, x_n)$ em I e quaisquer polinômios $g_1, \ldots, g_n$ em $G\{X\}$, o polinômio com traço $f(g_1, \ldots, g_n) \in I$.*

Observe que para qualquer álgebra com traço (A, τ), o ideal de todas as suas identidades com traço é um T_{Tr}-ideal. Diremos que uma identidade com traço $f \equiv 0$

segue das identidades com traço $g_i \equiv 0, i \in \Lambda$, se f pertence ao menor T-ideal com traço contendo todos os $g_i \equiv 0$, $i \in \Lambda$.

Considere a álgebra das matrizes de ordem n com o traço usual denotada por $(M_n(K), tr)$. O polinômio característico de uma matriz A de $M_n(K)$ é dado por:

$$\chi_A(\lambda) = det(A - \lambda I) = (-1)^n(\lambda^n + \sum_{i=1}^{n} c_i \lambda^{n-i}),$$

onde $c_1 = -tr(A)$ e $c_n = (-1)^n \det A$. Afirmamos que os coeficientes do polinômio caraterístico de uma matriz A são obtidos recursivamente por

$$\begin{aligned} c_1 &= -trA \\ c_2 &= -2^{-1}(c_1 trA + trA^2) \\ c_3 &= -3^{-1}(c_2 trA + c_1 trA^2 + trA^3) \\ &\vdots \\ c_n &= -n^{-1}(c_{n-1} trA + c_{n-2} trA^2 + \cdots + c_1 trA^{n-1} + trA^n). \end{aligned}$$

Introduzindo a notação $t_k = tr(A^k)$ temos que:

$$\begin{aligned} t_1 + c_1 &= 0 \\ t_k + c_1 t_{k-1} + \ldots + c_{k-1} t_1 + k c_k &= 0, k = 2, 3, \ldots, n. \end{aligned}$$

Essas equações são chamadas de **identidades de Newton** (ou Fórmulas de Newton) e assim o resultado segue. Do Teorema de Cayley–Hamilton temos que $\chi_A(A) = 0$ para todo $A \in M_n(K)$. Além disso, da minimalidade do grau do polinômio mínimo generalizado dado em (1.9) podemos chamar $f_n(x) = \chi_x(x) = m_{x,P}(x)$ de **o polinômio de Cayley–Hamilton de grau** n, onde x é uma variável.

Exemplo 1.8.9. *Se $A = M_n(K)$ é a álgebra das matrizes de ordem n sobre K, então $m_{x,P}(\lambda) = f_n(x)$ é a identidade de Cayley–Hamilton de grau n e Trd coincide com o traço usual de matrizes. Além disso, a identidade de Cayley–Hamilton é uma identidade com traço para a álgebra (A, tr). Sobre um corpo de característica zero, toda identidade com traço para (A, tr) segue da identidade de Cayley–Hamilton de grau n. Este último resultado foi obtido de forma independente por Procesi e por Razmyslov, ver [71, Coralário 4.4-(c)], ou [74].*

Observação 1.8.10. *Mais geralmente, se A é uma álgebra associativa nas potências de dimensão finita e de grau d, dizemos que o polinômio mínimo generalizado $m_{x,P}(\lambda)$ é a identidade de Cayley–Hamilton de grau $d = \deg(m_{x,P})$.*

Exemplo 1.8.11. *Seja $A = B_n(K)$ com traço dado por $tr(\alpha + v_\alpha) = 2\alpha$, onde $\alpha \in K$ e v_α um vetor no espaço vetorial V de dimensão n. O polinômio de Cayley-Hamilton de* *grau 2 e o polinômio*

$$L_{n+1}(x_1, \dots, x_n, x_{n+1}, y_1, \dots, y_n) = \sum (-1)^\sigma (x_{\sigma(n+1)} - (1/2)Tr(x_{\sigma(n+1)})) \prod_{k=1}^{n+1} H(x_{\sigma(k)}, y_k)$$

são identidades com traço para (A, tr). *Aqui* $H(x, y) = Tr(xy) - (1/2)Tr(x)Tr(y)$ *e* $\sigma \in S_{n+1}$. *Além disso, sobre um corpo infinito de característica diferente de dois, o resultado principal de Vasilovskii em [94] prova que o* T_{Tr}*-ideal das identidade com traço de* A *é gerado pelo polinômio de Cayley–Hamilton de grau* 2 *e por* L_{n+1}.

1.9 Aplicações Equivariantes e Invariantes

Definição 1.9.1. *Sejam* G *um grupo e* X *um conjunto não vazio. Definimos uma* ***ação de*** G ***em*** X *como sendo um aplicação*

$$\begin{aligned} \rho\colon G \times X &\rightarrow X \\ (g, x) &\longmapsto \rho(g, x) = g \cdot x. \end{aligned}$$

que satisfaz:

$$\epsilon \cdot x = x \qquad e \qquad (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x), \tag{1.12}$$

para quaisquer $g_1, g_2 \in G$ *e* $x \in X$.

Exemplo 1.9.2.

1. *A ação de* G *por multiplicação a esquerda ou por conjugação sobre si próprio.*
2. *Seja* M *um* G*-módulo, então* $\varphi\colon G \times M \rightarrow M$ *dado por* $\varphi(g, m) = g \cdot m$ *é uma ação de* G *em* M.

Definição 1.9.3. *Sejam* $\rho\colon G \times X \rightarrow X$ *uma ação de* G *em* X *e* $x \in X$. *Definimos a órbita de* x *por* ρ *e o estabilizador (ou subgrupo de isotropia) de* x *em relação a* ρ, *como sendo os conjuntos*

$$\mathcal{O}_\rho(x) = \{g \cdot x \mid g \in G\} \qquad e \qquad Stab_\rho(x) = \{g \in G \mid g \cdot x = x\},$$

respectivamente.

Observação 1.9.4. *Seja* $\rho\colon G \times X \rightarrow X$ *uma ação de* G *em* X.

1. *Dizemos que* ρ *é uma ação* ***transitiva*** *se determina uma única órbita em* X, *ou seja, se existe* $x \in X$ *tal que* $\mathcal{O}_\rho(x) = X$.
2. *Todo* $x \in X$ *tal que* $G = Stab_\rho(x)$ *é chamado* ***ponto fixo da ação*** *ou* ***ponto invariante***. *O conjunto de todos os pontos fixos em* X *será denotado usualmente por* X^G.

3. *Caso G seja finito, então $\mathcal{O}_\rho(x)$ é finito e $|\mathcal{O}_\rho(x)| = [G\colon Stab_\rho(x)]$, ou seja, $|\mathcal{O}_\rho(x)|$ divide $|G|$ para todo $x \in X$.*

4. *Caso X seja finito e $\mathcal{O}_1 = \mathcal{O}(x_1), \ldots, \mathcal{O}_n = \mathcal{O}(x_n)$ sejam órbitas distintas sob a ação de G tais que $\mathcal{O}_i \cap \mathcal{O}_j = \varnothing$, sempre que $i \neq j$ e $|X| = |\mathcal{O}_1| + \cdots + |\mathcal{O}_n|$, dizemos que $x_1, \ldots, x_n$ é um* ***sistema completo de representantes das órbitas de*** *X. Caso $\mathcal{O}_1, \ldots, \mathcal{O}_r$ sejam as órbitas unitárias (isto é, de comprimento 1), temos que $|X^G| = r$ e*
$$|X| = |X^G| + \sum_{i=r+1}^{n} |\mathcal{O}_i|.$$

5. *Seja X uma G-variedade algébrica. Se $x \in X$, então $Stab_\rho(x)$ é um subgrupo fechado de G (ver [84, Teorema 4.16, pág. 120]).*

Para maiores detalhes sobre essas observações indicamos a leitura de [53, Seção 1.12].

Uma aplicação entre espaços vetoriais é chamada **aplicação polinomial** se suas coordenadas são dadas por polinômios.

Definição 1.9.5. *Dados um grupo G e dois G-módulos V, W, uma* ***aplicação equivariante*** *é uma aplicação polinomial $\psi\colon V \to W$ que é compatível com a G-estrutura, ou seja, $\psi(g \cdot v) = g \cdot \psi(v)$, para todo $g \in G, v \in V$. Denotemos o conjunto das aplicações equivariantes por $hom_G(V, W)$.*

Observe primeiramente que $hom_G(V, W)$ é um subanel do anel $P_{V,W}$ das aplicações polinomiais de V em W formado por aqueles elementos fixados a esquerda pela ação do grupo G sobre $P_{V,W}$ da seguinte maneira:
$$g \in G, \psi \in P_{V,W}, \text{ então } (g \cdot \psi)(u) = g \cdot (\psi(g^{-1} \cdot u)).$$
Note que para φ sendo elemento fixado a esquerda pelo grupo G, tem-se:
$$\begin{aligned} \varphi(g \cdot v) &= (g \cdot \varphi)(g \cdot v) \\ &= (g \cdot \varphi)((g^{-1}g) \cdot v) \\ &= (g \cdot \varphi)(v). \end{aligned}$$
a inclusão oposta é imediata. Um caso particular é considerar as aplicações polinomiais $\psi\colon V \to W$ fixadas pela ação do grupo G, ou seja, $g \cdot \psi(v) = \psi(v)$. Denotemos tal conjunto por $inv_G(V, W)$ e as chamaremos de **aplicações invariantes**. Pode ser demonstrado que $inv_G(V, W) \subseteq hom_G(V, W)$.

Para completar essas observações preliminares, consideremos G um grupo agindo em uma álgebra A. Tome $V = A^n$ e $W = A$, e assim podemos considerar a ação diagonal de G sobre V dada por:
$$g \cdot (a_1, \ldots, a_n) = (g \cdot a_1, \ldots, g \cdot a_n).$$

Note que as aplicações projeção nas j-coordenadas, denotadas por

$$X_j\colon (a_1, \ldots, a_i) \to a_j,$$

são aplicações equivariantes chamadas **projeção equivariante na j-coordenada**.

1.10 Introdução aos Grupos Algébricos Lineares

Nesta seção, serão apresentadas as definições e algumas propriedades acerca de grupos algébricos lineares para o bom entendimento do nosso trabalho de tese. Assumiremos K é um corpo algebricamente fechado de característica zero. Para maiores detalhes sobre tal assunto indicamos a leitura de [22, 44, 68, 84].

Definição 1.10.1. *Definimos uma K-**representação** (ou **simplesmente representação) linear de** G **em um espaço vetorial** V como sendo um homomorfismo de grupos*

$$\begin{aligned} \varphi\colon G &\to GL(V) \\ g &\to \varphi(g) = \varphi_g. \end{aligned}$$

*Além disso, definimos o grau da representação linear φ como sendo a dimensão do espaço vetorial V. Dizemos que a representação linear φ é **fiel** se φ é injetivo.*

Exemplo 1.10.2. *A representação linear de um grupo G em um espaço vetorial V pode ser vista como a ação de grupo $G \times V \to V$ dada por $\varphi(g, v) = \varphi_g(v)$, para todo $g \in G$ e $v \in V$.*

Caso $\dim V = n$, com $n \in \mathbb{N}$, os grupos $GL(V)$ e $GL_n(K)$ são isomorfos. Neste caso, uma representação linear de G em V pode ser vista como um homomorfismo φ de G em $GL_n(K)$. Em particular, quando $n = 1$, podemos considerá-lo como um homomorfismo $\varphi\colon G \to K^\times$, onde $K^\times = K\backslash\{0\}$ é o grupo multiplicativo do corpo K. Nesta definição, podemos considerar que V é um G-módulo e consequentemente dizemos que φ é uma **representação irredutível** (completamente redutível) se V é um G-módulo irredutível (completamente redutível).

Exemplo 1.10.3. *Toda representação de grau 1 é irredutível. Toda representação irredutível é completamente redutível.*

Exemplo 1.10.4. *Sejam n um número natural maior que 2, C_n o grupo cíclico finito de ordem n e x um gerador de C_n. Podemos considerar a representação linear*

$$\begin{aligned} \varphi\colon C_n &\to GL_2(\mathbb{R}) \\ x^k &\to \varphi(x^k) = R_n^k, \end{aligned}$$

onde $R_n = \begin{pmatrix} cos\theta & sen\theta \\ -sen\theta & cos\theta \end{pmatrix}$, *com* $\theta = \dfrac{2\pi}{n}$. *Observamos que* φ *é uma representação irredutível. Caso existisse um subespaço* W *próprio não nulo teríamos que* $\varphi_g(Y) = \lambda_g Y$, *com* $W = \langle Y \rangle$ *e* $\lambda_g \in \mathbb{R}$ *para todo* $g \in C_n$. *Em particular,* R_n *teria autovalor real, o que é absurdo.*

Teorema 1.10.5. *Sejam* G *um grupo abeliano e* K *um corpo algebricamente fechado. Então toda* K*-representação de* G *irredutível de grau finito tem grau 1.*

Demonstração. Ver [80, Resultado 8.1.6, pág. 219] □

Teorema 1.10.6 (**Teorema de Maschke**). *Seja* G *um grupo finito de ordem* $|G|$. *Se* $char K$ *não divide* $|G|$ *então todo* G*-módulo* V *de dimensão finita é completamente redutível.*

Demonstração. Ver [54, Seção 5.2, pág 253] □

Segue do Teorema de Maschke que se M é um G-módulo de dimensão finita, então existem $N_1, N_2, \ldots, N_m$ submódulos simples de M tais que

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_m$$

e tal decomposição é única a menos de isomorfismo e ordenação (ver Teorema 1.1.33). Além disso, é possível demonstrar que a quantidade de representações irredutíveis de G sobre um corpo K, a menos de equivalência, é finito e este número é menor ou igual ao número de classes de conjugação de G, para maiores detalhes veja [54, Seção 5.3, página 261].

A demonstração do resultado principal do Capítulo 4, faz uso dos G-módulos completamente redutíveis; caso G seja finito o resultado segue do Teorema de Maschke, porém para o caso em que G é infinito este resultado não é tão obvio. Nosso objetivo no decorrer desta seção, é conhecer o conceito de grupos algébricos semissimples. Esta é uma teoria importante para o entendimento de G-módulos completamente redutíveis sobre um corpo de característica zero. Com esse objetivo é importante estabelecer as noções em detalhes.

Um **grupo algébrico** G é uma variedade que é também um grupo de modo que as aplicações multiplicação e inversa, que definem a estrutura de grupo, são morfismos de variedades. Se G é uma variedade afim, ou seja, um fechado de $\mathbb{A}^k$, então G é chamado **grupo algébrico linear**.

O conjunto $M_n(K)$ de todas as matrizes de ordem n sobre o corpo K pode ser identificado como a variedade afim $\mathbb{A}^{n^2}$. Denotando por $GL_n(K) = GL_n$ o conjunto de todas as matrizes de ordem n invertíveis com entradas em K, podemos observar que GL_n munido com o produto usual de matrizes é um grupo chamado **grupo geral linear**. Note que GL_n é um subconjunto aberto (por Zariski) do espaço $M_n(K)$ que não se anula no polinômio determinante $\det x$. Além disso, é fato conhecido da teoria que os subgrupos algébricos de um grupo algébrico, são os seus subgrupos fechados. A seguir daremos alguns exemplos de grupos algébricos lineares.

Exemplo 1.10.7. *O produto direto de dois (ou mais) grupos algébricos (munido com a topologia do produto) é novamente um grupo algébrico.*

Exemplo 1.10.8. *O grupo especial linear $SL_n(K)$ é um subgrupo fechado de $GL_n(K)$ na topologia de Zariski, definido pelos zeros da função $\det x - 1$. Além disso, seja g^t a matriz transposta da matriz $g \in M_n(K)$. Então para todo $M \in M_n(K)$ podemos definir o grupo*

$$G_M = \{g \in GL_n(K) \mid gMg^t = M\}.$$

Este é um grupo algébrico linear, com a condição de que $gMg^t = M$ é um polinômio nas entradas de g. Quando M for a matriz

$$\begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix},$$

onde $n = 2k$, temos que G_M é o grupo simplético $Sp_{2t}(K)$. Caso $M = I_n$, G_M será o grupo ortogonal $O_n(K)$.

Um caso particularmente interessante desta situação diz respeito ao centro de um grupo. Seja G um grupo algébrico linear, por definição, o centro $Z(G)$ de G é o subgrupo dado por

$$Z(G) = \{g \in G \mid gh = hg, \text{ para todo } h \in G\}.$$

Em outras palavras, $Z(G) = \bigcap_{h \in G} \{g \in G \mid gh = hg\}$ é um grupo algébrico linear, já que o conjunto $\{g \in G \mid gh = hg\}$ satisfaz a condição de que $gh = hg$ é um polinômio nas entradas de g, para $h \in G$ fixado.

Exemplo 1.10.9. *Seja G um grupo algébrico linear e $H \subseteq G$ um subgrupo normal fechado, então G/H é um grupo algébrico linear, para maiores detalhes ver [84, Teorema 5.3, pág. 269]. Segue que o* ***grupo geral linear projetivo****, definido como sendo o quociente $PGL_n = PGL_n(K) = GL_n/Z(GL_n)$, pois $Z(GL_n) = K^\times \cdot Id$, é um grupo algébrico linear.*

Exemplo 1.10.10. *Dados uma álgebra A de dimensão finita (não necessariamente associativa) e V o espaço vetorial de dimensão n associado à álgebra A, então o conjunto $Aut_K A$ é um subgrupo de $GL(V) \simeq GL_n(K)$. Além disso, fixando a, b elementos de A podemos definir o conjunto $S(a,b) = \{\varphi \in GL_n(K) \mid \varphi(ab) = \varphi(a)\varphi(b)\}$ que é fechado em $GL_n(K)$ e assim $Aut_K A = \bigcap \{S(a,b) \mid a, b \in A\}$ é fechado em $GL_n(K)$. Portanto, $Aut_K A$ é um grupo algébrico linear.*

Um importante resultado a respeito dos grupos algébricos lineares, porém de demonstração mais elaborada que os exemplos anteriores é a existência de uma representação como um grupo de matrizes, ou seja, se G é um grupo algébrico linear, então existem um inteiro positivo n e um isomorfismo de G sobre um subgrupo fechado de $GL_n(K)$. A demonstração de tal fato pode ser encontrada em [44, Seção 8.6, pág. 63].

Por definição, um **morfismo de grupos algébricos** é um homomorfismo de grupos $\varphi\colon G \to G'$ que é também um morfismo de variedades. É fácil verificar que $Ker\varphi$ e $Im\varphi$ são subgrupos fechado de G e G', respectivamente. Quando o grupo $G' = GL_n(K)$, dizemos que φ é uma representação racional. A seguir daremos a definição mais precisa de representação racional.

Definição 1.10.11. *Seja V um espaço vetorial.*

*(a) Se V for de dimensão finita, então uma representação de um grupo G em V, denotada por $\rho\colon G \to GL(V)$, é uma **representação G-racional** se ela é um homomorfismo de variedades. Neste caso, dizemos que V é um **G-módulo racional**.*

(b) Se dimensão de V for infinita, dizemos que V é G-módulo racional se ele for união de G-módulos racionais de dimensão finita, ou seja, todo $v \in V$ está contido em um espaço G-invariante de dimensão finita N e a restrição da ação de G sobre N é uma representação racional de G em N.

Exemplo 1.10.12. *O produto tensorial entre G-módulos racionais também é racional, munido com a respectiva ação diagonal pelo grupo G.*

Sejam A uma álgebra finitamente gerada e G um grupo algébrico linear tal que G age como um grupo de automorfismos da álgebra. Dizer que "G" age "racionalmente" sobre A implica que cada elemento de A está em um subespaço G-invariante de dimensão finita que ofereça uma representação racional de G.

Exemplo 1.10.13. *Sejam A uma álgebra de dimensão finita e $G = Aut_K(A)$ então A é um G-módulo racional, basta considerar a representação inclusão $\iota\colon Aut_K(A) \hookrightarrow GL_n(K)$, onde $n = \dim_K A$.*

Proposição 1.10.14. *[41, Lema 5.6] Seja R uma álgebra que é um G-módulo racional tal que G age sobre R como um grupo de automorfismos. Se S é uma R^G-álgebra comutativa qualquer, então G age na S-álgebra $R \otimes_{R^G} S$ como grupo de S-automorfismos e a representação é racional.*

Demonstração. Podemos definir a ação de G sobre $R \otimes_{R^G} S$ por $g \cdot (r \otimes s) = (g \cdot r) \otimes s$, com $r \in R$ e $s \in S$. A primeira afirmação é obvia. Para ver que a representação é racional, observamos que dado $h = \sum r_i \otimes s_i$ um elemento qualquer em $R \otimes_{R^G} S$, podemos definir M

como sendo o G-submódulo de R gerado por todos os r_i's. Consideramos $\sum M \otimes_K (Ks_i)$ o G-submódulo de $R \otimes_K S$ de dimensão finita que é um G-submódulo de $R \otimes_{R^G} S$ contendo h. □

Definição 1.10.15. *Seja G um grupo algébrico linear. Dizemos que G é **linearmente redutível**, se todo G-módulo racional é completamente redutível.*

Seja G um grupo algébrico linear. Um elemento g em G é dito ser **unipotente** se todos os seus autovalores são 1. Dizemos que G é **unipotente** se todos os seus elementos são unipotentes. Além disso, G é **solúvel** (resp. **nilpotente**), se ele é solúvel (resp. nilpotente) como grupo.

Definição 1.10.16. *Seja G um grupo algébrico. O **radical** $R(G)$ **de** G é o maior subgrupo normal solúvel conexo de G. Além disso, o **radical unipotente** $R_u(G)$ **de** G é o maior subgrupo normal unipotente conexo de G. Dizemos que G é semissimples (respectivamente redutível) se $R(G) = \{\epsilon\}$ (respectivamente $R_u(G) = \{\epsilon\}$).*

Lema 1.10.17. *[41, Corolário 5.35] Um grupo algébrico linear unipotente é solúvel.*

Observação 1.10.18. *Segue do lema anterior e da Definição 1.10.16 que um grupo semissimples é redutível.*

Observamos que Chevalley classificou, em [22], os grupos algébricos simples. Mais precisamente, se G é um grupo algébrico semissimples, então podemos associá-lo a um diagrama de Dynkin, obtendo assim uma classificação similar à dos grupos de Lie compactos, como grupos de Lie simples do tipo especial A_n, B_n, C_n, D_n, e os cinco grupos excepcionais E_6, E_7, E_8, F_4, G_2. Para maiores detalhes ver o comentário feito em [68, Seção 2.1.13, pág. 62]

Lema 1.10.19. *[84, Cap. 9, Teorema 5.4 e Corolário 5.6] Um grupo algébrico linear G é redutível se, e somente se, ele é linearmente redutível. Em particular, os grupos clássicos e excepcionais são linearmente redutível.*

Seja A uma álgebra associativa central simples munida de uma involução $(*)$. Pelos comentários feitos na Seção 1.7 temos que $Aut_K(A, \tau) = PSU_n(K)$ o grupo especial unitário projetivo. O próximo resultado classifica os grupos especiais unitários, a menos de isomorfismo.

Teorema 1.10.20. *Seja $A = M_n(K)$ a álgebra das matrizes de ordem n sobre o corpo K algebricamente fechado. Se G é o grupo especial unitário associado a involução $(*)$, então:*

1. *$G \simeq SO_n(K)$, se $* = t$;*
2. *$G \simeq Sp_n(K)$, se $* = s$;*

3. $G \simeq SL_n(K)$*, se* $(*)$ *é do segundo tipo.*

Demonstração. Ver [68, Proposição 2.15, pág. 86] □

Por fim, seja G um grupo linearmente redutível, então qualquer quociente G/H por um subgrupo algébrico normal de G é também linearmente redutível. De fato, dada uma representação V de G/H, obtém-se uma representação induzida por G (para o mesmo espaço vetorial associado). Então qualquer decomposição de V como uma representação de G é também um decomposição como representação de G/H. Como subespaços invariantes pela ação de G de V são ao mesmo tempo subespaços G/H-invariantes de V então as noções de subrepresentação irredutível coincidem, assim devemos obter uma decomposição de V como uma representação de G/H.

Deste comentário e do Lema 1.10.19 temos o seguinte resultado.

Teorema 1.10.21. *Consideramos* K *um corpo algebricamente fechado de característica zero e* A *uma álgebra de Jordan (ou associativa) central simples de dimensão finita. O grupo de automorfismos* $Aut_K(A)$ *é um grupo redutível.*

2 Propriedade de Primalidade para Polinômios Centrais

Neste capítulo consideraremos K sendo um corpo infinito de característica diferente de 2 e apresentaremos os resultados descritos em [33]. Primeiramente iremos considerar uma propriedade análoga à estabelecida por Regev em [78] para as álgebras $M_n(K)$ das matrizes, mas para outros tipo de álgebras e determinaremos em quais graduações elementares por um grupo em n-uplas distintas sobre álgebras das matrizes tal propriedade é satisfeita. Em seguida, provaremos que as álgebras $M_n(E)$ e $M_{a,b}(E)$ satisfazem a propriedade de primalidade para polinômios centrais. E por fim, concluiremos que, sobre um corpo de característica zero, toda álgebra verbalmente prima satisfaz tal propriedade.

Ressaltamos que o último resultado mencionado acima já foi obtido em [31] e completado em [83]. Aqui foi dada uma demonstração alternativa e que generaliza ambas as situações. Os resultados foram obtidos em colaboração com Diogo Diniz, UFCG, e foram aceitos para publicação na revista **Journal of Pure and Applied Algebra**.

Em todo capítulo, a menos de menção contrária, todas as álgebras e espaços vetoriais serão sobre K e todas as álgebras serão associativas e com unidade. Além disso, por simplicidade de notação, iremos mencionar polinômios centrais G-graduados para identificar os polinômios centrais G-graduados próprios.

2.1 Definições e Resultados Preliminares

Seja G um grupo abeliano com elemento neutro ϵ, denotaremos por $A = \oplus_{g\in G}A_g$ uma álgebra G-graduada associativa com unidade.

Definição 2.1.1. *A álgebra A satisfaz a **propriedade de primalidade para polinômios centrais G-graduados** se sempre que o produto de dois polinômios G-graduados em conjuntos disjuntos de variáveis for polinômio central graduado para A implicar que ambos os polinômios também são centrais graduados para A.*

Vale lembrar que dado um subconjunto S de $K\langle X_G\rangle$ denotaremos por $\langle S\rangle^{T_G}$ o T_G-espaço gerado por S. Se $S = \{f\}$ usaremos, simplesmente, $\langle f\rangle^{T_G}$ para denotar o T_G-espaço gerado por f. Além disso, sabe-se que $\langle f\rangle^{T_G}$ é gerado, como espaço vetorial, pelo conjunto

$$\{f(p_1,\ldots,p_n) \mid p_i \in (K\langle X_G\rangle)_{g_i}\},$$

(ver Proposição 1.5.8). Logo se f é um polinômio central graduado para A, então todo elemento de $\langle f\rangle^{T_G}$ é uma identidade graduada ou um polinômio central graduado para a álgebra A. Para o caso em que $G = \{\epsilon\}$ temos, nas referências clássicas utilizadas para o estudo básico de PI-álgebras, o seguinte resultado.

Proposição 2.1.2. *Sejam $f(x_1, \ldots, x_r)$ um polinômio multihomogêneo de grau d_i em x_i e $h_i(x_1, \ldots, x_r, z_i)$ a componente multihomogênea de $f(x_1 + z_1, \ldots, x_r + z_r)$ de grau 1 em z_i. Então*

$$[f(x_1, \ldots, x_r), x_{r+1}] = \sum_i h_i(x_1, \ldots, x_r, [x_i, x_{r+1}]). \tag{2.1}$$

Demonstração. A igualdade segue do fato que a aplicação $a \mapsto [a, x_{r+1}]$ é uma derivação de $K\langle X\rangle$, para maiores detalhes ver [43, pg. 9]. □

Agora, estamos aptos para enunciar o nosso primeiro resultado.

Proposição 2.1.3. *Sejam A uma álgebra G-graduada com uma base $\mathcal{B}$ consistindo de elementos homogêneos, V um subespaço de A e $f(x_{1,g_1}, \ldots, x_{n,g_n})$ um polinômio em $K\langle X_G\rangle$. As afirmações a seguir são equivalentes:*

(i) *Se $(a_1, \ldots, a_n)$ é uma substituição admissível qualquer por elementos de A, então o elemento $f(a_1, \ldots, a_n)$ está em V;*

(ii) *Para todo polinômio $f'(x_{1,g_1}, \ldots, x_{m,g_m})$ em $\langle f\rangle^{T_G}$ e toda substituição f'-admissível $(a_1, \ldots, a_m)$ de elementos em A, o elemento $f'(a_1, \ldots, a_m)$ está em V.*

(iii) *Para todo polinômio multihomogêneo $f'(x_{1,g_1}, \ldots, x_{m,g_m})$ em $\langle f\rangle^{T_G}$ e toda substituição f'-admissível $(b_1, \ldots, b_m)$ de elementos em $\mathcal{B}$, o elemento $f'(b_1, \ldots, b_m)$ está em V.*

Demonstração. Sabemos que o conjunto $S = \{f(p_1, \ldots, p_n) \mid p_i \in (K\langle X_G\rangle)_{g_i}\}$ gera $\langle f\rangle^{T_G}$ como um espaço vetorial. Suponha que a afirmação (i) seja válida, então tal afirmação é válida também para todos os elementos de S e portanto para todo f' em $\langle f\rangle^{T_G}$, o que conclui o item (ii). É claro que o item (ii) implica o item (iii), então falta demonstrar que o item (iii) implica (i). Assuma que o item (iii) seja válido e considere uma substituição admissível $(a_1, \ldots, a_n)$ por elementos de A. Como $\mathcal{B}$ é uma base para A, então podemos escrever $a_i = \sum_{j=1}^{n_i} \lambda_{ij} b_j$, $i = 1, \ldots, n$, onde os $b_j \in \mathcal{B}$ são elementos homogêneos de grau g_j. Defina, para cada $i = 1, \ldots, n$, o polinômio

$$q_i(x_{s_i+1,g_1}, \ldots, x_{s_i+n_i,g_{n_i}}) = \sum_{j=1}^{n_i} \lambda_{ij} x_{s_i+j,g_j}$$

em $K\langle X_G\rangle$, e escreva $f(q_1, \ldots q_m) = f_1 + \cdots + f_l$ como soma de componentes multihomogêneas. Como o corpo base é infinito, temos que os polinômios $f_1, \ldots, f_l$ estão em $\langle f\rangle^{T_G}$.

Consideremos ν a substituição de elementos de $K\langle X_G\rangle$ por elementos de A tal que x_{s_i+j,g_j} é substituído por b_j. Observe que o resultado dessa substituição feita no polinômio q_j será $q_j(b_1,\dots,b_{n_i}) = a_i$ e portanto

$$f(a_1,\dots,a_n) = f_1|_\nu + \dots + f_l|_\nu.$$

Segue de *(iii)* que cada componente $f_1|_\nu, \dots, f_l|_\nu$ está em V, e portanto $f(a_1,\dots,a_n)$ também está em V. Assim concluímos o resultado. □

Como consequência direta da proposição anterior, temos:

Corolário 2.1.4. *Sejam A uma álgebra graduada por um grupo G, V um subespaço de A e $f(x_{1,g_1},\dots,x_{m,g_m})$ um polinômio tal que para toda substituição f-admissível $(a_1,\dots,a_m)$ de elementos em A, o elemento $f(a_1,\dots,a_m)$ está em V. Então, para todo elemento b em A_ϵ e toda substituição f-admissível $(a_1,\dots,a_m)$, o comutador $[f(a_1,\dots,a_m),b]$ também está em V.*

Demonstração. Utilizando uma "pequena" adaptação da Proposição 2.1.2 teremos que

$$[f(x_{1,g_1},\dots,x_{m,g_m}),x_{m+1,\epsilon}] = \sum_i h_i(x_{1,g_1},\dots,x_{m,g_m},[x_{i,g_i},x_{m+1,\epsilon}]). \tag{2.2}$$

Observe que a variável $x_{m+1,\epsilon}$ é homogênea de grau ϵ, e consequentemente o comutador $[x_{i,g_i},x_{m+1,\epsilon}]$ tem grau g_i. Além disso, sabe-se que os polinômios

$$h_i(x_{1,g_1},\dots,x_{m,g_m},[x_{i,g_i},x_{m+1,\epsilon}])$$

estão no T_G-espaço gerado por f. Da Proposição 2.1.3, temos que para toda substituição h_i-admissível $(a_1,\dots,a_m,b)$ os elementos $h_i(a_1,\dots,a_m,[a_i,b])$ estão em V. E assim, o resultado segue diretamente da Igualdade (2.2). □

Para finalizar esta seção de preliminares, provaremos um resultado que será utilizado de forma recorrente nas demonstrações deste capítulo.

Proposição 2.1.5. *Sejam $f(x_{1,g_1},\dots,x_{r,g_r})$ e $g(x_{r+1,g_{r+1}},\dots,x_{s,g_s})$ polinômios em conjuntos disjuntos de variáveis em $K\langle X_G\rangle$. Se $f' \in \langle f\rangle^{T_G}$ e $g' \in \langle g\rangle^{T_G}$ então $f'\cdot g'$ está em $\langle f\cdot g\rangle^{T_G}$. Em particular, se $f\cdot g$ for um polinômio central graduado para uma álgebra G-graduada A, então $f'\cdot g'$ também o é.*

Demonstração. Da hipótese, temos que f' e g' são combinações lineares de polinômios da forma $f(p_1,\dots,p_r)$ e $g(q_1,\dots,q_s)$, respectivamente, onde $(p_1,\dots,p_r)$ e $(q_1,\dots,q_s)$ são substituições admissíveis por polinômios em $K\langle X_G\rangle$. Portanto, $f'\cdot g'$ é uma combinação linear de polinômios no conjunto

$$S = \{f(p_1,\dots,p_r)\cdot g(q_1,\dots,q_r) \mid p_1,\dots,p_r,q_1,\dots,q_s \in F\langle X\rangle\}.$$

Como f e g são polinômios em conjuntos disjuntos de variáveis e da caracterização de T_G-espaço temos que cada elemento de S estará em $\langle f \cdot g \rangle^{T_G}$. E portanto $f' \cdot g'$ está em $\langle f \cdot g \rangle^{T_G}$. A segunda parte é uma aplicação direta da primeira junto com a Proposição 2.1.3. □

2.2 Graduação Elementar sobre $M_n(K)$ e Propriedade de Primalidade

Nesta seção denotaremos por A a álgebra $M_n(K)$ e E_{ij} serão as matrizes elementares de A contendo 1 na (i, j)-ésima entrada e 0 nas demais. O objetivo principal desta seção é caracterizar as graduações elementares de A por n-uplas distintas que satisfazem a propriedade de primalidade para polinômios centrais graduados. Tal caracterização será demonstrada no fim desta seção, mas para chegarmos a este objetivo, precisaremos estabelecer uma sequência de resultados úteis.

Proposição 2.2.1. *Considere que A seja munida de uma graduação elementar e os polinômios $f(x_{1,g_1}, \ldots, x_{r,g_r})$ e $g(x_{r+1,g_{r+1}}, \ldots, x_{s,g_s})$ estejam em conjuntos disjuntos de variáveis. Se $f \cdot g$ é um polinômio central graduado para A, então existe uma matriz diagonal invertível P de modo que o resultado de toda substituição f-admissível (respectivamente g-admissível) é um múltiplo escalar da matriz P (respectivamente de P^{-1}).*

Demonstração. Segue por hipótese que existe pelo menos uma substituição admissível $A_1, \ldots, A_s$ tal que o elemento $f(A_1, \ldots, A_r) \cdot g(A_{r+1}, \ldots, A_s)$ seja uma matriz escalar não nula, implicando que $g(A_{r+1}, \ldots, A_s)$ é uma matriz invertível, a qual denotaremos por P^{-1}. Considerando $(B_1, \ldots, B_r)$ uma substituição f-admissível qualquer, temos que o produto $f(B_1, \ldots, B_r) \cdot g(A_{r+1}, \ldots, A_s)$ será uma matriz escalar. Portanto $f(B_1, \ldots, B_r)$ é um múltiplo escalar da matriz P para toda substituição f-admissível. De modo análogo, o resultado de toda substituição g-admissível é um múltiplo escalar de P^{-1}. Resta provar que P é uma matriz diagonal.

Do Corolário 2.1.4, temos que se M é uma matriz qualquer de grau ϵ e $(B_1, \ldots, B_r)$ é uma substituição f-admissível, então o comutador $[f(B_1, \ldots, B_r), M]$ será um múltiplo escalar da matriz P. Em particular, $[P, M] = \lambda_M P$ para algum escalar $\lambda_M \in K$. Como a graduação aqui considerada é elementar, podemos observar que as matrizes E_{kk} têm grau ϵ, para todo $k = 1, \ldots, n$. Consequentemente, para cada k, existe um escalar $\lambda_k \in K$ tal que

$$[P, E_{kk}] = \lambda_k P. \tag{2.3}$$

Escrevendo $P = \sum_{i,j} p_{ij}E_{ij}$ e considerando a igualdade (2.3) teremos

$$\sum_{i\neq k} p_{ik}E_{ik} - \sum_{j\neq k} p_{kj}E_{kj} = \lambda_k \left(\sum_{i,j} p_{ij}E_{ij}\right).$$

Se $\lambda_k = 0$ para todo k então $\sum_{i\neq k}(p_{ik}E_{ik} - p_{ki}E_{ki}) = 0$, implicando que $p_{ij} = 0$ para $i \neq j$, isto é, P é uma matriz diagonal. Suponha, agora, que exista algum k tal que $\lambda_k \neq 0$. Considerando a igualdade anterior, podemos observar que $\lambda_k p_{kk} = 0$ implicando que $p_{kk} = 0$ e os coeficientes que não estão na k-ésima linha ou coluna são nulos, isto é, $p_{ij} = 0$ quando $i \neq k$ e $j \neq k$. Além disso, $p_{ik} = \lambda_k p_{ik}$ e $-p_{kj} = \lambda_k p_{kj}$ para todo $i \neq k$ e $j \neq k$. Caso $p_{ik} \neq 0$ para algum $k \neq i$ teríamos $\lambda_k = 1$ e $p_{ki} = 0$ para todos $i \neq k$. Neste caso $P = \sum_{i\neq k} p_{ik}E_{ik}$ não seria uma matriz invertível, o que é uma contradição. Suponha agora que $p_{ki} \neq 0$ para algum $i \neq k$ então $\lambda_k = -1$ e assim $P = \sum_{i\neq k} p_{ki}E_{ki}$ também não seria invertível, providenciando novamente uma contradição. Em resumo, $P = 0$ se existir algum k tal que $\lambda_k \neq 0$, que é absurdo. Assim, o único caso considerado implicará que P é uma matriz diagonal, o que queríamos demonstrar. □

Definição 2.2.2. *Seja A a álgebra das matrizes $M_n(K)$ munida com uma graduação elementar. Denotemos por H o conjunto das permutações σ em S_n tais que o correspondente automorfismo Λ_σ, dado por $\Lambda_\sigma(E_{ij}) = E_{\sigma(i)\sigma(j)}$, é um automorfismo graduado de A.*

É fácil verificar que o conjunto H, definido acima, é um subgrupo de S_n e a aplicação $\sigma \mapsto \Lambda_\sigma$ é um homomorfismo de grupos. Deixaremos essa verificação para o leitor. Nos próximos resultados serão deduzidas algumas relações que envolvem o subgrupo H.

Proposição 2.2.3. *Se f é um polinômio em $K\langle X_G\rangle$ que não é identidade graduada para A e o resultado de toda substituição f-admissível é um múltiplo escalar de uma matriz M, então para todo $\sigma \in H$ existe um escalar não nulo $\lambda(\sigma)$ tal que*

$$\Lambda_\sigma(M) = \lambda(\sigma)^{-1}M.$$

Além disso, a aplicação $\lambda\colon H \to K^\times$ é um homomorfismo de grupos.

Demonstração. Da hipótese, existe uma substituição f-admissível de elementos em A tal que $f(A_1, \ldots, A_m) = \lambda M$ para algum escalar $\lambda \neq 0$. Como os automorfismos Λ_σ são graduados, então

$$\Lambda_\sigma(\lambda M) = \Lambda_\sigma(f(A_1, \ldots, A_m)) = f(\Lambda_\sigma(A_1), \ldots, \Lambda_\sigma(A_m)) = \lambda' M,$$

para algum escalar λ' que depende do elemento σ em H. Afirmamos que para cada $\sigma \in H$ existe um único escalar $\lambda(\sigma)$ tal que $\Lambda_\sigma(M) = \lambda(\sigma)^{-1}M$. De fato, suponha que o escalar

$\lambda'\lambda^{-1}$ seja nulo, então $\lambda' = 0$, e como Λ_σ é um automorfismo da álgebra A, podemos concluir que $f(A_1, \ldots, A_m) = 0$, o que é uma contradição. Logo, podemos definir $\lambda(\sigma) = \lambda\lambda'^{-1}$; a boa definição desse escalar segue do fato da matriz M ser não nula, assim concluímos a primeira parte da Proposição.

Para a segunda parte do resultado, basta observar que da Definição de Λ_σ e considerando $M = \sum\limits_{i,j} m_{ij}E_{ij}$ temos que

$$\begin{aligned}\lambda(\sigma\tau)^{-1}M = \Lambda_{\sigma\tau}(M) = \Lambda_{\sigma\tau}(\sum_{i,j} m_{ij}E_{ij}) &= \sum_{i,j} m_{ij}(E_{\sigma\tau(i)\sigma\tau(j)}) \\ &= \Lambda_\sigma\Lambda_\tau(M) = \lambda(\sigma)^{-1}\lambda(\tau)^{-1}M.\end{aligned}$$

Agora o resultado segue, novamente, do fato de M ser não nulo. □

Seja λ o homomorfismo dado na proposição anterior. Neste próximo lema, descreveremos as matrizes diagonais P que satisfazem a igualdade $\Lambda_\sigma(P) = \lambda(\sigma)^{-1}P$ em termos do homomorfismo λ e da ação canônica de H sobre o conjunto $\{1, 2, \ldots, n\}$.

Lema 2.2.4. *Seja $\lambda\colon H \to K^\times$ um homomorfismo de grupos e, para cada i, definimos $P(i) = \sum\limits_{\alpha\in \mathrm{H}} \lambda(\alpha)E_{\alpha(i)\alpha(i)}$. Então as seguintes afirmações são válidas:*

(i) Para todo $\sigma \in H$ temos $\Lambda_\sigma(P(i)) = \lambda(\sigma)^{-1}P(i)$;

(ii) As matrizes $P(i)$ e $P(j)$ têm entradas não nulas na mesma posição se, e somente se, i e j estão na mesma H-órbita;

(iii) Seja $i_1, \ldots, i_d$ um sistema completo de representantes das órbitas da ação canônica de H sobre $\{1, 2, \ldots, n\}$. A matriz diagonal P satisfaz

$$\Lambda_\sigma(P) = \lambda(\sigma)^{-1}P \tag{2.4}$$

para todo $\sigma \in H$ se, e somente se, P pode ser apresentada como uma combinação linear das matrizes $P(i_1)$, ..., $P(i_d)$.

Demonstração. Observe, inicialmente, que

$$\Lambda_\sigma(P(i)) = \sum_{\alpha\in H} \lambda(\alpha)E_{\sigma\alpha(i)\sigma\alpha(i)} = \lambda(\sigma)^{-1}\sum_{\alpha\in H} \lambda(\sigma\alpha)E_{\sigma\alpha(i)\sigma\alpha(i)} = \lambda(\sigma)^{-1}P(i),$$

o que prova o item (i).

Para a prova da afirmação (ii), suponha que $P(i)$ e $P(j)$ têm entradas não nulas na mesma posição. Isso implicará $\alpha(i) = \beta(j)$, para alguns α e β em H, isto é, $\beta^{-1}\alpha(i) = j$. Consequentemente i e j estão na mesma H-órbita. A afirmação recíproca é imediata.

Resta provar a afirmação (iii). Consideremos a matriz diagonal $P = \sum_i p_i E_{ii}$ que satisfaz a igualdade (2.4) e $\lambda_1, \ldots, \lambda_d$ escalares em K tais que a i_s-ésima entrada da matriz $\lambda_s P(i_s)$ seja p_{i_s}. Defina $P' = \sum_{s=1}^{d} \lambda_s P(i_s)$. Como P' é soma de matrizes diagonais, podemos escrevê-la na forma $P' = \sum_{i=1}^{n} p'_i E_{ii}$. Além disso, $i_1, \ldots, i_d$ é um sistema completo de representantes das órbitas da ação canônica de H. Segue da afirmação (ii) que os $P(i_s)$'s não possuem entradas não nulas na mesma posição e consequentemente $p_{i_s} = p'_{i_s}$ para todos $s = 1, \ldots, d$. Devemos provar que $P = P'$. Tomemos a k-ésima entrada da matriz P, então podemos considerar a matriz $p_k P(k)$. Da definição de sistema completo existe um s em $\{1, \ldots, d\}$ e um $\sigma \in H$ tal que $\sigma(s) = k$, e portanto $p_{\sigma(s)} = p'_{\sigma(s)}$ sempre que $p_s = p'_s$. Para a reciproca, basta observar que pela afirmação (i) a matriz P' também satisfaz a igualdade (2.4). Isto conclui a prova do lema. $\square$

Para algumas graduações elementares por n-uplas distintas de elementos de G é possível determinar uma matriz P nas condições do lema anterior e um polinômio f em $K\langle X_G\rangle$ que não é uma identidade graduada para A tal que o resultado por toda substituição admissível é um múltiplo escalar de P. Este último resultado será mostrado na próxima proposição, mas antes disso deduziremos as seguintes afirmações.

Lema 2.2.5. *Seja $x_{1,g_1} \cdots x_{n,g_n}$ um monômio multilinear de grau ϵ tal que a n-upla $(g_1, g_1g_2, \ldots, g_1 \cdots g_n)$ consiste de elementos de G distintos. Sejam $(E_{i_1j_1}, \ldots, E_{i_nj_n})$ e $(E_{k_1l_1}, \ldots, E_{k_nl_n})$ duas substituições admissíveis tais que o resultado de cada substituição é não nulo. Então existe $\sigma \in \mathrm{H}$ tal que*

$$(E_{k_1l_1}, \ldots, E_{k_nl_n}) = (E_{\sigma(i_1)\sigma(j_1)}, \ldots, E_{\sigma(i_n)\sigma(j_n)}).$$

Demonstração. O elemento $E_{i_1j_1} \cdots E_{i_nj_n}$ é não nulo e homogêneo de grau ϵ, assim devemos ter $j_1 = i_2, \ldots, j_{n-1} = i_n, j_n = i_1$, isto é, $E_{i_1j_1} \cdots E_{i_nj_n} = E_{i_1i_1}$. Além disso, a n-upla $(g_1, g_1g_2, \ldots, g_1 \cdots g_n)$ é composta de elementos distintos de G, implicando que $(i_1, \ldots, i_n)$ é uma permutação de $\{1, \ldots, n\}$. De fato, assumindo que $i_s = i_r$ para $s < r$, obteríamos $E_{i_1i_s} = E_{i_1i_r}$, com $\deg E_{i_1i_s} = g_2 \cdots g_s$ e $\deg E_{i_1i_r} = g_2 \cdots g_s g_{s+1} \ldots g_r$ distintos, o que é um absurdo. Analogamente $(k_1, \ldots, k_n)$ é também uma permutação. Consideremos σ como sendo uma permutação em S_n tal que $\sigma(i_s) = k_s$, para todo $s = 1, \ldots, n$. As substituições consideradas são todas admissíveis, e consequentemente o automorfismo de A tal que $E_{ij} \mapsto E_{\sigma(i)\sigma(j)}$ envia as matrizes $E_{i_1i_2}, \ldots, E_{i_{n-1}i_n}, E_{i_ni_1}$ em matrizes elementares de mesmo grau. Isto é, $\sigma \in H$, como queríamos demonstrar. $\square$

Lema 2.2.6. *Se A tem uma graduação elementar induzida por uma n-upla de elementos distintos de G então a órbita de todos os elementos no conjunto $\{1, 2, \ldots, n\}$ sob a ação canônica do grupo H tem exatamente $|H|$ elementos. Em particular, $|H|$ divide n.*

Demonstração. Fixe i um elemento qualquer do conjunto $\{1, 2, \ldots, n\}$. Da Observação 1.9.4 temos que $[H\colon Stab(i)] = |O(i)|$, onde $Stab(i)$ e $O(i)$ denotam o estabilizador e a órbita de i, respectivamente. Considere algum $\sigma \in H$ que satisfaz $\sigma(i) = i$, desse modo as matrizes $E_{i,j}$ e $E_{i,\sigma(j)}$ têm o mesmo grau, para todo j. Como a n-upla que determina a graduação consiste de elementos distintos, então $\sigma(j) = j$. Portanto o estabilizador de cada um dos elementos do conjunto $\{1, 2, \ldots, n\}$ é trivial, isto é, $|H| = |O(i)|$ para todo i em $\{1, 2, \ldots, n\}$. Por fim, basta observar que $n = \sum_{s=1}^{d} |O(i_s)|$ para algum sistema completo de representantes $i_1, \ldots, i_s$ das órbitas da ação canônica de H sobre $\{1, 2, \ldots, n\}$, o que conclui a demonstração. $\square$

Proposição 2.2.7. *Considere A uma álgebra munida da graduação elementar induzida pela n-upla $(h_1, \ldots, h_n)$ de elementos distintos de G. Se existir uma matriz diagonal não nula P e um polinômio graduado $f(x_{1,g_1}, \ldots, x_{m,g_m})$ que não seja identidade para A tal que o resultado de qualquer substituição admissível seja um múltiplo escalar de P então existe um homomorfismo (de grupos) $\lambda\colon H \to K^\times$ tal que P é igual a uma combinação linear de matrizes da forma $P(i_1), \ldots, P(i_d)$ nas condições do Lema 2.2.4. Reciprocamente, sejam $\lambda\colon H \to K^\times$ um homomorfismo e $P = diag(p_1, \ldots, p_n)$ uma matriz não nula escrita como combinação linear de matrizes $P(i_1), \ldots, P(i_d)$. Então o polinômio*

$$f(x_{1,g_1}, \ldots, x_{n,g_n}) = \sum_i p_i x_{\sigma^i(1),g_{\sigma^i(1)}} \ldots x_{\sigma^i(n),g_{\sigma^i(n)}}, \tag{2.5}$$

onde σ é o n-ciclo $(12\ldots n)$, $g_i = h_i^{-1}h_{i+1}$ para $i = 1, \ldots, n-1$ e $g_n = h_n^{-1}h_1$, não é uma identidade para A e tem a propriedade que para qualquer substituição f-admissível o resultado será um múltiplo escalar da matriz P.

Demonstração. Pela Proposição 2.2.3 temos que para todo σ em H existe um escalar não nulo $\lambda(\sigma)$ tal que $\Lambda_\sigma(P) = \lambda(\sigma)^{-1}P$. Aplicando agora o item (iii) do Lema 2.2.4 concluímos a primeira parte da proposição.

Já para provarmos a segunda parte do resultado observamos que o polinômio f é multilinear, portanto é suficiente demonstrar o resultado para substituições admissíveis de matrizes elementares. É claro que $f(E_{12}, \ldots, E_{n1}) = P$, o que implica que f não é uma identidade para A. Pelo Lema 2.2.5, toda substituição f-admissível de modo que o resultado seja não nulo é da forma $(\Lambda_\sigma(E_{12}), \ldots, \Lambda_\sigma(E_{n1}))$. Para concluir a demonstração, basta aplicar o item (iii) do Lema 2.2.4. $\square$

Seja G um grupo com exatamente n elementos, ou seja, $|G| = n$. Recordamos que uma graduação elementar de A induzida por uma n-upla de elementos distintos de G é chamada de **graduação produto cruzado**. A seguinte proposição é o último ingrediente na demonstração do teorema principal desta seção.

Proposição 2.2.8. *Seja A munida de uma graduação elementar induzida pela n-upla $(g_1, \ldots, g_n)$ de elementos distintos de G. Então A possui uma graduação produto cruzado pelo suporte da graduação se, e somente se, $|H| = n$. Além disso, nestas condições,* supp A *é um subgrupo de G isomorfo a H.*

Demonstração. Primeiramente vamos assumir, sem perda de generalidade, que a graduação elementar em A seja uma graduação produto cruzado. Assim para cada $g \in G$ existe uma permutação σ_g em S_n tal que

$$(gg_1, \ldots, gg_n) = (g_{\sigma_g(1)}, \ldots, g_{\sigma_g(n)}).$$

É fácil observar que a aplicação $\sigma\colon g \mapsto \sigma_g$ é um homomorfismo de grupos. De fato, sejam g, h elementos em G e observando a igualdade acima, temos que $g_{\sigma_g(j)} = gg_j$ para todo j. Portanto

$$g_{\sigma_g(\sigma_h(i))} = gg_{\sigma_h(i)} = ghg_i = g_{\sigma_{gh}(i)},$$

ou seja, $\sigma_g\sigma_h = \sigma_{gh}$. Caso $\sigma_g(j) = j$ para todo j, teremos que $g_j = gg_j$ implicando que $g = \epsilon$, isto é, o homomorfismo σ é injetivo. Por fim, iremos mostrar que a imagem de G por σ está em H. Seja E_{ij} uma matriz elementar de grau $g_i^{-1}g_j$, então para todo g em G o grau de $\Lambda_{\sigma_g}(E_{ij}) = E_{\sigma_g(i)\sigma_g(j)}$ é igual à

$$g_{\sigma_g(i)}^{-1}g_{\sigma_g(j)} = (gg_i)^{-1}(gg_j) = g_i^{-1}g_j,$$

o que conclui que Λ_{σ_g} é um automorfismo graduado. Isto significa que σ_g está em H para todo $g \in G$, implicando que $|H| \geqslant n$. Mas o Lema 2.2.6 implica que $|H|$ deve ser menor ou igual a n. Portanto σ é sobrejetiva. Concluímos que H e G são isomorfos e $|H| = n$.

Reciprocamente, assuma que $|H| = n$. O Lema 2.2.6 implica que existe apenas uma órbita, ou seja, a ação de H sobre $\{1, \ldots, n\}$ é transitiva. Tome g um elemento no suporte da graduação e uma matriz elementar E_{kl} de grau $g = g_k^{-1}g_l$. Assim, para todo i, existe σ em H tal que $\sigma(k) = i$ e a matriz elementar E_{ij} tem grau g se $j = \sigma(l)$. Agora se h é outro elemento que está no suporte da graduação então existe t tal que a matriz E_{jt} tenha grau $h = g_j^{-1}g_t$ e $E_{it} = E_{ij}E_{jt}$ tenha grau gh. Isto mostra que gh está no suporte. É claro que a matriz E_{tj} tem grau h^{-1}, e isso implica que h^{-1} está também no suporte da graduação. Além disso, para todo $h \in \operatorname{supp} A$, existem $i, j \in \{1, \ldots, n\}$ tais que $h = g_i^{-1}g_j$, considerando $\sigma_1 \in H$ tal que $\sigma_1(i) = 1$ temos que $h = g_1^{-1}g_{\sigma_1(j)}$. Tudo isso demonstra que o suporte desta graduação é um subgrupo de G de ordem n. Como os elementos $(\epsilon, g_1^{-1}g_2, \ldots, g_1^{-1}g_n)$ são elementos distintos em G, concluímos que a graduação é uma graduação produto cruzado sobre seu suporte e aplicando a primeira parte da proposição teremos que H e supp A são grupos isomorfos. □

Observação 2.2.9. *Segue da Proposição anterior que a graduação produto cruzado sobre a álgebra das matrizes definida nesta seção é um exemplo da graduação de G-produto* *cruzado apresentado na Definição 1.2.17. De fato, suponha que $A = M_n(K)$ possua uma graduação produto cruzado por um grupo G então a n-upla $(g_1, \ldots, g_n)$ é formada por todos elementos de G. Da Proposição 2.2.8 temos que para cada $g_i \in G$ existe $\sigma_i \in H$ tal que a aplicação $g_i \mapsto \sigma_i$ é um isomorfismo entre os grupos G e H. Para cada $i \in \{1, \ldots, n\}$, defina a matriz*

$$P(\sigma_i) = \sum_{j=1}^{n} E_{\sigma_i(j),\sigma_i(j+i)}.$$

Aqui iremos considerar, por abuso de notação, $j+i$ como sendo $\overline{j+i} \in \mathbb{Z}_n$. Observe que em todas as linhas da matriz $P(\sigma_i)$ existe apenas uma entrada não nula, pela definição do grupo H e $P(\sigma_i)^{-1} = \sum_{j=1}^{n} E_{\sigma_i(j+i),\sigma_i(j)}$, implicando que cada componente homogênea possui um elemento invertível. Porém, a $\mathbb{Z}_2$-graduação dada no Exemplo 1.2.5 da álgebra $M_4(K)$ é uma graduação $\mathbb{Z}_2$-produto cruzado dada na Definição 1.2.17, mas não é no sentido da definição dada nesta seção.

Estamos prontos para fazer uma caracterização das graduações elementares sobre A por n-uplas distintas que satisfazem a propriedade de primalidade. A demonstração deste resultado representa o “ápice” desta seção.

Teorema 2.2.10. *Seja A uma álgebra munida de uma graduação elementar induzida pela n-upla $(g_1, \ldots, g_n)$ de elementos distintos de G. A álgebra A satisfaz a propriedade de primalidade para polinômios centrais G-graduados se, e somente se, a graduação é uma graduação produto cruzado e o grupo G não possui representação linear de grau 1 além da trivial, ou seja, não existe homomorfismo $G \to K^\times$ não trivial.*

Demonstração. Vamos supor, por absurdo, que A não tenha a graduação produto cruzado. Então pela Proposição 2.2.8 temos que $|H| < n$. Neste caso o Lema 2.2.6 implica que o número d de órbitas em H agindo sobre $\{1, 2, \ldots, n\}$ é maior que 1. Considere $i_1, \ldots, i_d$ um sistema completo de representantes das órbitas da ação canônica de H sobre $\{1, 2, \ldots, n\}$ e junto com o homomorfismo trivial, podemos aplicar a Proposição 2.2.7 para obter um polinômio f de modo que o resultado obtido por toda substituição f-admissível é um múltiplo escalar da matriz diagonal

$$P = P(i_1) + \cdots + P(i_{d-1}) - P(i_d)$$

com $P^2 = I_n$. Observe que $d > 1$ implica que f não é um polinômio central graduado para A, mas o produto de duas copias de f em conjuntos disjuntos de variáveis é central. Segue que A não satisfaz a propriedade de primalidade. Suponha agora que a graduação em A seja produto cruzado, mas que G tenha uma representação de grau 1 não trivial. Pela Proposição 2.2.8 temos que H é isomorfo a G. Neste caso podemos considerar a existência de um homomorfismo não trivial $\lambda\colon H \to K^\times$ e considerar que a ação de H

sobre $\{1, 2, \ldots, n\}$ determina uma única órbita, digamos i_1, e assim $P = P(i_1)$. Aplicando o Lema 2.2.4, combinado com o homomorfismo λ e a Proposição 2.2.7 é possível obter um polinômio graduado f que não é identidade para A e que satisfaça ainda a propriedade de que o resultado de qualquer substituição f-admissível é um múltiplo escalar de P. Observe que $|H| = n$, então as entradas na diagonal de P estão na imagem de λ e portanto são raízes n-ésimas da unidade. Isto implica que $P^n = I_n$, e assim o produto de n copias de f em conjuntos disjuntos de variáveis é central. Como o homomorfismo λ é não trivial, temos que P não é uma matriz escalar e assim f não será central. Portanto, mais uma vez, A não satisfaz a propriedade de primalidade. Então a primeira parte do resultado segue.

Reciprocamente, assuma que a graduação em A seja uma graduação produto cruzado e que o único homomorfismo $G \to K^\times$ seja o trivial. Vamos fixar dois polinômios graduados $f(x_{1,g_1}, \ldots, x_{r,g_r})$ e $g(x_{r+1,g_{r+1}}, \ldots, x_{s,g_s})$ em conjuntos disjuntos de variáveis tais que o produto $f \cdot g$ seja um polinômio central graduado para A. Devemos provar que a matriz P obtida na Proposição 2.2.1 é um múltiplo escalar da matriz identidade; isto é suficiente para mostrar que f e g são polinômios centrais. Pela Proposição 2.2.3 existe um homomorfismo $\lambda\colon H \to K^\times$ tal que

$$\Lambda_\sigma(P) = \lambda(\sigma)^{-1}P.$$

Como a graduação é produto cruzado devemos ter que H e G são grupos isomorfos, e por hipótese λ deve ser o homomorfismo trivial. Além disso, pela ordem de H ser igual a n, o Lema 2.2.6 implica que a ação de H sobre $\{1, \ldots, n\}$ é transitiva. Neste caso, aplicando item (iii) do Lema 2.2.4, temos que P é uma matriz escalar. □

Observação 2.2.11. *A propriedade de primalidade pode não ser invariante por extensão de escalares. Por exemplo, considere o grupo $G = \mathbb{Z}_3$, se K for o corpo dos reais, então existe apenas uma $\mathbb{R}$-representações irredutível de grau 1, a trivial. Porém, caso K seja o corpo dos complexos, toda $\mathbb{C}$-representação irredutível é de grau 1, isto é, existem três $\mathbb{C}$-representações irredutíveis de grau 1. Aplicando o Teorema 2.2.10, $M_3(\mathbb{R})$ munida com sua $\mathbb{Z}_3$-graduação natural (a graduação de Vasilovsky) satisfaz a propriedade de primalidade para polinômios centrais $\mathbb{Z}_3$-graduado, mas $M_3(\mathbb{C})$ não.*

Como último resultado desta seção, provaremos que a propriedade de primalidade é invariante por graduação coarsening. Para rever os conceitos relacionados à graduação coarsening, direcionamos o leitor para a Definição 1.2.18.

Teorema 2.2.12. *Sejam $\Gamma\colon A = \bigoplus_{g\in G} A_g$ e $\Gamma'\colon A = \bigoplus_{h\in H} A_h$ graduações de uma álgebra A pelos grupos G e H, respectivamente. Além disso, considere que a H-graduação Γ' é um coarsening da G-graduação Γ. Se A satisfaz a propriedade de primalidade para polinômios centrais G-graduados, então ela também satisfaz a propriedade de primalidade para polinômios centrais H-graduados.*

Demonstração. Sejam $f(x_{1,h_1}, \ldots, x_{r,h_r})$ e $g(x_{r+1,h_{r+1}}, \ldots, x_{s,h_s})$ polinômios em conjuntos disjuntos de variáveis tais que o produto $f \cdot g$ seja um polinômio central H-graduado. Então existe uma substituição admissível $(A_1, \ldots, A_r, A_{r+1}, \ldots, A_s)$ tal que

$$f(A_1, \ldots, A_r) \cdot g(A_{r+1}, \ldots, A_s) \neq 0.$$

Considere, agora, uma substituição g-admissível tal que $g(A_{r+1}, \ldots, A_s)$ é uma matriz invertível. Como a H-graduação em A é um coarsening da G-graduação segue que cada matriz A_i é soma de matrizes homogêneas na G-graduação, digamos $A_i = B_{1,i} + \cdots + B_{k_i,i}$ onde todas as $B_{j,i}$ são matrizes de grau $g_{j,i}$ e $g_{k,i} \neq g_{l,i}$ se $k \neq l$. Definimos o polinômio G-graduado $p_i = \sum_{l=1}^{k_i} x_{i,g_{l,i}}$ e denotamos $\overline{f} = f(p_1, \ldots, p_r)$, $\overline{g} = g(p_{r+1}, \ldots, p_s)$. Observe que p_i e p_j são polinômios em conjuntos disjuntos de variáveis sempre que $i \neq j$ e portanto $\overline{f}$ e $\overline{g}$ também o são. É claro que se fizermos a substituição p_i-admissível $(B_{1,i}, \ldots, B_{k_i,i})$ em cada p_i o resultado obtido será A_i e portanto a substituição em $\overline{f}$ e $\overline{g}$ resultará em $f(A_1, \ldots, A_r)$ e $g(A_{r+1}, \ldots, A_s)$, respectivamente. Se o produto $\overline{f} \cdot \overline{g}$ for uma identidade graduada então $f(A_1, \ldots, A_r) \cdot g(A_{r+1}, \ldots, A_s) = 0$ e por $g(A_{r+1}, \ldots, A_s)$ ser invertível implica que $f(A_1, \ldots, A_r) = 0$, o que não é possível.

Assim $\overline{f} \cdot \overline{g}$ é um polinômio central G-graduado não-trivial, pois $f \cdot g$ é um polinômio central H-graduado. Como A satisfaz a propriedade de primalidade para polinômios centrais G-graduados isto implica que $\overline{f}$ e $\overline{g}$ são polinômios centrais G-graduados e portanto $f(A_1, \ldots, A_r)$ é um elemento pertencente ao centro de A. Isso prova que f é um polinômio central H-graduado. Usando passos completamente análogos provamos que g também é central H-graduado. □

2.3 Álgebra das Matrizes sobre uma Álgebra munida de uma Graduação Regular

Em [31], Diniz provou que o produto tensorial entre duas álgebras regulares satisfaz a propriedade de primalidade, se ambas satisfazerem a mesma propriedade, quando o corpo base é de característica zero. Em particular, a álgebra $M_n(E)$ satisfaz a propriedade de primalidade para polinômios centrais, uma vez que as álgebras $M_n(K)$ e E também a satisfazem. Recordamos aqui que a prova da propriedade em E foi feita na mesma referência. Vale ressaltar que a definição de álgebra regular foi dada na Seção 1.2, mais precisamente na Definição 1.2.21.

O principal objetivo desta seção é demonstrar que a álgebra $M_n(E)$ satisfaz a propriedade de primalidade quando o corpo base é infinito e de característica diferente de dois. Para isto, denotaremos por R uma álgebra regular (com unidade) e por A a álgebra das matrizes $M_n(K)$ de ordem n. Além disso, a álgebra $M_n(R)$ denotará a álgebra das matrizes de ordem n com entradas na álgebra regular R. Identificando a matriz escalar $diag(r, \ldots, r)$ como sendo o elemento r em R, podemos observar que R e A são subálgebras de $M_n(R)$. A graduação sobre $M_n(R)$, aqui considerada, será assumida de tal modo que R e A sejam subálgebras homogêneas e R seja graduada pelo grupo trivial. Assim a graduação $M_n(R) = \oplus_{g \in G}(M_n(R))_g$ terá componentes homogêneas da forma $(M_n(R))_g = \{rb \mid r \in R, b \in A_g\}$. O resultado principal desta seção (Teorema 2.3.15) é o seguinte: "se R é uma álgebra regular então $M_n(R)$ herda a propriedade de primalidade para os polinômios centrais graduados de A". Segue deste resultado e da propriedade de primalidade sobre A (com graduação trivial), obtida por Regev, a propriedade de primalidade para polinômios centrais ordinários em $M_n(E)$.

Observe que em muitos dos exemplos conhecidos de álgebras com graduação regular minimal por um grupo abeliano verifica-se que o centro da álgebra coincide com a componente neutra, ver Seção 1.2. Neste próximo resultado nós provaremos que a coincidência vale sob a seguinte condição mínima sobre a graduação regular:

Propriedade 2.3.1. *Para quaisquer $h, h' \in H$ e qualquer $0 \neq r_h \in R_h$ existe $s_{h'} \in R_{h'}$ com a propriedade de que $r_h s_{h'} \neq 0$.*

Proposição 2.3.2. *Seja R uma álgebra com uma graduação regular por um grupo H. Se a graduação regular for minimal e satisfaz a Propriedade 2.3.1 então $Z(R) = R_{\epsilon_H}$.*

Demonstração. Seja β o bicaracter que induz a H-graduação regular minimal de R. Para quaisquer $g, h \in H$ temos $r_g r_h = \beta(g,h) r_h r_g$ e $\beta(\epsilon_H, h) = 1$ implicando $R_{\epsilon_H} \subseteq Z(R)$. Observe que o centro $Z(R)$ é uma subálgebra homogênea de R. De fato, seja $z \in Z(R)$, então existem $z_1, \ldots, z_n$ elementos homogêneos de R tais que $z = z_1 + \cdots + z_n$. Como o grupo H é abeliano e ainda temos $rz = zr$ para todo $r \in R$, podemos tomar r como um elemento homogêneo. Isto implica que

$$(rz_1 - z_1 r) + \cdots + (rz_n - z_n r) = 0.$$

Por outro lado, a decomposição em componentes homogêneas é única, portanto obtemos que cada z_i está em $Z(R)$, o que conclui a afirmação. Suponha, por contradição, que $R_{\epsilon_H} \subsetneq Z(R)$ então existem elementos $h \neq \epsilon$ e $0 \neq z_h \in R_h$ tais que $z_h \in Z(R)$. Da hipótese desta proposição temos que dado qualquer $h' \in H$ existirá $w_{h'} \in R_{h'}$ tal que $z_h w_{h'} \neq 0$. Obteremos, desta forma, $w_{h'} z_h = z_h w_{h'} = \beta(h, h') w_{h'} z_h$ e concluímos que $\beta(h, h') = 1$ para todo $h' \in H$. Esta última afirmação contradiz a minimalidade da graduação regular. □

Observação 2.3.3. *Observamos que nenhuma das duas hipóteses da proposição anterior pode ser removida. Se R for uma álgebra com graduação regular que não seja minimal, então existe $h \in H \backslash \{\epsilon_H\}$ tal que $\beta(h, g) \neq 1$, para todo $g \in H$ e a inclusão será estrita.*

Por outro lado, considere a álgebra R definida da seguinte forma:

$$\langle 1, f, e_1, e_2, \ldots \mid fe_i = e_i f = 0, f^2 = 0, e_j e_j = -e_j e_i \rangle,$$

onde a subálgebra de R gerada pelos elementos e_i é a álgebra de Grassmann. Temos que a decomposição

$$R_0 = E_0 \quad e \quad R_1 = E_1 \oplus \langle f \rangle$$

é uma $\mathbb{Z}_2$-graduação regular minimal sobre R, porém f é central e portanto $Z(R)$ contém propriamente R_0.

Nosso próximo resultado caracterizará a verificação de quando um polinômio G-graduado é uma identidade para $M_n(R)$. Esse resultado será importante para a demonstração do teorema principal da seção.

Lema 2.3.4. *Seja R uma álgebra com uma graduação regular por um grupo abeliano H tal que $Z(R) = R_{\epsilon_H}$ e seja $M_n(R)$ munida de uma G-graduação tal que $R \subseteq (M_n(R))_{\epsilon_G}$. Se $f = f(x_{1,g_1}, \ldots, x_{r,g_r})$ é um polinômio tal que o resultado de toda substituição f-admissível de elementos em $M_n(R)$ está em R_h, para algum $h \neq \epsilon_H$, então f é uma identidade graduada para $M_n(R)$.*

Demonstração. Seja $(a_1, \ldots, a_r)$ uma substituição f-admissível de elementos em $M_n(R)$, segue do Corolário 2.1.4 que para todos $h' \in H$ e $m' \in R_{h'}$ o comutador $[f(a_1, \ldots, a_r), m']$ está em R_h. Aqui consideramos R contido em $(M_n(R))_{\epsilon_G}$, tomamos $V = R_h$ e por H ser um grupo abeliano, temos que ambos $f(a_1, \ldots, a_r) \cdot m'$ e $m' \cdot f(a_1, \ldots, a_r)$ estão em $R_{hh'}$. Portanto $[f(a_1, \ldots, a_r), m']$ está em $R_{hh'}$. Se $h' \neq \epsilon_H$ então $h \neq hh'$ implicando que $R_{hh'} \cap R_h = \{0\}$. Desta maneira podemos concluir que $[f(a_1, \ldots, a_r), m'] = 0$. Note que $f(a_1, \ldots, a_r)$ comuta com todo elemento em $R_{h'}$, para todo $h' \in H$ diferente de ϵ_H. Além disso, como $\beta(\epsilon_H, h) = 1$ podemos deduzir que $f(a_1, \ldots, a_r)$ comuta também com todos os elementos de R_{ϵ_H}. Isto implica que $f(a_1, \ldots, a_r)$ está em $Z(R) = R_{\epsilon_H}$. Neste caso, $f(a_1, \ldots, a_r)$ está em $R_h \cap R_{\epsilon_H} = \{0\}$, e portanto $f(a_1, \ldots, a_r) = 0$. Concluímos assim que f é uma identidade graduada para $M_n(R)$. □

Sejam R uma álgebra que possui uma graduação regular pelo grupo abeliano H e $\beta\colon H \times H \to K^\times$ o seu respectivo bicaracter. Se $m(x_1, \ldots, x_s)$ é um monômio de grau d_i em x_i e $(r_1, \ldots, r_s)$ uma s-upla de elementos H-homogêneos de R, então a condição *(P2)* da Definição 1.2.21 implicará que

$$m(r_1, \ldots, r_s) = \lambda r_1^{d_1} \cdots r_s^{d_s},$$

para algum escalar λ não nulo.

Observação 2.3.5. *O escalar λ descrito anteriormente não depende da s-upla de elementos escolhida de R, mas do monômio m, do bicaracter $\beta\colon H \times H \to K^\times$ e da s-upla $\boldsymbol{h} = (h_1, \ldots, h_s)$ tal que $r_i \in R_{h_i}$. Tal escalar será denotado por $\epsilon^R_{\boldsymbol{h},m}$, ou simplesmente por*

$\epsilon_{\boldsymbol{h},m}$ *se não tiver dúvida em qual álgebra regular estaremos trabalhando. Desta maneira temos que*

$$m(r_1, \ldots, r_s) = \epsilon_{\boldsymbol{h},m} r_1^{d_1} \cdots r_s^{d_s}.$$

Definição 2.3.6. *Sejam* $f(x_{1,g_1}, \ldots, x_{n,g_n})$ *um polinômio graduado multihomogêneo na álgebra* $K\langle X_G \rangle$ *e* $\boldsymbol{h} = (h_1, \ldots, h_n) \in H^n$*. Escrevendo* $f = \sum_i \alpha_i m_i$ *como uma combinação linear de monômios, podemos definir* $f_{\boldsymbol{h}}$ *como*

$$f_{\boldsymbol{h}}(x_{1,g_1}, \ldots, x_{n,g_n}) = \sum_i \epsilon_{\boldsymbol{h},m_i} \alpha_i m_i.$$

Observação 2.3.7. *Se* $f(x_{1,g_1}, \ldots, x_{n,g_n})$ *é um polinômio graduado multihomogêneo de grau* d_i *em* x_{i,g_i}*,* $r_i \in R_{h_i}$ *e* $a_i \in A$ *então*

$$f(r_1 a_1, \ldots, r_t a_t) = r_1^{d_1} \cdots r_t^{d_t} f_{\boldsymbol{h}}(a_1, \ldots, a_t),$$

onde $\boldsymbol{h} = (h_1, \ldots, h_t)$*.*

Para os próximos resultados iremos considerar que R é uma álgebra com uma H-graduação regular que satisfaz a seguinte propriedade:

Propriedade 2.3.8. *Para quaisquer dois monômios* m_1 *e* $m_2 \in K\langle X_H \rangle$*, em conjuntos disjuntos de variáveis, que não são identidades* H*-graduadas para a álgebra* R *teremos que o produto* $m_1 \cdot m_2$ *também não é identidade graduada para* R*.*

As álgebras com graduação regular apresentadas no Exemplo 1.2.23 satisfazem essa propriedade. Uma álgebra R que satisfaz a Propriedade 2.3.8 deverá satisfazer também uma propriedade graduada análoga à definição de álgebra verbalmente prima.

Proposição 2.3.9. *Seja* R *uma álgebra com uma* H*-graduação regular que satisfaz a Propriedade 2.3.8. Se* $f, g \in K\langle X_H \rangle$ *são polinômios graduados em conjuntos disjuntos de variáveis que não são identidades para* R *então* $f \cdot g$ *também não é identidade graduada para* R*.*

Demonstração. Da Proposição 2.1.3 podemos assumir, sem perda de generalidade, que os polinômios f, g são multihomogêneos. Pela Observação 2.3.5, temos que f, g são, módulo $Id_H(R)$, múltiplos escalares de monômios em conjuntos disjuntos de variáveis. Portanto, a Propriedade 2.3.8 implica que $f \cdot g$ não está em $Id_H(R)$. Logo $f \cdot g$ não é identidade graduada para a álgebra H-graduada R. □

Corolário 2.3.10. *Seja* R *uma álgebra munida de uma* H*-graduação regular minimal a qual satisfaz a Propriedade 2.3.8. Se* $R' = K\langle X_H \rangle / Id_H(R)$*, com a sua* H*-graduação canônica, então* $Z(R') = R'_{\epsilon_H}$*.*

Demonstração. Sejam $h, h' \in H$ e $r'_h = f + Id_H(R)$ um elemento não nulo em R'_h. Consideramos um m de modo que $x_{m,h'}$ não seja variável em f. A Proposição 2.3.9 implica que $f \cdot x_{m,h'}$ não está em $Id_H(R)$. Portanto $r'_h s'_{h'} \neq \bar{0}$, onde $s'_{h'} = x_{m,h'} + Id_H(R)$. Desta forma o resultado segue da Proposição 2.3.2. □

Na próxima proposição observaremos que as álgebras regulares R que satisfazem a Propriedade 2.3.8, são de fato verbalmente primas. Sobre um corpo algebricamente fechado de característica zero, existe uma descrição dessas álgebras que têm uma graduação regular não degenerada por um grupo finito. O leitor pode encontrar maiores detalhes em [4, Corolário 42].

Proposição 2.3.11. *Uma álgebra R com uma H-graduação regular que satisfaz a Propriedade 2.3.8 é verbalmente prima.*

Demonstração. Sejam $f(x_1, \ldots, x_t)$, $g(x_{t+1}, \ldots, x_s)$ polinômios em $K\langle X\rangle$ em conjuntos disjuntos de variáveis, nenhum deles uma identidade para R. Proposição 2.1.3 implica que existem polinômios multihomogêneos $f'(x_1, \ldots, x_{t'}) \in \langle f\rangle^T$, $g'(x_{t'+1}, \ldots, x_{s'}) \in \langle g\rangle^T$ e elementos homogêneos $r_1, \ldots, r_{t'}, \ldots, r_{s'}$ com $f'(r_1, \ldots, r_{t'}) \neq 0$ e $g(r_{t'+1}, \ldots, r_{s'}) \neq 0$. Pela Observação 2.3.5 e pela Propriedade 2.3.8, o produto $f'(x_1, \ldots, x_{t'}) \cdot g'(x_{t'+1}, \ldots, x_{s'})$ não é uma identidade para R. Como $f' \cdot g'$ está em $\langle f \cdot g\rangle^T$, podemos concluir, usando Proposição 2.1.3 que $f \cdot g$ não é uma identidade ordinária para R. □

Recordando o que foi demonstrado no Teorema 2.2.12, os próximos resultados nos providenciam que a Propriedade 2.3.8 é invariante por graduação coarsenings e ainda mais, que a propriedade de primalidade se transfere para álgebras que satisfazem as mesmas identidades G-graduadas.

Lema 2.3.12. *Seja R uma álgebra H-graduada regular. Então R satisfaz a Propriedade 2.3.8 se, e somente se, todo coarsening desta graduação satisfaz a Propriedade 2.3.8.*

Demonstração. Primeiramente, vamos supor que exista uma H'-graduação sobre R coarsening da H-graduação que não satisfaça a Propriedade 2.3.8. Isso implicaria a existência de m_1, m_2 monômios em $K\langle X_{H'}\rangle$, em conjuntos disjuntos de variáveis, que não são identidades H'-graduadas para a álgebra R, mas o produto $m_1 \cdot m_2$ o é. Logo, para toda substituição admissível $(r_1, \ldots, r_s, r_{s+1}, \ldots, r_t)$ teríamos $m_1(r_1, \ldots, r_s) \cdot m_2(r_{s+1}, \ldots, r_t) = 0$, onde os r_i's são elementos homogêneos na H'-graduação. Portanto podemos considerar uma substituição admissível tal que $m_1(r_1, \ldots, r_s)$ e $m_2(r_{s+1}, \ldots, r_t)$ sejam não nulos. Por outro lado, utilizando a mesma notação dada na demonstração do Teorema 2.2.12, podemos escrever cada $r_i = w_{1,i} + \cdots + w_{k_i,i}$ como soma de elementos homogêneos $w_{1,i}, \ldots, w_{k_i,i}$ na H-graduação de graus $h_{1,i}, \ldots, h_{k_i,i}$, respectivamente, e $h_{j,i} \neq h_{l,i}$, se $j \neq l$. Consideramos os polinômios $p_i = \sum_{l=1}^{k_i} x_{i,h_{l,i}}$ e definimos $\overline{m}_1 = m_1(p_1, \ldots, p_s)$ e $\overline{m}_2 = m_2(p_{s+1}, \ldots, p_t)$.

Observe que p_i, p_j são polinômios H'-graduados em conjuntos disjuntos de variáveis sempre que $i \neq j$. Isso implica que $\overline{m}_1$ e $\overline{m}_2$ são polinômios H-graduados em conjuntos disjuntos de variáveis. Obviamente a substituição de $x_{i,h_{l,i}}$ por $w_{l,i}$ em p_i resultará em r_i e portanto as substituições em $\overline{m}_1$ e $\overline{m}_2$ serão $m_1(r_1, \ldots, r_s)$ e $m_2(r_{s+1}, \ldots, r_t)$, respectivamente. Mas isto implica que $\overline{m}_1$ e $\overline{m}_2$ não são identidades H-graduadas. Por R satisfazer a Propriedade 2.3.8 em sua H-graduação, podemos utilizar a Proposição 2.3.9 e teremos que o produto $\overline{m}_1 \cdot \overline{m}_2$ não é identidades H-graduada. Mas isto contraria o fato de $m_1 \cdot m_2$ ser identidade H'-graduada.

A afirmação reciproca é imediata, uma vez que a H-graduação em R é coarsening nela própria. Portanto o lema está demonstrado. □

Lema 2.3.13. *Sejam B e B' álgebras graduadas por um mesmo grupo G. Se B e B' são G-PI-equivalentes, ou seja, $Id_G(B) = Id_G(B')$. Então B satisfaz a propriedade de primalidade para polinômios centrais graduados se, e somente se, B' também a satisfaz.*

Demonstração. Sejam $f(x_{1,g_1}, \ldots, x_{t,g_t})$ e $g(x_{t+1,g_{t+1}}, \ldots, x_{s,g_s})$ polinômios em $K\langle X_G \rangle$ em conjuntos disjuntos de variáveis que não sejam identidades para B', mas que $f \cdot g$ seja polinômio central graduado para B', isto é, $[f \cdot g, x_h]$ está em $Id_G(B')$, para qualquer $h \in G$. Como B e B' são G-PI-equivalentes, temos que $[f \cdot g, x_h] \in Id_G(B)$ implicando que $f \cdot g$ é um polinômio central G-graduado para B. Se B satisfaz a propriedade de primalidade para polinômios centrais graduados então $f(x_{1,g_1}, \ldots, x_{t,g_t})$ e $g(x_{t+1,g_{t+1}}, \ldots, x_{s,g_s})$ também são polinômios centrais G-graduados para B. Para concluir o resultado basta aplicar o "truque" da G-PI-equivalência novamente e observar que $f(x_{1,g_1}, \ldots, x_{t,g_t})$ e $g(x_{t+1,g_{t+1}}, \ldots, x_{s,g_s})$ são polinômios centrais G-graduados para B'. □

Lema 2.3.14. *Sejam R e R' duas álgebras regulares graduadas por um mesmo grupo abeliano finito H que são H-PI-equivalentes. Então $M_n(R)$ e $M_n(R')$ são G-PI-equivalentes.*

Demonstração. Denote por $\mathcal{B}'$ uma base para $M_n(R')$ consistindo de elementos homogêneos e suponha que exista um polinômio G-graduado multihomogêneo f em $K\langle X_G \rangle$ tal que $f \in Id_G(M_n(R)) \backslash Id_G(M_n(R'))$. Da Proposição 2.1.3, existe $f'(x_{1,g_1}, \ldots, x_{t,g_t})$ em $\langle f \rangle^{T_G}$ e uma substituição f'-admissível $(r'_1 a_1, \ldots, r'_t a_t)$ de elementos da base $\mathcal{B}'$ para os quais temos

$$f'(r'_1 a_1, \ldots, r'_t a_t) = {r'_1}^{d_1} \cdots {r'_t}^{d_t} f_{\mathbf{h}}(a_1, \ldots, a_t) \neq 0,$$

implicando que a substituição $f_{\mathbf{h}}$-admissível $(a_1, \ldots, a_t)$ de elementos de A é não nula. Segue que o monômio $m = m(x_{1,h_1}, \ldots, x_{t,h_t}) = x_{1,h_1}^{d_1} \cdots x_{t,h_t}^{d_t}$ não pertence a $Id_H(R')$. Aqui h_i denota o grau do elemento homogêneo r'_i na graduação de R' e $\mathbf{h} = (h_1, \ldots, h_t)$ é a t-upla obtida pela respectiva substituição admissível. Porém, se tomarmos quaisquer elementos $r_1, \ldots, r_t$ de R com h_i sendo o grau do elemento homogêneo r_i na graduação de R, teremos que

$$0 = f'(r_1a_1, \dots, r_ta_t) = {r_1}^{d_1} \cdots {r_t}^{d_t} f_{\mathbf{h}}(a_1, \dots, a_t),$$

o que é um absurdo já que $Id_H(R) = Id_H(R')$. □

De agora em diante, iremos considerar uma álgebra $M_n(R)$ munida de uma G-graduação tal que:

(Gr1) R é uma subálgebra homogênea e $R \subseteq (M_n(R))_\epsilon$;

(Gr2) A é uma subálgebra homogênea.

Agora estamos prontos para enunciar e demonstrar o resultado principal desta seção.

Teorema 2.3.15. *Seja $M_n(R)$ uma álgebra G-graduada que satisfaz as condições* (Gr1) *e* (Gr2)*. Se R possui uma graduação regular, por um grupo abeliano H, satisfazendo a Propriedade 2.3.8 e a álgebra $A = M_n(K)$ (com a G-graduação herdada de $M_n(R)$) satisfaz a propriedade de primalidade para polinômios centrais graduados, então a álgebra $M_n(R)$ também satisfaz a propriedade de primalidade.*

Demonstração. Primeiramente, provaremos que podemos assumir sem perda de generalidade que a álgebra regular R que satisfaz a Propriedade 2.3.8 possui centro da forma $Z(R) = R_{\epsilon_H}$, onde ϵ_H é o elemento neutro do grupo H. Segue do Lema 2.3.12 que toda graduação coarsening da H-graduação de R satisfaz a Propriedade 2.3.8. Além disso toda graduação regular de R admite um coarsening por uma imagem homomórfica sobre H que é minimal. Portanto podemos assumir que a álgebra R possui uma graduação regular minimal que satisfaz a Propriedade 2.3.8. Por simplicidade de notação, diremos que tal graduação é dada pelo grupo H. Observamos que a H-graduação canônica da álgebra $R' = F\langle X_H\rangle / Id_H(R)$ é uma graduação regular minimal que satisfaz a Propriedade 2.3.8. Aplicando o Corolário 2.3.10 temos que $Z(R') = R'_{\epsilon_H}$.

Consideramos a álgebra $M_n(R')$ munida com a G-graduação cuja as suas componentes homogêneas é dada por $(M_n(R'))_g = \{r'a \mid r' \in R', a \in A_g\}$. Pelo Lema 2.3.14, $M_n(R)$ e $M_n(R')$ satisfazem as mesmas identidades G-graduadas. Nestas condições, podemos aplicar o Lema 2.3.13 e concluir que $M_n(R)$ satisfaz a propriedade de primalidade se, e somente se, $M_n(R')$ também a satisfaz. Portanto daqui em diante iremos assumir que R possui uma graduação regular, por um grupo abeliano H, satisfazendo a Propriedade 2.3.8 e $Z(R) = R_{\epsilon_H}$.

Vamos agora demonstrar o resultado principal. Seja $f(x_{1,g_1}, \dots, x_{t,g_t})$ um polinômio graduado em $K\langle X_G\rangle$ tal que o produto $f \cdot g$ seja um polinômio central graduado para A_R para algum $g(x_{t+1,g_{t+1}}, \ldots, x_{s,g_s})$ cujo conjunto de variáveis em g é disjunta das de f. Provaremos que f é um polinômio central graduado para A_R. Primeiramente afirmamos que existem um polinômio $g'(x_{1,g_1}, \ldots, x_{m,g_m})$ em $\langle g \rangle^{T_G}$, uma m-upla $\mathbf{h} = (h_1, \ldots, h_m)$ em H^m e uma substituição $g'_{\mathbf{h}}$-admissível $(a_1, \ldots, a_m)$ de modo que $g'_{\mathbf{h}}(a_1, \ldots, a_m)$ seja elemento invertível da álgebra A.

Seja $\mathcal{B}_R$ (e $\mathcal{B}_A$) base de R (e A) de elementos homogêneos na H-graduação (e na G-graduação). É claro que

$$\mathcal{B} = \{mM \mid m \in \mathcal{B}_R, M \in \mathcal{B}_A\}$$

é uma base para $M_n(R)$. Como o produto $f \cdot g$ não é uma identidade graduada para $M_n(R)$, segue da Proposição 2.1.3 que existem $f'(x_{1,g_1}, \ldots, x_{m,g_m})$ em $\langle f \rangle^{T_G}$, $g'(x_{1,g_1}, \ldots, x_{m,g_m})$ em $\langle g \rangle^{T_G}$ e uma substituição admissível $(r_1a_1, \ldots, r_ma_m)$ de elementos em $\mathcal{B}$ tais que

$$f'(r_1a_1, \ldots, r_ma_m) \cdot g'(r_1a_1, \ldots, r_ma_m) \neq 0. \tag{2.6}$$

Segue da Proposição 2.1.5 que o elemento acima pertence ao centro da álgebra A_R. Denotamos por h_i o grau do elemento homogêneo r_i na graduação homogênea de R e $\mathbf{h} = (h_1, \ldots, h_m)$ a m-upla obtida pela substituição admissível anterior. Usando a Observação 2.3.7 podemos reescrever os elementos acima da forma

$$(r_1^{d_1} \cdots r_m^{d_m}) \cdot (r_1^{e_1} \cdots r_m^{e_m}) f'_{\mathbf{h}}(a_1, \ldots, a_m) \cdot g'_{\mathbf{h}}(a_1, \ldots, a_m), \tag{2.7}$$

onde d_i e e_i denotam os graus de x_{i,g_i} em f' e em g', respectivamente. Como o elemento (2.7) é central, temos que o produto

$$f'_{\mathbf{h}}(a_1, \ldots, a_m) \cdot g'_{\mathbf{h}}(a_1, \ldots, a_m) \tag{2.8}$$

está no centro de A, ou seja, é um múltiplo escalar da identidade de A diferente de zero por causa da equação (2.6). Portanto $g'_{\mathbf{h}}(a_1, \ldots, a_m)$ é um elemento invertível de A, obtendo assim a demonstração da afirmação.

Defina h^{-1} o grau do elemento $(r_1^{e_1} \cdots r_m^{e_m})$ na graduação regular de R. Provaremos, agora, que o resultado de qualquer substituição admissível no polinômio f está em R_h. Pela igualdade (2.6), temos que f não é identidade, então segue desta afirmação, do Lema 2.3.4 e da Definição de polinômio central graduado próprio que f é um polinômio central graduado para A_R. Sejam $f''(y_{1,g_1}, \ldots, y_{s,g_s})$ um polinômio em $\langle f \rangle^{T_G}$ e $(w_1b_1, \ldots, w_sb_s)$ uma substituição f''-admissível de elementos em $\mathcal{B}$. Denote por $\mathbf{k} = (k_1, \ldots, k_s)$ a s-upla obtida pela substituição f''-admissível com k_i sendo o grau do elemento homogêneo w_i na graduação regular de R. Aplicando, novamente, a Proposição 2.1.5 temos que o produto $f''(y_{1,g_1}, \ldots, y_{s,g_s}) \cdot g'(x_{1,g_1}, \ldots, x_{m,g_m})$ é um polinômio central graduado para A_R. Portanto o elemento

$$(w_1^{c_1} \cdots w_s^{c_s}) \cdot (r_1^{e_1} \cdots r_m^{e_m}) f''_{\mathbf{k}}(b_1, \ldots, b_s) \cdot g'_{\mathbf{h}}(a_1, \ldots, a_m), \tag{2.9}$$

onde c_i é o grau de y_{i,g_i} em f'', é central em $M_n(R)$. Se provarmos que $f''(w_1b_1, \ldots, w_sb_s)$ está em R_h, pela arbitrariedade de tal elemento, podemos aplicar o Lema 2.1.3 e isto implicará a afirmação que queremos demonstrar.

Assuma que

$$f''(w_1b_1, \ldots, w_sb_s) = (w_1^{c_1} \cdots w_s^{c_s})f''_{\mathbf{k}}(b_1, \ldots, b_k) \neq 0.$$

Além disso, podemos aplicar a Propriedade 2.3.8 de R e ainda podemos supor, sem perda de generalidade, que

$$(w_1^{c_1} \cdots w_s^{c_s}) \cdot (r_1^{e_1} \cdots r_m^{e_m}) \neq 0.$$

(Caso contrário basta trocar os elementos homogêneos $(w_1, \cdots, w_s)$ de R e utilizar o mesmo argumento.) Neste caso o produto $f''_{\mathbf{k}}(b_1, \ldots, b_m) \cdot g'_{\mathbf{h}}(a_1, \ldots, a_m)$ é um múltiplo escalar da identidade de A. Fixando a substituição $g'_{\mathbf{h}}$-admissível, temos que para toda substituição $f''_{\mathbf{k}}$-admissível o resultado do produto $f''_{\mathbf{k}} \cdot g'_{\mathbf{h}}$ é um múltiplo escalar da identidade de A. Como $f''_{\mathbf{k}}(b_1, \ldots, b_m)$ é um elemento não nulo em A e $g'_{\mathbf{h}}(a_1, \ldots, a_m)$ é invertível, temos que $f''_{\mathbf{k}} \cdot g'_{\mathbf{h}}$ não é uma identidade para A. Renomeando as variáveis se necessário, podemos supor que $f''_{\mathbf{k}}$ e $g'_{\mathbf{h}}$ são polinômios em conjuntos disjuntos de variáveis, e assim o produto $f''_{\mathbf{k}} \cdot g'_{\mathbf{h}}$ é um polinômio central para A. Por A satisfazer a propriedade de primalidade concluímos que $f''_{\mathbf{k}}$ é um polinômio central graduado para A. Portanto $f''_{\mathbf{k}}(b_1, \ldots, b_k)$ é um múltiplo escalar da identidade de A. Como $Z(R) = R_{\epsilon_H}$ e A é central, é claro que o centro de A está contido em R_{ϵ_H}. Além disso, pelo fato do elemento (2.9) estar em $Z(M_n(R))$ teremos $(w_1^{c_1} \cdots w_s^{c_s}) \cdot (r_1^{e_1} \cdots r_m^{e_m})$ em R_{ϵ_H}, implicando que $(w_1^{c_1} \cdots w_s^{c_s})$ está em R_h. A substituição f''-admissível foi escolhida arbitrariamente, logo concluímos que $f''(w_1b_1, \ldots, w_sb_s)$ está em R_h. Para o elemento g basta seguir passos totalmente análogos. Portanto, concluímos a demonstração. □

Observação 2.3.16. *Sobre um corpo de característica zero, a hipótese de R satisfazer a Propriedade 2.3.8 é completamente desnecessária, uma vez que podemos reduzir o trabalho para polinômios multilineares e tal propriedade segue diretamente de (P1) da Definição 1.2.21.*

Como consequência imediata do teorema anterior podemos deduzir os seguintes corolários.

Corolário 2.3.17. *Sejam $G = \{g_1, \ldots, g_r\}$ um grupo tal que o único homomorfismo $G \to K^\times$ é o trivial, k um número natural e $\boldsymbol{g} = (g_1, \ldots, g_1, \ldots, g_r, \ldots, g_r)$ uma n-upla de elementos de G onde cada elemento aparece k vezes. A álgebra das matrizes $M_n(K)$, onde $n = kr$, munida da graduação elementar induzida por $\boldsymbol{g}$ satisfaz a propriedade de primalidade para polinômios centrais graduados.*

Demonstração. Seja $R = M_k(K)$ e considere $M_r(R)$ munida com a G-graduação onde suas componentes homogêneas são dadas por $M_r(R)_g = \langle rE_{ij} \mid g_i^{-1}g_j = g\rangle$. Considerando $M_r(R)$ o espaço das matrizes em blocos, podemos definir o isomorfismo canônico $\varphi\colon M_r(R) \to M_n(K)$. Note que φ é um isomorfismo graduado se $M_n(K)$ possui a graduação elementar induzida por $\mathbf{g}$. Observe ainda que a álgebra R possui uma graduação regular que satisfaz a Propriedade 2.3.8 (ver Exemplo 1.2.23) e $M_r(R)$ satisfaz as condições (Gr1) e (Gr2). Portanto o resultado segue aplicando o teorema anterior junto com o Teorema 2.2.10. □

Corolário 2.3.18. *A álgebra $M_n(E)$ (munida com a graduação trivial) satisfaz a propriedade de primalidade para polinômios centrais.*

Demonstração. A $\mathbb{Z}_2$-graduação natural de E é regular e satisfaz as hipóteses do Teorema 2.3.15. Além disso, a álgebra $M_n(K)$ é central simples e, munida com a graduação trivial, satisfaz a propriedade de primalidade (ver [78]). □

O Corolário anterior generaliza o resultado principal de [31] que foi provado para álgebras sobre um corpo de característica zero.

Corolário 2.3.19. *Seja G um grupo cuja única representação irredutível de grau 1 é a trivial. Se $M_n(E)$ possui uma G-graduação tal que E é uma subálgebra homogênea com a graduação trivial e $M_n(K)$ é uma subálgebra homogênea com a graduação produto cruzado induzida por G, então $M_n(E)$ satisfaz a propriedade de primalidade para polinômios centrais G-graduados.*

Demonstração. Do Teorema 2.2.10, $M_n(K)$ satisfaz a propriedade de primalidade para polinômios centrais G-graduados. Aplicando o Teorema 2.3.15 obtemos que $M_n(E)$ herda a propriedade de $M_n(K)$. □

A álgebra $R = M_m(K)$ possui uma graduação regular que satisfaz as hipóteses do Teorema 2.3.15 (ver [13]). Aplicando o resultado principal desta seção, temos que a álgebra $M_n(R) \cong M_{mn}(K)$ das matrizes sobre o corpo K, com a graduação herdada do produto cruzado de $M_n(K)$, satisfaz a propriedade de primalidade para polinômios centrais graduados. Essa graduação é diferente da graduação produto cruzado de $M_{mn}(K)$.

Corolário 2.3.20. *Seja R uma álgebra que possua uma graduação regular, por um grupo abeliano H, satisfazendo a Propriedade 2.3.8. A álgebra R satisfaz a propriedade de primalidade para polinômios centrais (ordinários).*

Demonstração. Basta aplicar o Teorema 2.3.15 para $A = K$. □

Observação 2.3.21. *Sobre um corpo de característica zero, toda álgebra regular satisfaz a propriedade de primalidade para polinômios centrais (ordinários).*

Seja R uma álgebra que possua uma graduação regular, por um grupo abeliano H, satisfazendo a Propriedade 2.3.8. Uma pergunta natural a se fazer é a seguinte: "A álgebra R satisfaz a propriedade de primalidade para polinômios centrais H-graduados?" Tal afirmação não é verdadeira. Por exemplo, podemos considerar $R = E$ a álgebra de Grassmann de um espaço vetorial de dimensão infinita munida de sua $\mathbb{Z}_2$-graduação canônica e assim, $x_{1,\bar{1}}x_{2,\bar{1}}$ é um polinômio central $\mathbb{Z}_2$-graduado para R, mas $x_{1,\bar{1}}$ e $x_{2,\bar{1}}$ não o são. Mais geralmente, seja R uma álgebra que possua uma graduação regular por um grupo abeliano H, satisfazendo a Propriedade 2.3.8. Pela Demonstração do Teorema 2.3.15 e pela condição *(P2)* da Definição 1.2.21, o monômio $x_h x_{h^{-1}}$, para todo $h \in H$ com $h \neq \epsilon_H$, é central H-graduado para R, mas x_h e $x_{h^{-1}}$ não o são. Portanto, as álgebras que possuam uma graduação regular, por um grupo abeliano H, satisfazendo a Propriedade 2.3.8 não satisfazem a propriedade de primalidade para polinômios centrais H-graduados.

2.4 Propriedade de Primalidade para as Álgebras $M_{a,b}(E)$

Pelo Corolário 2.3.20, as álgebras verbalmente primas $M_n(K)$ e $M_n(E)$ satisfazem a propriedade de primalidade para polinômios centrais, já que possuem graduações regulares que satisfazem a Propriedade 2.3.8, ver Exemplos 1.2.8 e 1.2.25, respectivamente.

Sob a hipótese do corpo ter característica zero, em [31] Diniz provou que as álgebras $M_n(K)$, $M_n(E)$ e $M_{a,a}(E)$ satisfazem a propriedade de primalidade e em [83] Samoilov demonstrou, considerando um corpo de característica qualquer, que a propriedade de primalidade é válida para álgebras verbalmente primas se considerarmos "apenas" polinômios multilineares. Ressaltamos que o resultado de Samoilov em característica 0, implica na primalidade, pois podemos linearizar e "simetrizar" os nossos polinômios sem "perder" informação.

Assim, entre as importantes álgebras $M_n(K)$, $M_n(E)$ e $M_{a,b}(E)$, supondo o corpo infinito e de característica diferente de 2, a única para a qual precisamos verificar a propriedade de primalidade, é a álgebra $M_{a,b}(E)$. Note que se $a \neq b$ não é conhecida uma graduação regular para este tipo de álgebra.

Observação 2.4.1. *Por cálculos diretos podemos verificar que $M_{1,1}(E)$ também não satisfaz a propriedade de primalidade para polinômios centrais $\mathbb{Z}_2$-graduados. Basta observar que $x_{1,\bar{1}}^2 \cdot x_{2,\bar{1}}^2$ é um polinômio central $\mathbb{Z}_2$-graduado para $M_{1,1}(E)$, mas $x_{1,\bar{1}}^2$, $x_{2,\bar{1}}^2$ não o são.*

Nesta seção iremos apresentar a demonstração de que a álgebra $M_{a,b}(E)$ satisfaz a propriedade de primalidade para polinômios centrais no caso ordinário, para isto usaremos a $\mathbb{Z}_2$-graduação canônica de E.

Lema 2.4.2. *Sejam $A = A_0 \oplus A_1$ a álgebra $M_{a,b}(E)$ munida com sua $\mathbb{Z}_2$-graduação canônica e $f(x_1, \ldots, x_r)$ um polinômio em $K\langle X\rangle$ tal que para algum $g(x_{r+1}, \ldots, x_s)$, com* *conjuntos disjuntos de variáveis das de f, o produto $f \cdot g$ é um polinômio central para $M_{a,b}(E)$. Então existe um i em $\mathbb{Z}_2$ tal que $f(a_1, \ldots, a_r)$ está em A_i para quaisquer $a_1, \ldots, a_r$ em $M_{a,b}(E)$.*

Demonstração. Denote por $\mathcal{B}$ a base canônica de A. Provaremos a existência de polinômios multihomogêneos $f'(x_1, \ldots, x_m)$ em $\langle f \rangle^T$, $g'(x_1, \ldots, x_m)$ em $\langle g \rangle^T$ e de $b_1, \ldots, b_m$ em $\mathcal{B}$ tais que $f'(b_1, \ldots, b_m) \cdot g'(b_1, \ldots, b_m) \neq 0$. Caso contrário o polinômio da forma $f' \cdot g'$ satisfaz a condição (iii) da Proposição 2.1.3 com $V = 0$. Pela arbitrariedade da escolha de tais elementos, podemos aplicar mais um vez a Proposição 2.1.3 e teríamos que $f \cdot g$ é uma identidade para A. Mas isto é uma contradição.

Podemos considerar que os elementos $f'(b_1, \ldots, b_m)$ e $g'(b_1, \ldots, b_m)$ têm a forma mM e rR, onde M e R são matrizes em $M_n(K)$ e, m e r são monômios em E. A Proposição 2.1.5 implica que o produto não nulo $(mM)(rR)$ está em $Z(A)$. Portanto MR é um múltiplo escalar da matriz identidade e consequentemente R é invertível, já que $Z(A) \cong E_0$. Observe que rR é um elemento homogêneo na $\mathbb{Z}_2$-graduação de A, para se convencer disto observe que o elemento r é um monômio em E que tem o mesmo grau de R em suas respectivas $\mathbb{Z}_2$-graduação. Fixe i um elemento de $\mathbb{Z}_2$ tal que $g'(b_1, \ldots, b_m) = rR$ esteja em A_i. Para todo polinômio multihomogêneo $f''(x_{i_1}, \ldots, x_{i_s})$ em $\langle f \rangle^T$ e todo elemento $b_{i_1}, \ldots, b_{i_s}$ em $\mathcal{B}$, podemos escrever $f''(b_{i_1}, \ldots, b_{i_s}) = qQ$, onde q é um monômio em E e Q é uma matriz em $M_n(K)$. Se $qQ = 0$ então é óbvio que ele está em A_i. Agora suponhamos que $qQ \neq 0$, podemos assumir sem perda de generalidade que $qr \neq 0$, pois caso contrário podemos substituir elementos que se repetem em q e r por outros em $\mathcal{B}$ de mesmo grau e distintos. Como R é invertível e $Q \neq 0$ temos que o produto QR é não nulo e assim $(qQ)(rR) \neq 0$. Da Proposição 2.1.5, o produto $f'' \cdot g'$ é um polinômio central para A implicando que $(qQ)(rR)$ pertence a $Z(A) \subseteq A_0$. Considere que qQ está em A_j para algum j em $\mathbb{Z}_2$. Segue que $(qQ)(rR)$ também está em algum A_{j+i} e como $(qQ)(rR) \neq 0$ implicará que $j + i = 0$. Portanto qQ está em A_i. O resultado segue agora aplicando a Proposição 2.1.3 para $V = A_i$. □

Teorema 2.4.3. *Seja K um corpo infinito de característica diferente de 2. A álgebra $M_{a,b}(E)$ satisfaz a propriedade de primalidade para polinômios centrais.*

Demonstração. Sejam f e g polinômios em $K\langle X \rangle$ em conjuntos disjuntos de variáveis tais que o produto $f \cdot g$ seja um polinômio central para $A = M_{a,b}(E)$. Da proposição anterior existe i em $\mathbb{Z}_2$ tal que $f(a_1, \ldots, a_r)$ esteja em A_i para quaisquer $a_1, \ldots, a_r$ em $M_{a,b}(E)$. Das Proposições 2.1.2 e 2.4.2, temos que o comutador $[f(a_1, \ldots, a_r), b]$ estará em A_i, para todo b em A. Se b estiver em A_1 então os produtos $f(a_1, \ldots, a_r) \cdot b$ e $b \cdot f(a_1, \ldots, a_r)$ estarão em A_{i+1}, e consequentemente o comutador $[f(a_1, \ldots, a_r), b]$ também estará em A_{i+1}. Concluímos que $[f(a_1, \ldots, a_r), b]$ estará em $A_i \cap A_{i+1}$, implicando que $[f(a_1, \ldots, a_r), b] = 0$, isto é, $f(a_1, \ldots, a_r)$ comuta com qualquer elemento de A_1.

Resta mostrar que $f(a_1, \ldots, a_r)$ comuta com todos os elementos em A_0. Para este fim é suficiente provar que ele comuta com os elementos da forma $b = e_{i_1} \cdots e_{i_{2k}} E_{ij}$, para $k > 0$ e i, j em $\{1, 2, \ldots, a\}$ ou $\{a+1, a+2, \ldots, a+b\}$. Escolha um $t > a$ tal que $b_1 = e_{i_1} E_{it}$ e $b_2 = e_2 \cdots e_{i_{2k}} E_{ti}$ estejam em A_1. Como $b = b_1 \cdot b_2$ concluímos que $f(a_1, \ldots, a_r)$ comuta com b. Portanto o elemento $f(a_1, \ldots, a_r)$ é central em A, concluindo que f é um polinômio central para A. A prova de que g é um polinômio central segue passos totalmente análogos. Com isso terminamos a demonstração. $\square$

Observação 2.4.4. *Suponha K um corpo de característica zero. Concluímos que todas as álgebras verbalmente primas satisfazem a propriedade de primalidade para polinômios centrais (ordinários). Embora tal resultado já seja conhecido em [31] e [83], aqui demos uma demonstração alternativa.*

2.5 Propriedade de Primalidade para $A\hat{\otimes}R$ em $char K = 0$

Nesta seção iremos considerar K um corpo de característica zero. A seguir faremos um definição mais geral que o Envelope de Grassmann dado na Definição 1.2.26.

Definição 2.5.1 (*G*-**envelope**)**.** *Sejam A, R álgebras graduadas por um grupo G. Denotamos por*

$$A\hat{\otimes}R = \bigoplus_{g \in G} (A_g \otimes R_g)$$

a álgebra com a G-graduação tal que $(A\hat{\otimes}R)_g = A_g \otimes R_g$.

Observamos que a álgebra $M_{a,b}(E)$ é obtida como $M_{a+b}(K)\hat{\otimes}E$, onde $M_{a+b}(K)$ possui a $\mathbb{Z}_2$-graduação induzida pela $(a+b)$-upla $(0, \ldots, 0, 1, \ldots, 1)$ com a (resp. b) entradas iguais a 0 (resp. 1). Mais geralmente, se R possui uma graduação regular então existe uma correspondência entre as identidades graduadas de A e $A\hat{\otimes}R$ (ver [4, 12]).

Definição 2.5.2. *Seja $f(x_{1,g_1}, \ldots, x_{n,g_n})$ um polinômio em $K\langle X_G \rangle$ e escreva $f = \sum \lambda_i m_i$ como combinação linear de monômios G-graduados $m_1, \ldots, m_n$. Denotemos por f^* o polinômio $f^* = \sum \epsilon^R_{m_i} \lambda_i m_i$, onde $\epsilon^R_{m_i}$ é o escalar obtido da Observação 2.3.5.*

Proposição 2.5.3. *[4, Lema 27] Sejam K um corpo de característica zero, A e R álgebras G-graduada com a G-graduação em R sendo regular. Se f é um polinômio multilinear em $K\langle X_G \rangle$ então f é uma identidade graduada para A se, e somente se, f^* é uma identidade graduada para $A\hat{\otimes}R$.*

Observação 2.5.4. *A "operação envelope" na Definição 2.5.1 é involutiva. Mais precisamente, se o grupo G é finito e $\widetilde{R} = \hat{\otimes}^{|G|-1} R$ então $\widetilde{R}$ tem uma G-graduação regular e ainda $Id_G((A\hat{\otimes}R)\hat{\otimes}\widetilde{R}) = Id_G(A)$. Isto foi provado em [4, Teorema 6].*

Neste caso obtemos o seguinte teorema.

Teorema 2.5.5. *Sejam K um corpo de característica zero, A e R álgebras graduadas por um grupo finito G com a G-graduação em R sendo regular. Se os centros das álgebras A e $A\widehat{\otimes}R$ satisfazem $Z(A) \subseteq A_\epsilon$ e $Z(A\widehat{\otimes}R) \subseteq A_\epsilon\widehat{\otimes}R_\epsilon$ então A satisfaz a propriedade de primalidade para polinômios centrais G-graduados se, e somente se, $A\widehat{\otimes}R$ satisfaz a mesma propriedade.*

Demonstração. Sejam $f(x_{1,g_1}, \ldots, x_{r,g_r})$ e $g(x_{r+1,g_{r+1}}, \ldots, x_{s,g_s})$ polinômios em $K\langle X_G\rangle$ que são multilineares e em conjuntos disjuntos de variáveis. Observe que a aplicação linear $f \mapsto f^*$ é invertível no espaço dos polinômios multilineares com um conjunto de variáveis fixadas. Portanto todo polinômio multilinear é da forma h^* para algum h multilinear. Assumimos que a álgebra A satisfaça a propriedade de primalidade para polinômios centrais G-graduados; para provar que $A\widehat{\otimes}R$ também a satisfaz podemos considerar apenas polinômios multilineares, uma vez que a característica do corpo é zero, e portanto é suficiente provar que se $f^* \cdot g^*$ é central para $A\widehat{\otimes}R$ então f^*, g^* também o são. Afirmamos que f é central para A se, e somente se, f^* é central para $A\widehat{\otimes}R$. Assuma que f é um polinômio central para A, então para todo $g \in G$ o comutador $[f, x_g]$ é uma identidade graduada para A. A inclusão $Z(A) \subseteq A_\epsilon$ implica que f possui grau ϵ implicando que $[f, x_g]^* = [f^*, x_g]$. A Proposição 2.5.3 implica que $[f^*, x_g]$ é uma identidade graduada para $A\widehat{\otimes}R$, portanto f^* é um polinômio central graduado para $A\widehat{\otimes}R$. A prova que f é polinômio central graduado para A se f^* é central para $A\widehat{\otimes}R$ é análoga. Como $f^* \cdot g^*$ é central para $A\widehat{\otimes}R$ e $(f \cdot g)^* = f^* \cdot g^*$ concluímos que $f \cdot g$ é central para A. Isto implica que f, g são centrais para A e portanto f^*, g^* também são centrais para $A\widehat{\otimes}R$. Concluímos que $A\widehat{\otimes}R$ herda a propriedade de primalidade de A.

Assumindo agora que $A\widehat{\otimes}R$ satisfaça a propriedade de primalidade, pela Observação 2.5.4 e Lema 2.3.13 podemos concluir pela primeira parte do teorema que A também satisfaz a propriedade. □

Observação 2.5.6. *A hipótese que $Z(A) \subseteq A_\epsilon$ é necessária para provar que f^* é um polinômio central para $A\widehat{\otimes}R$ se f é central para A. No caso geral isso não é válido, por exemplo, podemos considerar A sendo a álgebra comutativa $E\widehat{\otimes}E$, onde E é a álgebra de Grassmann munida de sua $\mathbb{Z}_2$-graduação natural. Qualquer polinômio que não seja identidade para A é um polinômio central, em particular $x_{1,\bar{1}}$ é central. Sabemos que a álgebra $A\widehat{\otimes}E$ satisfaz as mesmas identidades graduadas que E e portanto $x_{1,\bar{1}}^* = x_{1,\bar{1}}$ não é um polinômio central para $A\widehat{\otimes}E$. Analogamente a inclusão $Z(A\widehat{\otimes}R) \subseteq A_\epsilon\widehat{\otimes}R_\epsilon$ também é necessária.*

Observação 2.5.7. *Por contas diretas (ver Observação 2.4.1) observamos que $M_{1,1}(E)$ não satisfaz a propriedade de primalidade, porém temos outra maneira de rever esta conclusão. Do Teorema 2.2.10 temos que $M_2(K)$ munida de sua $\mathbb{Z}_2$-graduação natural* *não satisfaz a propriedade de primalidade, e o resultado anterior implicará que* $M_{1,1}(E)$, *munida de sua* $\mathbb{Z}_2$*-graduação, também não a satisfará.*

Observação 2.5.8. *Assuma que o corpo base seja infinito e de característica diferente de 2. A primeira implicação do Teorema 2.5.5 é válida adicionando a Propriedade 2.3.8. Já para a recíproca, devemos considerar dois monômios em variáveis DISJUNTAS. Mas isso quer dizer que, essencialmente, temos de considerar polinômios multilineares em conjuntos disjuntos de variáveis Então a propriedade é válida para o caso geral mas apenas em polinômios multilineares, como em [83].*

3 Identidades e Polinômios Centrais de Álgebras de Divisão Graduadas Reais

Sejam K um corpo de característica zero e A uma álgebra graduada por um grupo abeliano finito G sobre o corpo K. Di Vincenzo e Nardozza [28] mostraram como se podem obter informações sobre as identidades $G \times \mathbb{Z}_2$-graduadas de $A \otimes_K E$ conhecendo as identidades graduadas da álgebra A. Posteriormente Brandão, Koshlukov e Alves [5] usando algumas técnicas adicionais obtiveram a descrição dos polinômios centrais $G \times \mathbb{Z}_2$-graduados das álgebras anteriores. No entanto, não é fácil obter informações sobre identidades e polinômios centrais $G \times H$-graduados no caso $A \otimes_K R$, com R sendo uma álgebra graduada por um grupo abeliano finito H e tão pouco no caso em que K é um corpo infinito de característica prima.

Neste capítulo iremos considerar R uma álgebra munida de uma graduação regular por um grupo abeliano finito H sobre o corpo K e, como resultado principal, obteremos informações sobre os polinômios centrais $G \times H$-graduados de $A \otimes_K R$ conhecendo polinômios centrais G-graduados de A que contêm uma base de suas identidades G-graduadas, como T_G-espaço. Além disso, Diniz e Castilho [32] conseguiram extrair informações análogas para o $T_{G\times H}$-ideal das identidades graduadas de tais álgebras.

Em artigos recentemente publicados ou submetidos, Bahturin e Zaicev [16], bem como Rodrigo–Escudero [81] classificaram as álgebras de divisão graduadas simples e de dimensão finita sobre o corpo dos números reais. Mais geralmente, a classificação das álgebras de divisão graduadas reais de dimensão finita está sendo estudada por Bahturin e Zaicev (ver [17]). Considerando uma relação entre algumas dessas álgebras graduadas e as álgebras regulares temos como objetivo principal deste capítulo determinar uma base finita para o T_G-ideal das identidades graduadas e do T_G-espaço dos polinômios centrais graduados para as álgebras de divisão graduadas classificadas em [16, 17, 81]. Para obter êxito, devemos aplicar o resultado principal para estas álgebras. Por outro lado, as técnicas que utilizaremos para determinar uma base para as identidades e polinômios centrais graduados nos casos da graduação de Pauli não regular e da álgebra $\mathcal{E}(\epsilon, 2^k)$ serão diferentes. Os resultados foram aceitos para publicação na revista **International Journal of Algebra and Computation** e podem ser encontrados em [34] sendo obtidos em colaboração com Diogo Diniz, UFCG, e Sergio Mota, UESC.

Em todo capítulo, o grupo cíclico de ordem finita igual à s gerado pelo elemento a será denotado por $(a)_s$. Além disso alguns dos resultados apresentados podem ser deduzidos (sem qualquer alteração nas respectivas demonstrações) numa situação mais geral: considerando o corpo apenas infinito. Como alguns dos principais resultados deste capítulo exigem característica 0, nós iremos restringir as considerações no caso de corpos de característica 0.

3.1 Definições e Resultados Preliminares

Sejam G e H grupos cujos elementos neutros denotaremos por ϵ e ϵ_H, respectivamente. Um espaço vetorial V, que possui uma decomposição em soma direta de subespaços $\Gamma\colon V = \oplus_{g\in G} V_g$, é chamado **espaço vetorial graduado pelo grupo** G. Se $\Gamma'\colon V' = \oplus_{h\in H} V'_h$ é outro espaço graduado, então uma transformação linear $\varphi\colon \Gamma \to \Gamma'$ é dita ser **homomorfismo graduado** se para todo $g \in G$, existir um $h \in H$ tal que $\varphi(V_g) \subseteq V'_h$. Se φ for invertível e seu inverso for um homomorfismo graduado, dizemos que Γ e Γ' são **graduações equivalentes**. Uma G-graduação sobre uma álgebra A é uma graduação sobre A como espaço vetorial $\Gamma\colon A = \oplus_{g\in G} A_g$ tal que $A_g A_h \subseteq A_{gh}$ para todo g, h em G.

Definição 3.1.1. *Sejam $\Gamma\colon A = \oplus_{g\in G} A_g$ e $\Gamma'\colon B = \oplus_{h\in H} B_h$ álgebras graduadas por G e H, respectivamente. As álgebras graduadas A e B são ditas **fracamente isomorfas** se existir um isomorfismo de grupos $\alpha\colon G \to H$ e um isomorfismo de álgebras $\varphi\colon A \to B$ tal que $\varphi(A_g) = B_{\alpha(g)}$ para todo g em G.*

Se G e H são os suportes de A e B, respectivamente, e a graduação Γ é forte (isto é, $A_g A_h = A_{gh}$ para todo $g, h \in G$) então as graduações Γ e Γ' são equivalentes se, e somente se, elas são fracamente isomorfas.

Definição 3.1.2. *A álgebra graduada $\Gamma\colon A = \oplus_{g\in G} A_g$ é uma **álgebra de divisão graduada** (ou Γ é uma graduação de divisão sobre A) se A tem unidade e todo elemento homogêneo não nulo em A é invertível.*

Observação 3.1.3. *Considerando a Definição 1.2.17, temos que toda álgebra de divisão graduada possui uma graduação G-produto cruzado. Porém a recíproca não é verdadeira, basta tomar a $\mathbb{Z}_n$-graduação canônica sobre a álgebra das matrizes $M_n(K)$, de ordem $n > 1$, dado no Exemplo 1.2.5.*

Seja G um grupo abeliano finito. Observe, inicialmente, que Γ é uma graduação de divisão se, e somente se, a componente neutra A_ϵ de Γ é um anel de divisão sobre K. Considerando $K = \mathbb{C}$ o corpo dos complexos, temos que qualquer álgebra de divisão G-graduada complexa R é isomorfa à álgebra de grupo torcida $\mathbb{C}^\sigma G$, onde a aplicação $\sigma\colon G \times G \to K^\times$ é um 2-cociclo sobre G, isto é, uma aplicação que satisfaz

$$\sigma(g,h)\sigma(gh,k) = \sigma(g,hk)\sigma(g,k),$$

ver [40, Teorema 2.13]. Neste caso podemos definir $\beta(g,h) := \sigma(g,h)\sigma(h,g)^{-1}$ um bicaracter antissimétrico. Reciprocamente, todo bicaracter antissimétrico é obtido de um 2-cociclo, ver [86, Lema 2]. A álgebra $\mathbb{C}^\sigma G$ é um espaço vetorial complexo de base G munido da multiplicação definida por $g \cdot h := \sigma(g,h)gh$, portanto a terminologia "torcida". A G-graduação canônica nesta álgebra será denotada por $P(\beta)$. Por [40, Teorema 2.15], $\mathbb{C}^\sigma G \cong M_n(\mathbb{C})$ com a graduação de Pauli e $G \cong \mathbb{Z}_{l_1}^2 \times \cdots \times \mathbb{Z}_{l_r}^2$, com $l_1 \cdots l_r = n$. Além disso, a classe dos isomorfismos correspondentes a cada graduação está em correspondência biunívoca com os bicaracteres antissimétricos $\beta\colon G \times G \to \mathbb{C}^\times$.

No caso em que R é uma álgebra G-graduada de divisão complexa simples, temos uma classificação mais geral. O seguinte resultado caracteriza a graduação de divisão em álgebras semisimples sobre um corpo algebricamente fechado de característica qualquer, sem qualquer restrição sobre o grupo G.

Proposição 3.1.4. *[11, Proposição 2] Seja R uma álgebra semisimples de dimensão finita sobre um corpo algebricamente fechado, graduada por um grupo G. Então $R = \oplus_{g\in G} R_g$ é uma álgebra de divisão graduada se, e somente se,* $\operatorname{supp} R$ *é um subgrupo de G e* $\dim R_g = 1$ *para qualquer $g \in$* $\operatorname{supp} R$.

Segue destes cometários que, sobre o corpo dos complexos, o produto tensorial entre duas álgebras de divisão graduadas é de novo uma álgebra de divisão graduada. Isto deixa de ser verdade no caso real. De fato, do Teorema 1.1.24 temos que as únicas álgebras de divisão sobre os reais de dimensão finita são $\mathbb{R}, \mathbb{C}$ ou $\mathbb{H}$. Assim, $D_1 \otimes_{\mathbb{R}} D_2$, onde $D_i = \mathbb{R}, \mathbb{C}$ ou $\mathbb{H}$, é uma álgebra de divisão se, e somente se, pelo menos um dos D_i for $\mathbb{R}$. Se R e S são álgebras de divisão graduadas pelos grupos G e H, respectivamente, temos que $R \otimes_{\mathbb{R}} S$ é uma álgebra de divisão graduada se, e somente se, sua componente neutra for uma álgebra de divisão e de dimensão finita sobre os reais. Isto implica que a componente neutra de R ou S deve ser unidimensional. Sistematizamos esses comentários na observação a seguir.

Observação 3.1.5. *Sejam R e S duas álgebras de divisão graduadas reais de dimensão finita, então $R \otimes_{\mathbb{R}} S$ é uma álgebra de divisão graduada se, e somente se, a componente neutra de R ou S for unidimensional.*

Observação 3.1.6. *Sejam $A = \oplus_{g\in G} A_g$ e $B = \oplus_{h\in H} B_h$ duas álgebras graduadas fracamente isomorfas, então existem $\alpha\colon G \to H$ e $\varphi\colon A \to B$ isomorfismos de grupos e de álgebras, respectivamente, tais que $\varphi(A_g) = B_{\alpha(g)}$ para todo g em G. É claro que um polinômio $f \in K\langle X_G\rangle$ é uma identidade G-graduada para A (respectivamente polinômio central G-graduado) se, e somente se, $\Phi(f)$ é uma identidade H-graduada (respectivamente polinômio central H-graduado) para B, onde $\Phi\colon K\langle X_G\rangle \to K\langle X_H\rangle$ é o isomorfismo tal que $\Phi(x_{ig}) = x_{i\alpha(g)}$. Além disso, se S é uma base para o T_G-ideal $Id_G(A)$ (respectivamente o T_G-espaço $C_G(A)$), então $\Phi(S)$ é uma base para o T_H-ideal $Id_H(B)$ (respectivamente o T_H-espaço $C_H(B)$).*

Além disso, quando $\Gamma\colon A = \oplus_{g\in G} A_g$ é uma álgebra de divisão G-graduada, então o suporte $H = \operatorname{supp}\Gamma$ é um subgrupo de G e $A = \oplus_{h\in H} A_h$ é uma H-graduação sobre A. Se $S \subset K\langle X_H\rangle$ é um base para $Id_H(A)$ (respectivamente $C_H(A)$) então o conjunto $S \cup \{x_{1g} \mid g \in G\backslash H\}$ é uma base para $Id_G(A)$ (respectivamente $C_G(A)$).

De agora em diante, sempre que $\Gamma\colon A = \oplus_{g\in G} A_g$ for uma álgebras de divisão G-graduada, assumiremos que $G = \operatorname{supp}\Gamma$.

3.2 Identidades e Polinômios Centrais Graduados: de A para $A\otimes R$

Sejam R uma álgebra regular, graduada por um grupo abeliano finito H, e A uma álgebra G-graduada. O resultado principal desta seção (Teorema 3.2.7) fornecerá uma base para os polinômios centrais da álgebra $A \otimes_K R$ com sua $G \times H$-graduação canônica, obtida de uma base para os polinômios centrais G-graduados de A que contém uma base para $Id_G(A)$ como T_G-espaço.

Seja $\mathbf{g} = (g_1, \ldots, g_n)$ uma n-upla de elementos do grupo G. Denotemos por $P_{\mathbf{g}}$ o conjunto de todos os polinômios multilineares em variáveis $x_{1,g_1}, \ldots, x_{n,g_n}$. Fixamos uma n-upla $\boldsymbol{h} = (h_1, \ldots, h_n)$ de elementos em H. A descrição das bases para $A \otimes R$ está em termos das aplicações multilineares $\phi_{\boldsymbol{h}}\colon P_{\mathbf{g}} \to P_{\mathbf{g}\times\boldsymbol{h}}$, onde $\mathbf{g} \times \boldsymbol{h} = ((g_1, h_1), \ldots, (g_n, h_n))$ e foram introduzidas no artigo [12]. Uma permutação $\tau \in S_n$, junto com $\boldsymbol{h}$, determina um escalar não nulo $\lambda_\tau^{\boldsymbol{h}}$ em K tal que

$$r_1 \cdots r_n = \lambda_\tau^{\boldsymbol{h}} r_{\tau(1)} \cdots r_{\tau(n)}, \tag{3.1}$$

onde $r_i \in R_{h_i}$ para cada $i = 1, \ldots, n$. Definimos

$$\phi_{\boldsymbol{h}}(x_{g_{\tau(1)},\tau(1)} \cdots x_{g_{\tau(n)},\tau(n)}) = \lambda_\tau^{\boldsymbol{h}} x_{(g_{\tau(1)},h_{\tau(1)}),\tau(1)} \cdots x_{(g_{\tau(n)},h_{\tau(n)}),\tau(n)},$$

e estendemos $\phi_{\boldsymbol{h}}$ para todo $P_{\mathbf{g}}$ por linearidade.

Observação 3.2.1. *Observe que os escalares obtidos em (3.1) representam um caso particular dos escalares da Observação 2.3.5 para $d_1 = \cdots = d_s = 1$.*

Teorema 3.2.2. *[32, Teorema 5.5] Sejam R uma álgebra munida de uma graduação regular por um grupo abeliano H e A uma álgebra G-graduada qualquer. Se $S \subseteq \bigcup_{\substack{\mathbf{g}\in G^n\\ n\in\mathbb{N}}} P_{\mathbf{g}}$ for uma base, de polinômios multilineares, para o T_G-ideal $Id_G(A)$, então o conjunto*

$$\widetilde{S} = \{\phi_{\boldsymbol{h}}(f) \mid f(x_{1g_1}, \ldots, x_{ng_n}) \in S, \boldsymbol{h} \in H^n\},$$

é uma base para o $T_{G\times H}$-ideal $Id_{G\times H}(A \otimes_K R)$.

Nesta seção R terá centro homogêneo minimal no sentido que

$$Z(R) = \bigoplus_{h' \in H'} R_{h'}, \tag{3.2}$$

onde H' denotará o subgrupo de G definido na Igualdade (1.7).

Observação 3.2.3. *Sejam $f(x_{g_1,1}, \ldots, x_{g_n,n})$ um polinômio multilinear e $\boldsymbol{h}$ uma n-upla em H^n. Segue da definição da aplicação $\phi_{\boldsymbol{h}}$ que a igualdade*

$$\phi_{\boldsymbol{h}}(f)(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n) = f(a_1, \ldots, a_n) \otimes_K r_1 \cdots r_n, \tag{3.3}$$

vale para qualquer substituição $\phi_{\boldsymbol{h}}(f)$-admissível $(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n)$. (Ver [12, Teorema 3.1] ou Observação 2.3.7.) Isto implica que $\phi_{\boldsymbol{h}}(f)$ é uma identidade graduada para $A \otimes_K R$ se, e somente se, f é uma identidade graduada para A.

Lema 3.2.4. *Sejam $f(x_{g_1,1}, \ldots, x_{g_n,n})$ um polinômio multilinear em $K\langle X_G \rangle$ e uma n-upla $\boldsymbol{h} = (h_1, \ldots, h_n)$ de elementos em H. Suponha a Igualdade (3.2) válida. Então $\phi_{\boldsymbol{h}}(f)$ é um polinômio central próprio para $A \otimes_K R$ se, e somente se, f é um polinômio central próprio para A e $(h_1 \cdots h_n) \in H'$.*

Demonstração. É claro que se $\phi_{\boldsymbol{h}}(f)$ é um polinômio central próprio para $A \otimes_K R$, então para toda substituição $\phi_{\boldsymbol{h}}(f)$-admissível $(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n)$ o elemento (3.3) pertence ao centro de $A \otimes_K R$. Assim teremos que $f(a_1, \ldots, a_n)$ está em $Z(A)$ e o elemento homogêneo $(r_1 \cdots r_n)$ está em $Z(R)$. Como $\phi_{\boldsymbol{h}}(f)$ é próprio, isso implicará a existência de uma substituição f-admissível $(a_1, \ldots, a_n)$ tal que $f(a_1, \ldots, a_n) \neq 0$. Portanto, f é um polinômio central próprio para A e $(h_1 \cdots h_n) \in H'$. A afirmação reciproca segue imediatamente da Igualdade (3.3). □

Nosso próximo teorema é um resultado análogo ao Teorema 3.2.2 para polinômios centrais graduados. A demonstração deste resultado necessita da utilização do seguinte lema.

Lema 3.2.5. *[32, Lema 5.4] Sejam $f = f(x_{g_1 1}, \ldots, x_{g_m m}) \in P_{\mathbf{g}}$ e $(w_1, \ldots, w_m)$ uma f-substituição admissível de monômios em $K\langle X_G \rangle$ tais que $f(w_1, \ldots, w_m) \in P_{\boldsymbol{k}}$, para algum $\boldsymbol{k} \in G^n$. Se $\boldsymbol{h} \in H^n$, então existem $\boldsymbol{h'} \in H^m$ e elementos homogêneos $b_1, \ldots, b_m$ em $K\langle X_{G \times H} \rangle$ tais que $\phi_{\boldsymbol{h}}(f(w_1, \ldots, w_m)) = \gamma \phi_{\boldsymbol{h'}}(f)(b_1, \ldots, b_m)$.*

Observação 3.2.6. *A m-upla $\boldsymbol{h'}$ do lema anterior é obtida da seguinte forma: para cada i em $\{1, \ldots, m\}$, define-se $b_i = \phi_{\boldsymbol{h}}(w_i)$ e $h'_i = \deg_H(b_i)$ e portanto $\boldsymbol{h'} = (h'_1, \ldots, h'_m)$. Desta forma concluímos que $h'_1 \cdots h'_m = h_1 \cdots h_n$, com $\boldsymbol{h} = (h_1, \ldots, h_n)$ e $n \geqslant m$.*

Estamos prontos para demonstrar o resultado principal desta seção.

Teorema 3.2.7. *Sejam A uma álgebra graduada por um grupo G e R uma álgebra regular graduada por um grupo abeliano H com bicaracter $\beta\colon H \times H \to K^\times$ tal que o centro seja da forma (3.2). Se $S = S_1 \cup S_2 \subseteq \bigcup_{\substack{\mathbf{g}\in G^n \\ n\in\mathbb{N}}} P_{\mathbf{g}}$ é uma base, de polinômios multilineares, para o T_G-espaço $C_G(A)$ tal que S_1 gera $Id_G(A)$ como um T_G-espaço, então o conjunto $\widetilde{S} = \widetilde{S}_1 \cup \widetilde{S}_2$, onde*

$$\widetilde{S}_1 = \{\phi_{\boldsymbol{h}}(f) \mid f(x_{g_1,1}, \dots, x_{g_n,n}) \in S_1, \boldsymbol{h} \in H^n\}$$

e

$$\widetilde{S}_2 = \{\phi_{\boldsymbol{h}}(f) \mid f(x_{g_1,1}, \dots, x_{g_n,n}) \in S_2, \boldsymbol{h} = (h_1, \dots, h_n) \in H^n, h_1 \cdots h_n \in H'\},$$

é uma base para o $T_{G\times H}$-espaço $C_{G\times H}(A \otimes R)$.

Demonstração. A inclusão $\widetilde{S} \subseteq C_{G\times H}(A\otimes R)$ segue da Observação 3.2.3 e do Lema 3.2.4, portanto o $T_{G\times H}$-espaço $\langle \widetilde{S}\rangle^{T_{G\times H}}$ está contido em $C_{G\times H}(A\otimes R)$. Reciprocamente, seja $f(x_{(g_1,h_1),1}, \dots, x_{(g_n,h_n),n})$ um elemento multilinear qualquer em $C_{G\times H}(A\otimes R)$. Denotando $\mathbf{g} = (g_1, \dots, g_n)$ e $\mathbf{k} = ((g_1,h_1), \dots, (g_n,h_n))$ observamos que todo $f \in P_{\mathbf{k}}$ será escrito da forma:

$$f = \sum_{\sigma\in S_n} \alpha_\sigma x_{(g_{\sigma(1)},h_{\sigma(1)})\sigma(1)} \cdots x_{(g_{\sigma(n)},h_{\sigma(n)})\sigma(n)},$$

para alguns $\alpha_\sigma \in K$. Pode-se obter o polinômio

$$f' = \sum_{\sigma\in S_n} (\lambda_\sigma^{\boldsymbol{h}})^{-1} \alpha_\sigma x_{g_{\sigma(1)},\sigma(1)} \cdots x_{g_{\sigma(n)},\sigma(n)},$$

em $P_{\mathbf{g}}$, onde $\lambda_\sigma^{\boldsymbol{h}} \in K^\times$ são coeficientes obtidos a partir da definição de $\phi_{\boldsymbol{h}}$ pela n-upla $\boldsymbol{h} = (h_1, \dots, h_n)$ de elementos em H, com a propriedade de que $\phi_{\boldsymbol{h}}(f') = f$. Do Lema 3.2.4, f' é um polinômio central graduado para A. Portanto existem $p_1, \dots, p_n$ em S, substituições p_i-admissíveis $(w_1^i, \dots, w_{k_i}^i)$ e escalares α_i tais que

$$f' = \sum_{i=1}^n \alpha_i p_i(w_1^i, \dots, w_{k_i}^i). \tag{3.4}$$

Uma vez que f' e os polinômios p_i são multilineares podemos assumir, sem perda de generalidade, que os w_k^i's são também monômios multilineares. O Lema 3.2.5 implica a existência de $\mathbf{h}^i \in H^{k_i}$, substituições $\phi_{\mathbf{h}^i}(p_i)$-admissíveis $(b_1^i, \dots, b_{k_i}^i)$ e escalares $\gamma_i \in K^\times$ tais que

$$\phi_{\mathbf{h}}(p_i(w_1^i, \dots, w_{k_i}^i)) = \gamma_i \phi_{\mathbf{h}^i}(p_i)(b_1^i, \dots, b_{k_i}^i),$$

para todo $i = 1, \dots, n$. Segue da Igualdade anterior e de (3.4) que

$$f = \phi_{\mathbf{h}}(f') = \sum_i \gamma_i' \phi_{\mathbf{h}^i}(p_i)(b_1^i, \dots, b_{k_i}^i), \tag{3.5}$$

onde $\gamma_i' = \alpha_i\gamma_i$. Se f é uma identidade graduada para $A \otimes_K R$ então segue da Observação 3.2.3 que f' é uma identidade graduada para A. Neste caso podemos assumir que os polinômios $p_1, \ldots, p_n$ estão em S_1, e consequentemente os polinômios $\phi_{\mathbf{h}^i}(p_i)$ estão em $\widetilde{S}_1$ (que é um subconjunto de $\widetilde{S}$) e da Igualdade (3.5) temos que f está em $\langle \widetilde{S} \rangle^{T_{G\times H}}$. Agora, vamos supor que f não é uma identidade graduada para $A \otimes_K R$. Como f é multilinear então existe uma substituição f-admissível da forma $(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n)$ de elementos da base de $A \otimes_K R$ tal que $f(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n) \neq 0$. Portanto $f(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n)$ é um elemento central não trivial. A Igualdade (3.3) implica que

$$f(a_1 \otimes_K r_1, \ldots, a_n \otimes_K r_n) = f'(a_1, \ldots, a_n) \otimes_K r_1 \cdots r_n,$$

e assim $r_1 \cdots r_n$ é um elemento central não nulo em R de grau $h_1 \cdots h_n$. Como R satisfaz a igualdade $Z(R) = \bigoplus_{h \in H'} R_h$ concluímos que $h_1 \cdots h_n \in H'$. Além disso, os polinômios $p_1, \ldots, p_n$ estão em S e pela Observação 3.2.6 concluímos que $\phi_{\mathbf{h}^i}(p_i)$ está em $\widetilde{S}$ para todo $i = 1, \ldots, n$. Portanto, segue novamente da Igualdade (3.5) que f pertence ao $\langle \widetilde{S} \rangle^{T_{G\times H}}$. $\square$

Sabemos que $S = S_1 \cup S_2$, onde $S_1 = \{x_1[x_2, x_3]x_4\}$ e $S_2 = \{x_1\}$, forma uma base de polinômios multilineares para o T-espaço $C(K)$ tal que S_1 gera as identidades de K como T-espaço. Considere R uma álgebra com H-graduação regular que satisfaça as hipóteses do teorema anterior. A álgebra $K \otimes_K R$ com sua $\{\epsilon\} \times H$-graduação natural é fracamente isomorfa a R com sua H-graduação. Portanto como consequência do teorema temos o seguinte resultado:

Corolário 3.2.8. *Seja R uma álgebra regular graduada por um grupo abeliano H com bicaracter $\beta\colon H \times H \to K^\times$ tal que o centro seja da forma (3.2). Os polinômios*

$$x_{1h}, h \in H'$$

e

$$x_{1h_1}\left(x_{2h_2}x_{3h_3} - \beta_R(h_2, h_3)x_{3h_3}x_{2h_2}\right)x_{h_4,4}, \text{ onde } h_i \in H, i = 1, \ldots, 4.$$

formam uma base para o T_H-espaço $C_H(R)$.

Observação 3.2.9. *Analogamente, como um corolário do Teorema 3.2.2, concluímos que o conjunto*

$$x_{1,h_1}x_{2,h_2} - \beta(h_1, h_2)x_{2,h_2}x_{1,h_1},$$

onde $h_1, h_2 \in H$, é uma base para as identidades H-graduadas de R.

Observação 3.2.10. *Observe que $S_2 = \{x_1\}$ é uma base para o T-espaço dos polinômios centrais do corpo K, contudo o conjunto de indeterminadas x_{1h}, com $h \in H'$, não gera $C_H(R)$ como T_H-espaço. Portanto, como em [5], a relação entre as bases de $C_G(A)$ e $C_{G\times H}(A \otimes_K R)$ não é imediata.*

As álgebras de divisão graduadas reais simples de dimensão finita, graduadas por um grupo abeliano finito G, foram classificadas em [16, 81]. Nesta seção iremos apresentar o resultado principal descrito em [16] e descreveremos bases para os T_G-ideais das identidades graduadas e do T_G-espaço de polinômios centrais graduadas para cada uma dessas álgebras.

3.2.1 Álgebras de Divisão Graduadas Reais simples

Apresentaremos, inicialmente, as graduações de divisão básicas que serviram de "alicerce" para a elaboração de sua classificação. Um desses elementos é a $\mathbb{Z}_2$-graduação sobre o corpo $\mathbb{C}$ dos números complexos:

$$\Gamma\colon \mathbb{C} = \mathbb{C}_0 \oplus \mathbb{C}_1,$$

onde $\mathbb{C}_0 = \langle 1 \rangle$ e $\mathbb{C}_1 = \langle i \rangle$. Iremos denotar por $\mathbb{C}^{(2)}$ a graduação definida anteriormente sobre $\mathbb{C}$. Os outros elementos para esta classificação são as graduações de divisão nas álgebras $M_2(\mathbb{R})$, $\mathbb{H}$, $M_2(\mathbb{C})$, $M_4(\mathbb{R})$ e $M_n(\mathbb{C})$. Estas são bem conhecidas, mas apesar disso decidimos inclui-las neste texto por motivos de completude da exposição.

(a) **Graduação com Divisão sobre $M_2(\mathbb{R})$:** Seja $G = (a)_2 \times (b)_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Uma graduação de divisão sobre $S = M_2(\mathbb{R})$ pode ser obtida pelas matrizes de Sylvester:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Observe que $A^2 = B^2 = I$, $AB = C = -BA$, portanto uma graduação de divisão por G é obtida pelas componentes homogêneas

$$S_\epsilon = \langle I \rangle,\ S_a = \langle A \rangle,\ S_b = \langle B \rangle,\ S_c = \langle C \rangle,$$

aqui $c = ab$ e I é a matriz identidade. Essa graduação é regular e o centro de $M_2(\mathbb{R})$ é a componente neutra. Denotemos essa graduação por $M_2^{(4)}$. Além disso, a decomposição

$$R_\epsilon = \langle I, C \rangle,\ R_a = \langle A, B \rangle,$$

onde a é o gerador do grupo $H = (a)_2 \cong \mathbb{Z}_2$, é um coarsening de $M_2^{(4)}$ que é também uma graduação de divisão sobre $M_2(\mathbb{R})$. Está última graduação será denotada por $M_2^{(2)}$.

(b) **Graduação com Divisão sobre $\mathbb{H}$:** Seja $\{1, i, j, k\}$ a base canônica da álgebra dos quatérnios $\mathbb{H}$. A multiplicação é determinada pelas relações

$$i^2 = j^2 = -1,\ ij = -ji = k.$$

Como $\mathbb{H}$ é uma álgebra de divisão, então qualquer graduação sobre $\mathbb{H}$ a torna uma álgebra de divisão graduada. Existem, a menos de isomorfismo fraco, duas graduações não triviais sobre $\mathbb{H}$ que iremos descrever a seguir. A graduação pelo grupo $G = (a)_2 \times (b)_2$ é a decomposição

$$R_\epsilon = \langle 1 \rangle,\ R_a = \langle i \rangle,\ R_b = \langle j \rangle,\ R_c = \langle k \rangle$$

onde $c = ab$. Esta graduação é regular e a componente neutra é o centro dos quatérnios. Denotemos esta álgebra de divisão graduada por $\mathbb{H}^{(4)}$. Um coarsening desta graduação é

$$S_\epsilon = \langle 1, i \rangle, S_a = \langle j, k \rangle,$$

e ela é graduada pelo grupo $H = (a)_2 \cong \mathbb{Z}_2$. Denotaremos está última graduação por $\mathbb{H}^{(2)}$.

(c) **Graduação com Divisão sobre** $M_2(\mathbb{C})$**:** Seja $G = (a)_4 \times (b)_2$. Uma G-graduação de divisão sobre $R = M_2(\mathbb{C})$, que denotaremos por $M_2^{(8)}$, é obtida como sendo a álgebra graduada de componentes homogêneas

$$R_\epsilon = \langle I \rangle,\ R_a = \langle \omega A \rangle,\ R_{a^2} = \langle iI \rangle,\ R_{a^3} = \langle i\omega A \rangle$$
$$R_b = \langle C \rangle,\ R_{ab} = \langle \omega B \rangle,\ R_{a^2b} = \langle iC \rangle,\ R_{a^3b} = \langle i\omega B \rangle,$$

onde $w = \dfrac{1}{\sqrt{2}}(1+i)$ é a 8-ésima raiz da unidade tal que $\omega^2 = i$. Esta graduação é regular e seu centro é dado por $R_\epsilon \oplus R_{a^2}$. Outra graduação de divisão sobre $S = M_2(\mathbb{C})$ é a graduação dado pelo grupo $H = (a)_4$ obtida como um coarsening de $M_2^{(8)}$ tendo componentes homogêneas

$$S_\epsilon = \langle I, C \rangle, S_a = \langle \omega A, \omega B \rangle, S_{a^2} = \langle iI, iC \rangle, S_{a^3} = \langle i\omega A, i\omega B \rangle,$$

esta graduação será denotada por $M_2(\mathbb{C}, \mathbb{Z}_4)$.

(d) **Graduação com Divisão sobre** $M_4(\mathbb{R})$**:** Sabemos que $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$ e $M_4(\mathbb{R})$ são isomorfos, para se convencer disso basta tomar o isomorfismo $M_2(\mathbb{R}) \otimes_{\mathbb{R}} M_2(\mathbb{R}) \cong M_4(\mathbb{R})$ com base formada por tensores de matrizes de Sylvester. Da Observação 3.1.5, temos que este isomorfismo transfere a estrutura de álgebra de divisão graduada de $\mathbb{H}^{(4)} \otimes_{\mathbb{R}} \mathbb{H}$ para $M_4(\mathbb{R}) \cong M_2(\mathbb{R}) \otimes_{\mathbb{R}} M_2(\mathbb{R})$. Assim, $R = M_4(\mathbb{R})$ admite uma graduação de divisão pelo grupo $G = (a)_2 \times (b)_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, denotado por $M_4^{(4)}$, cujas componentes homogêneas são as seguintes:

$$\begin{aligned} R_\epsilon &= \langle I \otimes_{\mathbb{R}} I, C \otimes_{\mathbb{R}} I, A \otimes_{\mathbb{R}} C, B \otimes_{\mathbb{R}} C \rangle, \\ R_a &= \langle I \otimes_{\mathbb{R}} C \rangle R_\epsilon, R_b = \langle C \otimes_{\mathbb{R}} A \rangle R_\epsilon, R_c = \langle C \otimes_{\mathbb{R}} B \rangle R_\epsilon, \end{aligned}$$

onde $c = ab$. Desta maneira obtemos que $\mathbb{H}^{(4)} \otimes_{\mathbb{R}} \mathbb{H}$ e $M_4^{(4)}$ são duas álgebras de divisão graduadas e isomorfas (como álgebras graduadas).

(e) **Graduação de Pauli:** Agora, descreveremos as *graduações de Pauli* sobre a álgebra real $R = M_n(\mathbb{C})$. Observe que R é também uma álgebra sobre $\mathbb{C}$ (ver Exemplo 1.2.8). Se a decomposição $\Gamma\colon R = \bigoplus_{g\in G} R_g$ é uma graduação de divisão pelo grupo G para R, como álgebra sobre $\mathbb{C}$, então ele é também uma graduação de divisão para R sobre $\mathbb{R}$. Tais graduações são chamadas de graduações de Pauli. As graduações de divisão Γ são graduações regulares para R como álgebra sobre $\mathbb{C}$ e podem ser descritas em termos do bicaracter associado $\beta\colon G \times G \to \mathbb{C}^\times$. Esta graduação é regular como álgebra real se, e somente se, a imagem de β está em $\mathbb{R}^\times$. Nos referiremos à Γ como uma *graduação de Pauli não regular* se ele não é uma graduação de Pauli regular como álgebra real. Observamos que segue da classificação de tais graduações, dada no Corolário 1.2.13, que Γ é uma graduação de Pauli regular se, e somente se, $G \cong \mathbb{Z}_2^{2k}$ para algum k.

Nossos estudos sobre identidades e polinômios centrais graduados das álgebras de divisão graduadas reais baseiam-se nas classificações feitas nos trabalhos [16, 17, 81]. O principal resultado do artigo [16] é o seguinte.

Teorema 3.2.11. *Qualquer graduação de divisão sobre uma álgebra real simples $M_n(D)$, onde D é uma álgebra de divisão real, é fracamente isomorfa a uma das álgebra dos seguintes tipos:*

$D = \mathbb{R}$: *(i)* $(M_2^{(4)})^{\otimes k}$;

(ii) $M_2^{(2)} \otimes (M_2^{(4)})^{\otimes(k-1)}$, *um coarsening de (i);*

(iii) $M_4^{(4)} \otimes (M_2^{(4)})^{\otimes(k-2)}$, *um coarsening de (i);*

$D = \mathbb{H}$: *(iv)* $\mathbb{H}^{(4)} \otimes (M_2^{(4)})^{\otimes k}$;

(v) $\mathbb{H}^{(2)} \otimes (M_2^{(4)})^{\otimes k}$, *um coarsening de (iv);*

(vi) $\mathbb{H} \otimes (M_2^{(4)})^{\otimes k}$, *um coarsening de (v);*

$D = \mathbb{C}$: *(vii)* $\mathbb{C}^{(2)} \otimes (M_2^{(4)})^{\otimes k}$;

(viii) $\mathbb{C}^{(2)} \otimes M_2^{(2)} \otimes (M_2^{(4)})^{\otimes(k-1)}$, *um coarsening de (vii);*

(ix) $\mathbb{C}^{(2)} \otimes \mathbb{H} \otimes (M_2^{(4)})^{\otimes(k-1)}$, *um coarsening de (vii);*

(x) $M_2^{(8)} \otimes (M_2^{(4)})^{\otimes(k-1)}$;

(xi) $M_2(\mathbb{C}, \mathbb{Z}_4) \otimes (M_2^{(4)})^{\otimes(k-1)}$, *um coarsening de (x);*

(xii) $M_2^{(8)} \otimes M_2^{(2)} \otimes (M_2^{(4)})^{\otimes(k-2)}$, *um coarsening de (x);*

(xiii) $M_2^{(8)} \otimes \mathbb{H} \otimes (M_2^{(4)})^{\otimes(k-2)}$, *um coarsening de (x);*

(xiv) *Graduação de Pauli.*

Nenhuma das graduações de tipos diferentes ou do mesmo tipo mas com valores diferentes de k é fracamente isomorfa a outra.

Observação 3.2.12. *A álgebra do tipo (xii) foi inserida no teorema anterior apenas para fazer o enunciado do teorema similar ao escrito no artigo [17] dos mesmos autores.*

3.2.2 Identidades e Polinômios Centrais Graduados em Álgebras de Divisão Graduadas Reais simples

Nesta subseção iremos descrever bases para as identidades e para os polinômios centrais para cada uma das álgebras listadas no Teorema 3.2.11. As graduações acima consideradas são as: regulares, produto tensorial de uma álgebra apresentada na Seção 3.2.1 com uma álgebra munida de uma graduação regular ou a graduação de Pauli não regular. Para maiores detalhes indicamos a leitura do artigo [14].

3.2.2.1 Graduação com Divisão em Álgebra Regular

Das álgebras apresentadas no Teorema 3.2.11 as que possuem uma graduação regular são (i), (iv), (vii), (x) e a graduação de Pauli regular em (xiv). Da Observação 1.2.24, temos que o produto tensorial entre duas álgebras regulares ainda é regular. Na mesma observação descrevemos um modo de determinar o bicaracter da graduação produto tensorial.

Seja R uma álgebra de divisão graduada real cuja graduação seja regular. Se β_R é o bicaracter correspondente à graduação regular sobre R por um grupo abeliano finito G gerado pelo conjunto $S = \{s_1, \ldots, s_k\}$, então ele é determinado pelo conjunto de valores reais $\beta(s_i, s_j)$, para $1 \leqslant i < j \leqslant k$. Além disso cada $\beta(s_i, s_j)$ é uma raiz da unidade e portanto igual a ± 1. Portanto, β_R é determinado pelo conjunto de pares (s_i, s_j) tal que $\beta(s_i, s_j) = -1$. Tais pares são determinados por simples verificação nas álgebras apresentadas na Seção 3.2.1. Podemos usar então a Observação 1.2.24 para obter o bicaracter para as álgebras (i), (iv), (vii), (x) do Teorema 3.2.11. As álgebras em (i) e (iv) são álgebra graduadas pelo grupo $G_{2k} = (a_1)_2 \times (b_1)_2 \times \cdots \times (a_k)_2 \times (b_k)_2$ e as álgebras em (vii) e (x), respectivamente pelos grupos

$$\begin{aligned} G_{2k+1} &= (a_0)_2 \times (a_1)_2 \times (b_1)_2 \times \cdots \times (a_k)_2 \times (b_k)_2, \\ H_k &= (a_1)_4 \times (b_1)_2 \times (a_2)_2 \times (b_2)_2 \times \cdots \times (a_k)_2 \times (b_k)_2. \end{aligned}$$

Os bicaracteres são apresentados na tabela a seguir:

Álgebra	**Grupo Graduado**	**Bicaracter**
$(M_2^{(4)})^{\otimes k}$, $\mathbb{H}^{(4)} \otimes (M_2^{(4)})^{\otimes(k-1)}$	G_{2k}	$\beta_k(a_i, b_i) = -1,\ i = 1, \ldots, k$
$\mathbb{C}^{(2)} \otimes (M_2^{(4)})^{\otimes k}$	G_{2k+1}	$\gamma_k(a_i, b_i) = -1,\ i = 1, \ldots, k$
$M_2^{(8)} \otimes (M_2^{(4)})^{\otimes(k-1)}$	H_k	$\delta_k(a_i, b_i) = -1,\ i = 1, \ldots, k$

A $\mathbb{Z}_2^2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$-graduação sobre $M_2(\mathbb{C})$, denotada por $M_2^{(4)} \otimes_{\mathbb{R}} \mathbb{C}$, é uma graduação canônica da classe de isomorfismo correspondente a um único bicaracter não degenerado sobre $\mathbb{Z}_2^2$. Mais geralmente, podemos considerar $G = \mathbb{Z}_2^{2k}$, e assim a_i e b_i serão elementos geradores de G para cada i, além disso β é definido como sendo $\beta(a_i, b_i) = -1$. Neste caso, a graduação de Pauli regular sobre $M_n(\mathbb{C})$, para $n = 2^k$, é fracamente isomorfa a $M_2(\mathbb{C})^{\otimes k}$, onde $M_2(\mathbb{C})$ tem a sua graduação de Pauli canônica para algum k. Esta álgebra pode ser canonicamente vista como uma álgebra graduada pelo grupo G_{2k}. Desta maneira seu correspondente bicaracter é β_k, para maiores detalhes ver [40, Exemplo 2.24].

A Observação 3.2.9 descreve uma base para as identidades H-graduadas de uma álgebra regular pelo grupo H. Note que os bicaracteres β_k e δ_k são não degenerados e

$$H' = \{h' \in H \mid \gamma_k(h', h) = 1, \text{ para todo } h \in H\} = (a_0)_2.$$

Portanto, uma base para os polinômios centrais graduados de uma álgebra de divisão graduada real simples cuja graduação seja regular é obtida aplicando o Corolário 3.2.8.

3.2.2.2 Produtos Tensoriais entre Álgebras de Divisão Graduadas

Bases para as identidades e para os polinômios centrais para as álgebras (ii), (iii), (v), (vi), $(viii)$, (ix), (xi), (xii) e $(xiii)$ listadas no Teorema 3.2.11, podem ser obtidas aplicando os Teoremas 3.2.2 e 3.2.7 desde que as bases dos polinômios centrais e identidades graduadas das álgebras $\mathbb{H}$, $\mathbb{H}^{(2)}$, $M_2^{(2)}$ e $M_2(\mathbb{C}, \mathbb{Z}_4)$ sejam conhecidas. Segue dos próximos resultados que são conhecidas tais bases para as álgebras $\mathbb{H}$, $\mathbb{H}^{(2)}$ e $M_2^{(2)}$.

Teorema 3.2.13. *[35] Seja K um corpo de característica zero. O polinômio standard $S_4(x_1, x_2, x_3, x_4)$ e o polinômio de Hall $[[x_1, x_2] \circ [x_3, x_4], x_5]$ formam uma base para o T-ideal das identidades de $M_2(K)$.*

Teorema 3.2.14. *[67] Seja K um corpo de característica zero. Os polinômios*

$$[x_1, x_2][x_3, x_4] + [x_3, x_4][x_1, x_2] \quad e \quad x_5 S_4(x_1, x_2, x_3, x_4)$$

formam uma base para o T-espaço dos polinômios centrais de $M_2(K)$.

Sejam $\theta\colon G \to G'$ um homomorfismo de grupos sobrejetivo e A uma álgebra graduada pelo grupo G. Denote por $\Gamma\colon A = \oplus_{g \in G} A_g$ a G-graduação de A. Podemos obter uma G'-graduação de A chamada de **graduação quociente induzida por** θ, denotada por ${}^{\theta}\Gamma\colon A = \oplus_{g' \in G'} A_{g'}$, cujas componentes homogêneas são dadas por $A_{g'} = \oplus_{g \in \theta^{-1}(g')} A_g$. Listaremos uma sequência de critérios para que as identidades graduadas de duas álgebras graduadas coincidam. Tais resultados foram obtidos em [14].

Proposição 3.2.15. *[14, Lema 1] Sejam A uma álgebra com G-graduação regular com bicaracter correspondente β_A e B uma álgebra G-graduada. Então $Id_G(A) = Id_G(B)$ se, e somente se, a G-graduação sobre B é regular com bicaracter $\beta_B = \beta_A$.*

Proposição 3.2.16. *[14, Proposição 1] Sejam A e B álgebras com G-graduações Γ_A e Γ_B respectivamente, e $\theta\colon G \to G'$ um homomorfismo de grupos. Se $Id_G(\Gamma_A) = Id_G(\Gamma_B)$ então $Id_{G'}({}^\theta\Gamma_A) = Id_{G'}({}^\theta\Gamma_B)$.*

Seja $G = (a)_2 \times (b)_2$ e $G' = (b)_2$. É fácil observar que as álgebras $\mathbb{H}^{(4)}$ e $M_2^{(4)}$ são álgebras regulares, graduadas por um mesmo grupo, e possuem o mesmo bicaracter. Da Proposição 3.2.15, $Id_G(\mathbb{H}^{(4)}) = Id_G(M_2^{(4)})$. Além disso, pela Proposição 3.2.16, $Id_{G'}(\mathbb{H}^{(2)}) = Id_{G'}(M_2^{(2)})$ e, em particular $Id(\mathbb{H}) = Id(M_2(\mathbb{R}))$. Agora, considere M como sendo a álgebra $M_2(\mathbb{R})$ munida da $\mathbb{Z}_2$-graduação natural (ver Exemplo 1.2.5) e o homomorfismo de grupos $\theta\colon G \to G'$ dado por $\theta(a) = \epsilon_{G'}$ e $\theta(b) = b$. Podemos obter M como uma álgebra quociente (induzida por θ) da álgebra R onde suas componentes homogêneas serão

$$R_\epsilon = \langle I\rangle,\ R_a = \langle B\rangle,\ R_b = \langle A\rangle,\ R_c = \langle C\rangle,$$

aqui $c = ab$ e I é a matriz identidade. Observe que a graduação em R é regular com o mesmo bicaracter β da álgebra $M_2^{(4)}$ e segue, das Proposições 3.2.15 e 3.2.16, que $Id_{G'}(M) = Id_{G'}(M_2^{(2)}) = Id_{G'}(\mathbb{H}^{(2)})$. Os próximos resultados descrevem bases para os polinômios centrais e identidades $\mathbb{Z}_2$-graduadas para M.

Lema 3.2.17. *[27, Lema 2] O conjunto consistindo dos polinômios $x_{1,\bar{0}}x_{2,\bar{0}} - x_{2,\bar{0}}x_{1,\bar{0}}$ e $x_{1,\bar{1}}x_{2,\bar{1}}x_{3,\bar{1}} - x_{3,\bar{1}}x_{2,\bar{1}}x_{1,\bar{1}}$ forma uma base para o T_2-ideal das identidades graduadas para $M_2(K)$ munido da $\mathbb{Z}_2$-graduação canônica.*

Teorema 3.2.18. *[20, Teorema 4] O conjunto consistindo dos polinômios*

$$x_{1,\bar{1}}^2,\quad x_{1,g}[x_{2,\bar{0}}, x_{3,\bar{0}}]x_{4,h},\quad x_{1,g}\left(x_{2,\bar{1}}x_{3,\bar{1}}x_{4,\bar{1}} - x_{4,\bar{1}}x_{3,\bar{1}}x_{2,\bar{1}}\right)x_{5,h},$$

onde $g, h \in \mathbb{Z}_2$, gera o T_2-espaço dos polinômios centrais graduados para a álgebra $M_2(K)$ munida da $\mathbb{Z}_2$-graduação canônica.

Observação 3.2.19. *É fato conhecido que o polinômio $x_{1,\bar{1}}^2$ no teorema anterior pode ser substituído pelo polinômio multilinear $x_{1,\bar{1}}x_{2,\bar{1}} + x_{2,\bar{1}}x_{1,\bar{1}}$ obtendo assim uma base de polinômios multilineares.*

Notação 3.2.20. *Seja $q\colon G \to G'$ um homomorfismo de grupos. Seja $f(x_{g_1,1}\dots, x_{g_n,n})$ um polinômio em $K\langle X_G\rangle$, denotamos por $Q(f)$ o polinômio $f(x_{q(g_1),1}\dots, x_{q(g_n),n})$ em $K\langle X_{G'}\rangle$ dado pelo homomorfismo canônico $Q\colon K\langle X_G\rangle \to K\langle X_{G'}\rangle$(a ação deste homomorfismo é dada por $Q(x_{i,g}) = x_{i,q(g)}$).*

Para completar a nossa descrição falta determinar bases para as identidades e polinômios centrais graduados para a álgebra graduada $M_2(\mathbb{C}, \mathbb{Z}_4)$. Usaremos a proposição seguinte para determinar tais bases.

Proposição 3.2.21. *Seja $A = \bigoplus_{g \in G} A_g$ uma álgebra graduada pelo grupo G e assuma a existência de um elemento g em G tal que A_g contém um elemento central invertível. Se $Q\colon K\langle X_G\rangle \to K\langle X_{G/\langle g\rangle}\rangle$ é um homomorfismo tal que $Q(x_{i,g}) = x_{i,q(g)}$, onde $q\colon G \to G/\langle g\rangle$ é o homomorfismo canônico, e S' é uma base de polinômios multilineares para o $T_{G/\langle g\rangle}$-ideal $Id_{G/\langle g\rangle}(A)$ munido da graduação induzida por q, então o conjunto*

$$S = \{f \in K\langle X_G\rangle \mid Q(f) \in S'\}$$

é uma base para o T_G-ideal $Id_G(A)$.

Demonstração. Seja $f(x_{1,g_1}, \ldots, x_{n,g_n})$ um polinômio multilinear em $K\langle X_G\rangle$. Denote por a o elemento central invertível em A_g. Consideremos a aplicação $\varphi_a\colon A_h \to A_{hg}$ dada por $\varphi_a(b) = ba$. Observamos que φ é bijetivo, pois a é invertível, e para todo $b \in A_{hg}$, podemos tomar o elemento $ba^{-1} \in A_h$ tal que $\varphi_a(ba^{-1}) = b$. Concluímos que um elemento homogêneo de grau $q(h)$ pode ser escrito como uma soma de elementos da forma ba^k, onde $b \in A_h$ e algum k inteiro. Uma vez que $Q(f)$ é um polinômio multilinear, então ele é uma identidade graduada para A se, e somente se, nós obtemos zero como resultado para qualquer substituição $Q(f)$-admissível da forma $(b_1a^{k_1}, \ldots, b_na^{k_n})$, onde $k_1, \ldots, k_n$ são inteiros e $(b_1, \ldots, b_n)$ é uma substituição f-admissível. Por a ser central, é claro que

$$Q(f)(b_1a^{k_1}, \ldots, b_na^{k_n}) = a^k f(b_1, \ldots, b_n),$$

onde $k = k_1 + \cdots + k_n$. Portanto, $Q(f)$ é uma identidade graduada para A com a graduação induzida por q se, e somente se, f é uma identidade G-graduada para A. Consequentemente, $S \subseteq Id_G(A)$ e portanto $\langle S\rangle_{T_G} \subseteq Id_G(A)$. Por outro lado, assuma que $f(x_{1,g_1}, \ldots, x_{n,g_n}) \in Id_G(A)$, então podemos escrever $Q(f)$ da forma

$$Q(f) = \sum_{i=1}^{n} u_i s_i'(w_i^1, \ldots, w_i^{k_i})v_i, \tag{3.6}$$

onde $s_i' \in S'$, $u_i, v_i, w_i^1, \ldots, w_i^{k_i} \in K\langle X_{G/\langle g\rangle}\rangle$. Além disso, para cada $x_{\overline{h}}$ em $X_{G/\langle g\rangle}$ fixemos um h no conjunto quociente $\overline{h}$ e consideremos o homomorfismo $R\colon K\langle X_{G/\langle g\rangle}\rangle \to K\langle X_G\rangle$ definido por $R(x_{\overline{h}}) = x_h$, desta maneira, podemos assumir que $R(x_{i,q(g_i)}) = x_{i,g_i}$, para $i = 1, \ldots, n$. Assim $Q \circ R$ é o homomorfismo identidade de $K\langle X_{G/\langle g\rangle}\rangle$ e por

$$f = R \circ Q(f) = \sum_{i=1}^{n} R(u_i)R(s_i')(R(w_i^1), \ldots, R(w_i^{k_i}))R(v_i),$$

temos que $Q(R(s_i')) = s_i'$ implicando que $R(s_i') \in S$. Concluímos que qualquer identidade multilinear G-graduada para A está no T_G-ideal $\langle S\rangle_{T_G}$, isto é, no T_G-ideal gerado por S. Portanto $Id_G(A) \subseteq \langle S\rangle_{T_G}$. □

Observação 3.2.22. *Se assumimos, na proposição anterior, que S' é uma base de polinomios multilineares para o $T_{G/\langle g\rangle}$-espaço $C_{G/\langle g\rangle}(A)$, com a graduação induzida, então uma simples modificação da combinação em (3.6) implicará que S é uma base para o T_G-espaço $C_G(A)$.*

Sejam $G = (a)_4$ e Γ a graduação pelo grupo G sobre $M_2(\mathbb{C})$ que corresponde a $M_2(\mathbb{C}, \mathbb{Z}_4)$. A álgebra $M_2(\mathbb{C}, \mathbb{Z}_4)$ tem um elemento invertível central de grau a^2. As componentes homogêneas da graduação sobre $S = M_2(\mathbb{C})$, induzidas por q, são os subespaços complexos gerados por I e C (a componente de grau ϵ) e o gerado por A e B, respectivamente. É claro que esta álgebra é isomorfa a $M_2^{(2)} \otimes \mathbb{C}$ como álgebras graduadas e portanto satisfaz as mesmas identidades e polinômios centrais de $M_2^{(2)}$. Assim, os resultados anteriores implicam no seguinte corolário.

Corolário 3.2.23. *Sejam $G = (a)_4$ e R a álgebra $M_2(\mathbb{C})$ munida da G-graduação fracamente isomorfa a $M_2(\mathbb{C}, \mathbb{Z}_4)$.*

(i) Uma base para $Id_G(R)$ consiste dos polinômios

$$x_{1k}x_{2k} - x_{2k}x_{1k} \quad e \quad x_{1h}x_{2h}x_{3h} - x_{3h}x_{2h}x_{1h},$$

onde $k \in \{e, a^2\}$ e $h \in \{a, a^3\}$.

(ii) Uma base para $C_G(R)$ consiste dos polinômios

$$x_{1h}x_{2h} + x_{2h}x_{1h}, \quad x_{1g}[x_{2k}, x_{3k}]x_{4g}, \quad x_{1g}\left(x_{2h}x_{3h}x_{4h} - x_{4h}x_{3h}x_{2h}\right)x_{5g},$$

onde $k \in \{e, a^2\}$, $h \in \{a, a^3\}$ e $g \in G$.

3.2.2.3 Graduação de Pauli Não Regular

Seja A a álgebra real $M_n(\mathbb{C})$ munida da graduação de Pauli não regular graduada por um grupo abeliano finito G, com bicaracter complexo $\beta_A \colon G \times G \to \mathbb{C}$. As graduações de divisão complexas sobre $M_n(\mathbb{C})$ foram classificadas em [40, Teorema 2.13] e o seu bicaracter β_A é não degenerado (ver Exemplo 1.2.8).

Observação 3.2.24. *Por definição, f é um polinômio central graduado próprio para A se, e somente se, f não é uma identidade graduada e $\deg_G(f) = e$. Portanto se S é uma base para $Id_G(A)$ então $\{x_{1e}\} \cup S'$ é uma base para $C_G(A)$, onde S' é o conjunto dos polinômios $x_{ig} f x_{jh}$ com $f \in S$, g, $h \in G$ e i, j de modo que x_{ig} e x_{jh} são variáveis que não aparecem em f.*

Segue da Observação anterior que para determinar uma base para o T_G-espaço graduado $C_G(A)$, é suficiente obter uma base para $Id_G(A)$. Dada $\mathbf{g} = (g_1, \ldots, g_n)$ uma n-upla de elementos de G e uma permutação σ em S_n, é possível determinar $\gamma_\sigma^{\mathbf{g}}$ um número complexo não nulo tal que

$$a_1 \cdots a_n = \gamma_\sigma^{\mathbf{g}} a_{\sigma(1)} \cdots a_{\sigma(n)},$$

para quaisquer elementos $a_1 \in A_{g_1}, \ldots, a_n \in A_{g_n}$. Se $\gamma_\sigma^{\mathbf{g}}$ for um número real então

$$x_{i_1,g_1} \cdots x_{i_n,g_n} - \gamma_\sigma^{\mathbf{g}} x_{i_{\sigma(1)},g_{\sigma(1)}} \cdots x_{i_{\sigma(n)},g_{\sigma(n)}}, \tag{3.7}$$

é uma identidade graduada de A para qualquer n-upla $(i_1, \dots, i_n)$ de índices. Se σ, τ são permutações em S_n tais que $\gamma_\sigma^{\mathbf{g}}, \gamma_\tau^{\mathbf{g}} \in \mathbb{C}\backslash\mathbb{R}$ são linearmente independentes sobre $\mathbb{R}$ então existem números p, $q \in \mathbb{R}$ para os quais $p(\gamma_\sigma^{\mathbf{g}})^{-1} + q(\gamma_\tau^{\mathbf{g}})^{-1} + 1 = 0$. Isso implica que o polinômio

$$x_{i_1,g_1} \cdots x_{i_n,g_n} + p x_{i_{\sigma(1)},g_{\sigma(1)}} \cdots x_{i_{\sigma(n)},g_{\sigma(n)}} + q x_{i_{\tau(1)},g_{\tau(1)}} \cdots x_{i_{\tau(n)},g_{\tau(n)}} \tag{3.8}$$

é uma identidade graduada de A para qualquer n-upla $(i_1, \dots, i_n)$ de índices.

Proposição 3.2.25. *Toda identidade graduada para A pode ser escrita como uma combinação linear das identidades polinomiais graduadas (3.7) e (3.8).*

Demonstração. Seja f uma identidade graduada de A. Podemos assumir que o polinômio graduado f é multilinear e escrito da forma $f = \sum_{\sigma \in S_n} \mu_\sigma m_\sigma$, onde μ_σ são escalares reais e $m_\sigma = x_{i_{\sigma(1)},g_{\sigma(1)}} \cdots x_{i_{\sigma(n)},g_{\sigma(n)}}$, para cada $\sigma \in S_n$. Denotemos $\mathbf{g} = (g_1, \dots, g_n)$ e assumimos, sem perda de generalidade, que $\mu_{id} = 1$. Definiremos por "s" a quantidade de escalares não nulos μ_σ. O resultado será provado por indução sobre s.

Como monômios em $K\langle X_G \rangle$ não são identidades graduadas para A teremos que $s > 1$. Se $s = 2$ então f é da forma (3.7). Se $\gamma_\sigma^{\mathbf{g}} \in \mathbb{R}$ para algum $\sigma \in S_n$ tal que $\mu_\sigma \neq 0$ então podemos considerar o polinômio

$$f - \left(x_{i_1,g_1} \cdots x_{i_n,g_n} - \gamma_\sigma^{\mathbf{g}} x_{i_{\sigma(1)},g_{\sigma(1)}} \cdots x_{i_{\sigma(n)},g_{\sigma(n)}}\right).$$

Ele é uma identidade graduada para A com $s-1$ ou $s-2$ escalares não nulos, portanto o resultado segue pela hipótese de indução. Caso $\gamma_\sigma^{\mathbf{g}} \in \mathbb{C}\backslash\mathbb{R}$ para todo $\sigma \in S_n$ tal que $\mu_\sigma \neq 0$ então $s > 2$. Sejam σ, $\tau \in S_n$ tais que μ_σ e μ_τ sejam escalares reais não nulos. Se $\gamma_\sigma^{\mathbf{g}}$ e $\gamma_\tau^{\mathbf{g}}$ forem linearmente dependentes sobre $\mathbb{R}$ então existirá $p \in \mathbb{R}$ tal que $m_\sigma - p m_\tau$ seja uma identidade graduada para A da forma (3.7). Neste caso aplicaremos a hipótese de indução para

$$f - \mu_\sigma (m_\sigma - p m_\tau)$$

e o resultado segue. Por fim, Se $\gamma_\sigma^{\mathbf{g}}$ e $\gamma_\tau^{\mathbf{g}}$ forem linearmente independentes sobre $\mathbb{R}$ existirão escalares $p, q \in \mathbb{R}$ não nulos com a propriedade que $p(\gamma_\sigma^{\mathbf{g}})^{-1} + q(\gamma_\tau^{\mathbf{g}})^{-1} + 1 = 0$ e o resultado segue aplicando a hipótese de indução ao polinômio

$$f - \left(x_{i_1,g_1} \cdots x_{i_n,g_n} + p x_{i_{\sigma(1)},g_{\sigma(1)}} \cdots x_{i_{\sigma(n)},g_{\sigma(n)}} + q x_{i_{\tau(1)},g_{\tau(1)}} \cdots x_{i_{\tau(n)},g_{\tau(n)}}\right).$$

Desta forma a proposição está demonstrada. □

Por [2, 91], o T_G-ideal $Id_G(A)$ admite uma base finita de identidades quando o corpo base é de característica 0. Portanto existe um conjunto finito de polinômios da forma

(3.7) e (3.8) que gera $Id_G(A)$ como T_G-ideal. Nosso objetivo agora é exibir de maneira explícita tal conjunto finito de identidades. Sejam g, $h \in G$, se $\beta_A(g,h) \in \mathbb{R}$ então

$$x_{1,g}x_{2,h} - \beta_A(g,h)x_{2,h}x_{1,g}, \tag{3.9}$$

é uma identidade graduada para A do tipo (3.7). Se $\beta_A(g,h) \in \mathbb{C}\backslash\mathbb{R}$ então podemos considerar $p, q \in \mathbb{R}$ tais que $\beta_A(g,h)$ seja raiz da equação quadrática $z^2 + pz + q$. Neste caso,

$$x_{1,g}x_{2,g}x_{3,h} + p(x_{1,g}x_{3,h}x_{2,g}) + q(x_{3,h}x_{1,g}x_{2,g}), \tag{3.10}$$

é uma identidade graduada para A do tipo (3.8).

Lema 3.2.26. *Sejam $f(x_{1,g_1}, \ldots, x_{n,g_n})$ um polinômio multilinear em $K\langle X_G\rangle$ e A uma álgebra com a graduação de Pauli não regular tal que $\beta_A(g,h) \neq i$, para quaisquer $g, h \in G$. Suponha f uma identidade graduada para A. Então existe um polinômio multilinear $f'(x_{1,g'_1}, \ldots, x_{m,g'_m})$ em $Id_G(A)$, onde $g'_1, \ldots, g'_m$ são elementos distintos de G, tais que f está no T_G-ideal gerado por f' junto com os polinômios (3.9) e (3.10).*

Demonstração. Demonstraremos o lema por indução sobre a quantidade n de indeterminadas. No caso em que $n = 2$ a afirmação é óbvia pela identidade (3.9). Se $g_1, \ldots, g_n$ são elementos de G distintos não há o que fazer. Caso contrário, existem índices $i < j$ tais que $g_i = g_j$. Desta maneira, renomeando as variáveis se necessário, podemos assumir que $i = n-1$ e $j = n$. Seja m um monômio em f, afirmamos que existe um polinômio multilinear $f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, x_{n-1,g'})$ com $g' = g_n^2$, tal que

$$m - f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, (x_{n-1,g_{n-1}} \cdot x_{n,g_n}))$$

está no T_G-ideal gerado por (3.9) e (3.10), uma vez que cada componente homogênea da graduação é unidimensional. Sejam w_1, w_2 e w_3 monômios tais que

$$m = w_1x_{n-1,g}w_2x_{n,g}w_3,$$

onde $g = g_{n-1} = g_n$. Denote por h o grau do monômio w_2. Se $\beta_A(g,h) \in \mathbb{R}$ então

$$w_1x_{n-1,g}w_2x_{n,g}w_3 - \beta_A(g,h)w_1w_2x_{n-1,g}x_{n,g}w_3$$

é uma consequência de um polinômio do tipo (3.9), neste caso $f_m = \beta_A(g,h)w_1w_2x_{n-1,g'}w_3$.

Se, por outro lado, $\beta_A(g,h) \in \mathbb{C}\backslash\mathbb{R}$ tomaremos p, q números reais tais que $\beta_A(g,h)$ é uma raiz da equação quadrática $z^2 + pz + q$ e como $\beta_A(g,h)$ é uma raiz da unidade distinta do complexo $i = \sqrt{-1}$ então $p \neq 0$. Neste caso, podemos considerar

$$f_m = \lambda_1w_1x_{n-1,g'}w_2w_3 + \lambda_2w_1w_2x_{n-1,g'}w_3,$$

onde $\lambda_1 = -\dfrac{1}{p}$, $\lambda_2 = -\dfrac{q}{p}$. Claramente

$$m - f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, (x_{n-1,g} \cdot x_{n,g}))$$

é uma consequência de (3.10) e isto prova a afirmação. Agora escreva $f = \sum_i \lambda_i m_i$, onde m_i são monômios e $\widehat{f} = \sum_i \lambda_i f_{m_i}$. A diferença

$$f(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, x_{n-1,g_{n-1}}, x_{n,g_n}) - \widehat{f}(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, (x_{n-1,g_{n-1}} \cdot x_{n,g_n}))$$

está no T_G-ideal gerado por (3.9) e (3.10). Concluímos que

$$\widehat{f}(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, (x_{n-1,g_{n-1}} \cdot x_{n,g_n}))$$

é uma identidade graduada para A. Uma vez que A possui uma graduação de Pauli teremos que cada componente homogênea é unidimensional e assim o polinômio multilinear $\widehat{f}$ é uma identidade graduada para A com menos de n indeterminadas. Pela hipótese de indução, existe uma identidade graduada $f'(x_{1,g'_1}, \ldots, x_{m,g'_m})$, onde $g'_1, \ldots, g'_m$ são todos distintos, com a propriedade de que $\widehat{f}$ está no T_G-ideal gerado por f' junto com as identidades (3.9) e (3.10). É claro que f também estará neste T_G-ideal. □

Teorema 3.2.27. *Seja A uma álgebra com uma graduação de Pauli não regular tal que para quaisquer g, $h \in G$ temos $\beta_A(g, h) \neq i$. O conjunto S dos polinômios (3.9) e (3.10) junto com os polinômios (3.7) e (3.8), onde $g_1, \ldots, g_n$ são elementos distintos de G, forma uma base para $Id_G(A)$.*

Demonstração. É claro que $S \subseteq Id_G(A)$, e consequentemente $\langle S\rangle_{T_G} \subseteq Id_G(A)$. A inclusão oposta é obtida aplicando o Lema 3.2.26 e a Proposição 3.2.25. □

Resta analisar o caso em que $\beta_A(g, h) = i$ para alguns $g, h \in G$. É claro que neste caso o polinômio

$$x_{1,g}x_{2,h}x_{3,g} - x_{3,g}x_{2,h}x_{1,g}, \tag{3.11}$$

é uma identidade graduada para A.

Observação 3.2.28. *O polinômio (3.11) é também uma identidade para A no caso em que $\beta_A(g, h) \neq i$. Neste caso ele é obtido como uma consequência das identidades (3.9) e (3.10).*

Sejam g, h_1, h_2, h_3 elementos de G tais que $\beta_A(g, h_s) = i$, para $s = 1, 2, 3$. O polinômio

$$x_{1,g}x_{2,h_1}x_{3,g}x_{4,h_2}x_{5,g}x_{6,h_3}x_{7,g} + x_{1,g}x_{3,g}x_{5,g}x_{7,g}x_{2,h_1}x_{4,h_2}x_{6,h_3} \tag{3.12}$$

é uma identidade graduada para A.

Lema 3.2.29. *Sejam A uma álgebra munida da graduação de Pauli não regular por um grupo G e $f(x_{1,g_1}, \ldots, x_{n,g_n})$ um polinômio multilinear. Se f é uma identidade graduada para A então existe um polinômio multilinear $f'(x_{1,g'_1}, \ldots, x_{m,g'_m})$ em $Id_G(A)$, onde para cada $g \in G$ o número de índices j tais que $g'_j = g$ é no máximo 3, e ainda f está no T_G-ideal gerado por f' junto com os polinômios (3.9), (3.10), (3.11) e (3.12).*

Demonstração. A demonstração segue passos análogos ao que foi feito na demonstração do Lema 3.2.26. Se g_1, ..., g_n são elementos de G de modo que o número de índices i com $g_i = g$ é no máximo 3 então não há o que fazer. Caso contrário existem índices $i < j < k < l$ tais que $g_i = g_j = g_k = g_l$. Denotaremos por g este elemento. Seja m um monômio em f e considere w_i, $i = 0, 1, 2, 3, 4$, monômios satisfazendo a propriedade

$$m = w_0 x_{i,g} w_1 x_{j,g} w_2 x_{k,g} w_3 x_{l,g} w_4. \tag{3.13}$$

Denote por h_i o grau do monômio w_i. Renomeando as variáveis se necessário, podemos assumir sem perda de generalidade que $\{n, n-1, n-2, n-3\} = \{i, j, k, l\}$. Se $\beta_A(g, h_1) \neq i$ usaremos a identidade (3.11) para assumir que $i = n-1$ e $j = n$. Então, como na demonstração do Lema 3.2.26, é possível determinar um polinômio $f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, x_{n-1,g^2})$ tal que

$$m - f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, (x_{n-1,g_{n-1}} \cdot x_{n,g_n})) \tag{3.14}$$

está no T_G-ideal gerado por (3.9) e (3.10).

Analogamente, caso $\beta_A(g, h_j) \neq i$ para $j = 2$ ou $j = 3$ podemos obter um polinômio multilinear $f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, x_{n-1,g^2})$ tal que m esteja no T_G-ideal gerado por f_m e os polinômios (3.9), (3.10) e (3.11). Finalmente, assuma que $\beta_A(g, h_j) = i$ para todo $j = 1, 2, 3$, neste caso considere

$$f_m(x_{1,g_1}, \ldots, x_{n-2,g_{n-2}}, x_{n-1,g^2}) = -w_0 x_{n-3,g} x_{n-2,g} x_{n-1,g^2} w_1 w_2 w_3 w_4.$$

É claro que a diferença em (3.14), para este polinômio, está no T_G-ideal gerado pelos polinômios (3.11) e (3.12).

Agora escrevemos $f = \sum_i \lambda_i m_i$, onde m_i são monômios e $\widehat{f} = \sum_i \lambda_i f_{m_i}$. O polinômio multilinear $\widehat{f}$ é uma identidade para A em $n-1$ indeterminadas e o resultado segue por indução sobre n. $\square$

A prova do Teorema 3.2.27 produz junto com o Lema 3.2.29 (em vez de Lema 3.2.26) o seguinte resultado.

Teorema 3.2.30. *Seja A uma álgebra munida de uma graduação de Pauli não regular. O conjunto S dos polinômios (3.12) junto com os polinômios (3.7) e (3.8) tais que para qualquer $g \in G$ o número de índices j com $g_j = g$ é no máximo 3, forma uma base para $Id_G(A)$ como T_G-ideal.*

3.3 Bases para as Identidades e Polinômios Centrais Graduados para Álgebras de Divisão Graduadas Reais

Nesta seção iremos descrever bases para as identidades e para os polinômios centrais graduadas para álgebras de divisão graduadas reais, classificadas em [17]. A nossa descrição será dada em termos de 5 classes das álgebras de divisão graduadas que serão denominadas "graduações básicas" e serão apresentadas a seguir.

3.3.1 Álgebras de Divisão Graduadas Reais

Seja G um grupo abeliano finito. É fato conhecido que toda álgebra de divisão G-graduada complexa R é isomorfa à álgebra de grupo torcida $\mathbb{C}^\sigma G$ e a classe dos isomorfismos correspondentes a cada graduação está em correspondência biunívoca com os bicaracteres antissimétricos $\beta\colon G \times G \to \mathbb{C}^\times$ (rever comentários antes da Proposição 3.1.4). A G-graduação canônica nesta álgebra será denotada por $P(\beta)$.

No caso de álgebras de divisão graduadas reais, a situação é diferente. Listaremos a seguir alguns casos que vão servir de fundamento para a classificação geral.

(a) **Comutativo:** Sejam m um número natural maior do que 1 e $\varepsilon \in \{1, -1\}$. Denotaremos por $\mathcal{D}(m, \varepsilon)$ a subálgebra real da álgebra complexa de grupo $\mathbb{C}(g)_m$ (do grupo cíclico de ordem m) gerada por μg, onde $\mu^m = \varepsilon$. Esta é uma álgebra de divisão que é $(g)_m$-graduada, comutativa e regular. É fácil verificar que $\mathcal{D}(m, \varepsilon)$ pode ser vista como uma álgebra real graduada gerada por um elemento x de grau g, definido com a relação $x^m = \varepsilon$. Observamos que $\mathcal{D}(2, -1)$ é fracamente isomorfa a $\mathbb{C}^{(2)}$.

(b) **Componente neutra de dimensão 1:** Uma álgebra de divisão graduada R com $\dim R_\epsilon = 1$, cujo suporte é o produto direto de dois grupos cíclicos $G = (g)_k \times (h)_l$, pode ser descrita como uma subálgebra da álgebra $S = \mathbb{R}G \otimes M_2(\mathbb{C})$ definida da seguinte forma. Sejam μ, $\nu \in \{1, -1\}$, fixaremos números complexos ε, η tais que $\varepsilon^k = \mu$, $\eta^l = \nu$ e denotaremos por $\mathrm{D}(k, l; \mu, \nu)$ a subálgebra de S gerada por $u = g \otimes \epsilon A$ e $v = h \otimes \eta B$. Aqui $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ são as matrizes de Sylvester introduzidas na Seção 3.2.1. A álgebra S possui uma graduação canônica dada pelas componentes homogêneas $S_g = (\mathbb{R}g) \otimes M_2(\mathbb{C})$. É claro que $\mathcal{D}(k, l; \mu, \nu)$ é uma álgebra de divisão graduada real. Além disso, $uv = -vu$ e o conjunto de elementos $u^i v^j = g^i h^j \otimes \varepsilon^i \eta^j A^i B^j$, onde $0 \leqslant i < k, 0 \leqslant j < l$, forma uma base de elementos homogêneos para $\mathcal{D}(k, l; \mu, \nu)$. Portanto $\mathcal{D}(k, l; \mu, \nu)$ é uma graduação regular. Além disso, observamos que $\mathcal{D}(2, 2, 1, 1)$ e $\mathcal{D}(2, 2, -1, -1)$ são fracamente isomorfas a $M_2^{(4)}$ e $\mathbb{H}^{(4)}$, respectivamente.

(c) **Componente neutra de dimensão 2 comutativa:** Seja $R = \oplus_{g \in G} R_g$ uma álgebra de divisão real tal que $R_\epsilon \cong \mathbb{C}$, então podemos considerar R como uma álgebra de divisão graduada complexa. A classificação de tais álgebras foi dada por comentários iniciais desta seção. Podemos denotar a respectiva graduação complexa por $P(\beta)$. Logo, denotaremos a graduação de tal álgebra real por $P(\beta)_\mathbb{R}$. Esta é a *graduação de Pauli*.

(d) **Componente neutra de dimensão 2 não comutativa:** Sejam n um número natural e $\varepsilon \in \{1, -1\}$. Denotaremos por $\mathcal{E}(n, \varepsilon)$ a subálgebra de $\mathbb{R}(g)_n \otimes M_2(\mathbb{C})$ gerada por $u = 1 \otimes C$ e $v = g \otimes \varepsilon A$. Aqui A, B e C são as matrizes de Sylvester e $C = AB$.

(e) **Componente neutra de dimensão 4:** Seja $R = \oplus_{g \in G} R_g$ uma álgebra de divisão real tal que $R_\epsilon \cong \mathbb{H}$. Pode-se verificar que $R \cong \mathbb{H} \otimes C$, onde $C = \oplus_{g \in G} C_g$ é uma subálgebra de divisão graduada com C_g sendo o centralizador de R_ϵ, para cada R_g de dimensão 1. Note que nos itens (a) e (b) foram dados exemplos de álgebras de divisão graduadas cujas componentes homogêneas são de dimensão 1.

Observação 3.3.1. *Não estamos preocupados com a construção das álgebras citadas anteriormente, e sim, em suas caracterizações (para maiores detalhes ver [17]).*

Teorema 3.3.2. *[17, Teorema 9.1] Seja $\Gamma : R = \oplus_{g \in G} R_g$ uma graduação de uma álgebra de divisão graduada real de dimensão finita R com $G = \operatorname{supp} \Gamma$. Então uma das seguintes alternativas é verdadeira.*

(i) Se R é comutativa com $\dim\, R_\epsilon = 1$ então Γ é equivalente ao produto tensorial graduado de álgebras do tipo $\mathcal{D}(m; \eta)$.

(ii) Se R é não comutativa com $\dim R_\epsilon = 1$ então Γ é equivalente ao produto tensorial graduado de algumas copias de $\mathcal{D}(2^k, 2^l; \mu, \nu)$ e de $\mathcal{D}(m; \eta)$, onde m, k, l são números naturais com $m > 1$ e μ, ν, $\eta = \pm 1$.

(iii) Se $\dim\, R_\epsilon = 4$ então Γ é isomorfo ao produto tensorial graduado de $\mathbb{H}$ com a graduação trivial, algumas copias de $\mathcal{D}(2^k, 2^l; \mu, \nu)$ e algumas copias de $\mathcal{D}(m; \eta)$, onde k, l, m são números naturais com $m > 1$ e μ, ν, $\eta = \pm 1$.

(iv) Se $\dim R_\epsilon = 2$ e R_ϵ não é central então Γ é equivalente ao produto tensorial graduado de uma álgebra do tipo $\mathcal{E}(n, \varepsilon)$, algumas copias de $\mathcal{D}(2^k, 2^l; \mu, \nu)$ e algumas copias de graduações do tipo $\mathcal{D}(m; \eta)$ onde m, k, l são números naturais com $m > 1$, n é uma potência de 2, e ε, μ, ν, $\eta = \pm 1$.

(v) Se $\dim\, R_\epsilon = 2$ e R_ϵ é central então Γ é isomorfo à $P(\beta)_\mathbb{R}$ para algum bicaracter antissimétrico complexo $\beta \colon G \times G \to \mathbb{C}^\times$.

3.3.2 Bases para as Identidades e Polinômios Centrais Graduados

As álgebras em (i) e (ii) possuem uma graduação regular, e assim as bases para os polinômios centrais e para as identidades graduadas foram descritas no Corolário 3.2.8 e na Observação 3.2.9, respectivamente. Já as álgebras do tipo (iii) são produto tensorial graduado de $\mathbb{H}$, munido da graduação trivial, e uma álgebra regular, graduada por um grupo abeliano. Neste caso as bases foram obtidas na Seção 3.2.2.2. As álgebras do tipo (v) possuem graduação de Pauli não regular cujas bases foram descritas na Seção 3.2.2.3.

Portanto, resta determinar as bases dos polinômios centrais e das identidades graduadas para as álgebras do tipo (iv). Pelos Teoremas 3.2.2 e 3.2.7 é necessário considerar apenas as álgebras $\mathcal{E}(\varepsilon, 2^k)$.

Proposição 3.3.3. *Sejam $G = (g)_n$ um grupo cíclico de ordem n, onde $n = 2^k$ para algum k, $H = \langle g^2 \rangle$ e $q\colon G \to G/H$ o homomorfismo canônico de grupos. Se f é um polinômio multilinear em $K\langle X_{G/H} \rangle$ então f é uma identidade graduada (resp. polinômio central graduado) para $\mathcal{E}(\varepsilon, n)$, munido da graduação induzida por q se, e somente se, f é uma identidade graduada (resp. polinômio central graduado) para $M_2(\mathbb{R})$ com a G/H-graduação fracamente isomorfa a $M_2^{(2)}$.*

Demonstração. O elemento $w = g \otimes \varepsilon I$ é um elemento central invertível em $\mathbb{R}(g)_n \otimes M_2(\mathbb{C})$. Seja $R = \mathcal{E}(\varepsilon, n)$ munido da graduação induzida por q e denote por $G' = \{\epsilon, a\}$ o grupo G/H. O conjunto

$$\mathcal{B} = \{w^{2m}(1 \otimes I), w^{2m}(1 \otimes C), w^{2m-1}(1 \otimes A), w^{2m-1}(1 \otimes B) \mid m = 0, 1, \ldots, 2^{k-1}\}$$

é uma base para R de elementos G-homogêneos.

Observe inicialmente que $v = w(1 \otimes A)$ e u são elemento em $\mathcal{B}$, implicando que $R \subseteq \langle \mathcal{B} \rangle_K$ (subálgebra homogênea gerada por $\mathcal{B}$). Além disso $w^{-1} = g^{n-1} \otimes \varepsilon I \in \mathcal{B}$ e $w^2 = g^2 \otimes I = v^2$. Aplicando uma indução sobre m, temos que $\mathcal{B} \subseteq R$. Resta mostrar que os elementos em $\mathcal{B}$ são linearmente independentes. Mas os conjuntos $\{w^{2m}(1 \otimes I), w^{2m}(1 \otimes C)\}$ e $\{w^{2n}(1 \otimes I), w^{2n}(1 \otimes C)\}$ (resp. $\{w^{2m-1}(1 \otimes A), w^{2m-1}(1 \otimes B)\}$ e $\{w^{2n-1}(1 \otimes A), w^{2n-1}(1 \otimes B)\}$) estão na mesma componente homogênea se, e somente se, $m = n$. Além disso, w^{2m} e w^{2m-1} possuem graus distintos.

Consequentemente, é suficiente mostrar que $w^{2m}(1 \otimes I), w^{2m}(1 \otimes C)$ são linearmente independentes entre si, para cada m escolhido. Mas isto segue do fato de w ser invertível e A, B e C serem as matrizes de Sylvester. O caso $w^{2m-1}(1 \otimes A), w^{2m-1}(1 \otimes B)$ é análogo.

Seja $f(x_{1g'_1}, \ldots, x_{ng'_n})$ um polinômio multilinear em $K\langle X_{G'} \rangle$. Este polinômio é uma identidade graduada para R se, e somente se, o resultado de qualquer substituição f-admissível de elementos em $\mathcal{B}$ é zero. Seja $(a_1, \ldots, a_n)$ uma substituição f-admissível de elementos em $\mathcal{B}$, então $a_i = w^{p_i}(1 \otimes b_i)$, onde $b_i \in \{I, A, B, C\}$ e p_i um número natural. Neste caso $(b_1, \ldots, b_n)$ é uma substituição admissível de elementos homogêneos da base de $M_2(\mathbb{R})$ na G'-graduação fracamente isomorfa a $M_2^{(2)}$, ver item (a) da Seção 3.2.1. Segue que $f(a_1, \ldots, a_n) = w^p(1 \otimes f(b_1, \ldots, b_n))$, onde $p = p_1 + \cdots + p_n$. Como w é um elemento central invertível, podemos concluir que f é uma identidade graduada (resp. polinômio central graduado) para R se, e somente se, ele é uma identidade graduada (resp. polinômio central graduado) para $M_2(\mathbb{R})$ munida com G'-graduação fracamente isomorfa à $M_2^{(2)}$. $\square$

Seja $v = g \otimes \varepsilon A$, o elemento $v^2 = g^2 \otimes \epsilon^2 I$ é homogêneo central invertível de grau g^2. Portanto a proposição anterior junto com a Proposição 3.2.21, Lema 3.2.17 e Teorema 3.2.18 implicará na demonstração do seguinte resultado:

Corolário 3.3.4. *Sejam $G = (g)_{2^k}$ e R a álgebra de divisão graduada $\mathcal{E}(\varepsilon, 2^k)$.*

(i) Uma base para o T_G-ideal $Id_G(R)$ consiste dos polinômios

$$x_{1k}x_{2k} - x_{2k}x_{1k} \quad e \quad x_{1h}x_{2h}x_{3h} - x_{3h}x_{2h}x_{1h},$$

onde $k \in \{g^{2m} \mid m = 0, 1, \ldots, 2^{k-1}\}$ e $h \in \{g^{2m+1} \mid m = 0, 1, \ldots, 2^{k-1}\}$.

(ii) Uma base para o T_G-espaço $C_G(R)$ consiste dos polinômios

$$x_{1h}x_{2h} + x_{2h}x_{1h}, \quad x_{1g'}[x_{2k}, x_{3k}]x_{4h'} \quad e \quad x_{1g'}\left(x_{2h}x_{3h}x_{4h} - x_{4h}x_{3h}x_{2h}\right)x_{5h'},$$

onde $k \in \{g^{2m} \mid m = 0, 1, \ldots, 2^{k-1}\}$, $h \in \{g^{2m+1} \mid m = 0, 1, \ldots, 2^{k-1}\}$ e g', $h' \in G$.

4 Mergulho em Álgebras de Jordan

Neste capítulo iremos demonstrar um resultado análogo ao obtido por Procesi em [72], mas no caso das álgebras de Jordan $B_n(K)$ (ver Exemplo 1.7.15). O objetivo principal deste capítulo é descrever uma condição necessária para que uma álgebra R possa ser mergulhada em $B_n(C)$, a álgebra de Jordan de uma forma bilinear sobre uma álgebra comutativa e associativa C. Para isto iremos apresentar resultados análogos aos que foram obtidos em [9, 72]. Observamos que alguns dos resultados apresentados neste capítulo podem ser demonstrados sobre um corpo infinito de característica diferente de dois. Por outro lado, a restrição do corpo ter característica zero é essencial já que a demonstração do resultado principal utilizará a teoria de grupos algébricos semissimples. Por este motivo assumimos, a menos de menção contraria, K um corpo de característica 0.

4.1 Definições e Resultados Preliminares

Seja A uma álgebra de dimensão finita (não necessariamente associativa), podemos fixar um elemento $a \in A$ e denotar por D_a (resp. E_a) o operador multiplicação à direita (resp. esquerda) por a. Além disso, considerando $K\{Y\}$ a álgebra livre livremente gerada pelo conjunto $Y = \{y_1, \dots, y_k\}$. Observamos que todo elemento $f = f(y_1, \dots, y_k)$ em $K\{Y\}$ define aplicações polinomiais sobre A^k dadas por

$$D_f, E_f \colon A^k \to End_K A, \tag{4.1}$$

onde $D_f(a_1, \dots, a_k) = D_{f(a_1,\dots,a_k)}$ e $E_f(a_1, \dots, a_k) = E_{f(a_1,\dots,a_k)}$.

Um problema bastante interessante na teoria de invariantes é a descrição da álgebra de invariantes de A por um grupo G. Denotamos por $K[A^k]$ a álgebra de funções polinomiais $A^k \to K$. Seja Tr_k a subálgebra de $K[A^k]$ gerada pelo conjunto

$$\{tr(T_{f_1} \dots T_{f_t}) \mid T \in \{D, E\} \text{ e } f_1, \dots, f_t \in K\{Y\}\},$$

e G agindo como grupo de automorfismos da álgebra A da seguinte forma:

$$g \cdot T_f = gT_f g^{-1} = T_{g \cdot f}.$$

Claramente $Tr_k \subseteq K[A^k]^G$, porém a igualdade no caso geral não é tão simples. Em particular, Artin conjecturou, em [10], que se $A = M_n(K)$ então $Tr_k = K[A^k]^G$, sendo demonstrado posteriormente por Procesi em [71]. Mais precisamente temos o seguinte exemplo.

Exemplo 4.1.1. *Sejam $A = M_n(K)$, "tr" o traço usual de matrizes e G o grupo de automorfismos da álgebra A. Consideramos $X_j\colon (A_1, \ldots, A_k) \to A_j$, as* ***projeções equivariantes****, onde A_i são matrizes em $M_n(K)$. Em [71], Procesi demonstrou que qualquer função polinomial invariante de k matrizes é combinação linear de produtos de elementos da forma*

$$tr(X_{i_1} \ldots X_{i_t}),$$

onde $t \leqslant 2^n - 1$. Note ainda que para quaisquer $a, b \in A$, temos que

$$tr(T_a) = ntr(a), \quad tr(E_a D_b) = tr(a)tr(b). \tag{4.2}$$

De fato, seja $\mathcal{B}$ a base de A formada pelas matrizes elementares E_{ij} então todo elemento de A pode ser escrito da forma $a = \sum_{r,s=1}^{n} a_{rs}E_{rs}$ e daí

(i) $E_a(E_{ij}) = aE_{ij} = \sum_{r=1}^{n} a_{ri}E_{rj}$;

(ii) $D_a(E_{ij}) = E_{ij}a = \sum_{s=1}^{n} a_{js}E_{is}$;

(iii) $E_aD_b(E_{ij}) = a(E_{ij}b) = a(\sum_{t=1}^{n} b_{jt}E_{it}) = \sum_{r,t=1}^{n} (a_{ri}b_{jt})E_{rt}$, *com* $b = \sum_{u,t=1}^{n} b_{ut}E_{ut}$.

Assim, as matrizes de E_a e D_a, com respeito a base $\mathcal{B}$, são da forma

$$\begin{pmatrix} \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{11} \end{pmatrix}_{n\times n} & & \\ & \ddots & \\ & & \begin{pmatrix} a_{nn} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix}_{n\times n} \end{pmatrix}$$

e

$$\begin{pmatrix} \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix}_{n\times n} & & \\ & \ddots & \\ & & \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix}_{n\times n} \end{pmatrix}$$

respectivamente. Além disso, temos que a matriz associada à E_aD_b é da forma

$$\begin{pmatrix} \begin{pmatrix} a_{11}b_{11} & & \\ & \ddots & \\ & & a_{11}b_{nn} \end{pmatrix}_{n\times n} & & \\ & \ddots & \\ & & \begin{pmatrix} a_{nn}b_{11} & & \\ & \ddots & \\ & & a_{nn}b_{nn} \end{pmatrix}_{n\times n} \end{pmatrix}.$$

Portanto, a conjectura de Artin é válida para $M_n(K)$.

Observação 4.1.2. *Analogamente, temos a validade da conjectura para o caso da álgebra com involução $(M_n(K), *)$, onde $* = t$ ou s são as involuções transposta e simplética (quando n é par) usuais de matrizes, respectivamente, para maiores detalhes ver [71]. Mais geralmente, se A for uma álgebra simples de dimensão finita segue do Teorema 1.1.42 e da aplicação traço ser invariante por extensão do corpo (ver construção do traço genérico feita na Seção 1.6) que A satisfaz um análogo a conjectura de Artin.*

Exemplo 4.1.3. *Considere $A = B_n(K) = K \oplus V$ a álgebra de Jordan de uma forma bilinear f (ver Exemplo 1.7.15) e o traço dado por $trd(\alpha \cdot 1_K + v) = 2\alpha$. Seja $\mathcal{B}$ a base de A formada por 1 e elementos ortogonais em relação a forma f sobre o espaço vetorial V, digamos que $\mathcal{B} = \{1, e_1, \ldots, e_n\}$ e assim todo elemento de A pode ser escrito da forma $a = \alpha_0 + \sum_{r=1}^{n} \alpha_r e_r$ implicando $E_a(1) = a \cdot 1 = a$ e $E_a(e_i) = a \cdot e_i = \alpha_0 e_i + \alpha_i f(e_i, e_i)$, para todo $i = 1, \ldots, n$. A matriz de E_a, com respeito a base $\mathcal{B}$, é da forma*

$$\begin{pmatrix} \alpha_0 & & \\ & \ddots & \\ & & \alpha_0 \end{pmatrix}.$$

Por A ser comutativa, D_a possui a mesma representação matricial que E_a. Além disso, considerando $b = \beta_0 + \sum_{r=1}^{n} \beta_r e_r$, temos

(i) $E_aE_b(1) = (\alpha_0\beta_0 + f(v_a, v_b)) + (\alpha_0 v_b + \beta_0 v_a)$;

(ii) $E_aE_b(e_i) = E_a(\beta_0 e_i + f(v_b, e_i)) = (\alpha_0 f(v_b, e_i) + \beta_0 f(v_a, e_i)) + (\alpha_0\beta_0 e_i + f(v_b, e_i)v_a)$

onde $v_a = \sum_{r=1}^{n} \alpha_r e_r$ e $v_b = \sum_{r=1}^{n} \beta_r e_r$. Isso implica que a matriz de E_aE_b com respeito a base

$\mathcal{B}$ é da forma

$$\begin{pmatrix} \alpha_0\beta_0 + f(v_a, v_b) & & & \\ & \alpha_0\beta_0 + \beta_1\alpha_1 f(e_1, e_1) & & \\ & & \ddots & \\ & & & \alpha_0\beta_0 + \beta_n\alpha_n f(e_n, e_n) \end{pmatrix}.$$

Assim, $Tr(E_a) = \left(\frac{n+1}{2}\right) trd(a)$ *e*

$$Tr(E_aE_b) = (n-1)\alpha_0\beta_0 + 2[(\alpha_0\beta_0) + f(v_a, v_b)] = trd(ab) + \frac{(n-1)}{4} trd(a)trd(b),$$

para todo $a, b \in A$*, já que* $n > 1$*. Os invariantes polinomiais de* A *são gerados pelos produtos de elementos da forma* $trd(X_{i_1})$ *ou* $trd(X_{i_1}X_{i_2})$*, onde* X_i *são aplicações equivariantes, entraremos em maiores detalhes nesta discussão na Seção 4.4. Portanto, um análogo a conjectura de Artin é também válido para o caso* $B_n(K)$*.*

Exemplo 4.1.4. *Consideremos, agora, a álgebra de Albert (ver Exemplo 1.7.19) que denotaremos novamente por* A*. Foi provado por Iltyakov, em [47, 48] que a álgebra dos invariantes polinomiais de* A *sob a ação do grupo* $G = Aut_K(A)$ *satisfaz um análogo a conjectura de Artin para os casos em que* $k \leqslant 3$*. Já para o caso* $k > 3$ *a questão de que essas álgebras coincidem está aberta até o momento.*

Motivado por alguns desses exemplos, Iltyakov [46] reformulou uma conjectura que generaliza a conjectura de Artin de maneira que $Tr_k = K[A^k]^G$ se A é simples. Porém Popov [70] construiu uma álgebra simples de modo que a igualdade anterior não seja verdadeira (ver [70, Subseção 4,7]). Tomando uma álgebra A central simples associativa ou de Jordan de dimensão finita sobre um corpo K de característica 0 podemos considerar o traço genérico Trd sobre A e denotar por Tr'_k a nova subálgebra de $K[A^k]$ gerada pelos elementos $Trd(v) = Trd \circ v$, onde $v = v(y_1, y_2, \ldots, y_k)$ é um polinômio na álgebra livre $K\{Y\}$ livremente gerada pelo conjunto $Y = \{y_1, \ldots, y_k\}$. Do Corolário 1.6.2 temos que $Tr'_k \subseteq K[A^k]^G$, onde G age como um grupo de automorfismos da álgebra A.

Usando esses comentários e focando no fato de que este trabalho pretende estabelecer condições para imersão de uma álgebra em $B_n(C)$, para alguma álgebra comutativa C, podemos reescrever uma forma "interna" da conjectura proposta por Artin, Iltyakov e Popov, da seguinte maneira:

Conjectura 4.1.5. *Seja* G *um grupo algébrico linear redutível não trivial. Se* G *age como o grupo dos automorfismos de uma álgebra* A *central simples de dimensão finita, então* $Tr'_k = K[A^k]^G$*.*

Observe que a conjectura é válida para todos os exemplos listados anteriormente, inclusive para o caso em que A é a álgebra de Cayley-Dickson (sobre o corpo dos números complexos, ver [87]).

4.2 A-Aplicação Universal

Consideremos $\mathcal{V}$ uma variedade de álgebras (como por exemplo, associativas, associativas com involução, de Jordan, de Lie, entre outras) e denotaremos por A alguma álgebra central simples de dimensão finita nesta variedade. Além disso, dizemos que uma álgebra é **comutativa-associativa** se ela é uma álgebra comutativa na variedade de todas as álgebras associativas.

Sejam $\mathcal{B}_A = \{a_1, \ldots, a_n\}$ uma base da álgebra A e C uma álgebra comutativa-associativa sobre K. Então qualquer elemento v em $A \otimes_K C$ pode ser escrito da forma $v = \sum_{i=1}^{n} a_i \otimes c_i$, onde $c_i \in C$. Além disso, os elementos $c_1, \ldots, c_n$ são chamados **coeficientes do elemento v sobre C**.

Observação 4.2.1. *Sejam R e S anéis, e $\eta\colon R \to S$ um homomorfismo entre anéis. Denotaremos por η_A o homomorfismo $(Id_A \otimes \eta)\colon A \otimes_K R \to A \otimes_K S$, e dizemos que η_A é o homomorfismo induzido por η.*

Nesta seção iremos determinar e provar um resultado análogo ao demonstrado por Amitsur em [9]. Mais precisamente, iremos demonstrar o seguinte resultado.

Teorema 4.2.2. *Sejam A uma álgebra central simples de dimensão finita e R uma álgebra, ambas em uma variedade $\mathcal{V}$. Então existe uma álgebra comutativa-associativa, denotada por S, e um homomorfismo $\rho\colon R \to A \otimes_K S$ satisfazendo as seguintes condições:*

(a) Os coeficientes dos elementos em $\{\rho(r) \mid r \in R\}$ sobre S geram, junto com 1, a álgebra comutativa-associativa S.

(b) Para quaisquer álgebra comutativa-associativa F e homomorfismo $\sigma\colon R \to A \otimes_K F$ existe um homomorfismo $\eta_A\colon A \otimes_K S \to A \otimes_K F$ induzido pelo homomorfismo $\eta\colon S \to F$ tal que $\eta_A \rho = \sigma$.

Notação 4.2.3. *Dizemos que o par (S, ρ), dado no teorema anterior, é a **A-aplicação universal de** R.*

Para demonstrar o teorema anterior usaremos o seguinte resultado, o qual pode ser encontrado em [49, Teorema 1, pág. 109] ou [90, Corolário 2.2].

Teorema 4.2.4. *Se B é uma álgebra qualquer, então todo ideal $\mathfrak{I}$ de $A \otimes_K B$ tem a forma $A \otimes_K I$ para um ideal I de B unicamente determinado. Em particular, se B é uma álgebra simples então $A \otimes_K B$ é também uma álgebra simples.*

Definição 4.2.5. *Sejam A uma álgebra central simples de dimensão finita e R uma álgebra, ambas em uma variedade $\mathcal{V}$. Assuma que existam C e C' álgebras comutativas-associativas* *tais que $\varphi\colon R \to A \otimes_K C$ e $\varphi'\colon R \to A \otimes_K C'$ sejam homomorfismos de álgebras. Um isomorfismo de pares (C, φ) em (C', φ') é um isomorfismo $\psi\colon C \to C'$ tal que $\varphi' = \psi_A \varphi$.*

Antes de provar a existência da A-aplicação universal iremos demonstrar, a menos de isomorfismo, a unicidade deste par. Mais precisamente, demonstraremos a seguinte proposição.

Proposição 4.2.6. *Sob as condições do Teorema 4.2.2. Se existir o par (S, ρ), então (S, ρ) é unicamente determinado, a menos de isomorfismo de par. Além disso, dados S, ρ e σ então η_A é unicamente determinado.*

Demonstração. Começamos fixando uma álgebra comutativa-associativa F e um homomorfismo $\sigma\colon R \to A \otimes_K F$. Suponha que existam η, $\eta'\colon S \to F$ homomorfismos satisfazendo o Teorema 4.2.2, isto é, $\eta_A \rho = \eta'_A \rho = \sigma$. Então $\eta_A \rho(r) = \eta'_A \rho(r)$, para todo r de R sobre K. Isso implica que $\eta(s) = \eta'(s)$ para todo s gerador de S, como álgebra. Portanto $\eta = \eta'$.

Consideremos agora (S, ρ) e (S', ρ') A-aplicações universais de uma álgebra R satisfazendo as condições (a) e (b) do Teorema 4.2.2. Então existem homomorfismos $\varsigma_A\colon A \otimes_K S \to A \otimes_K S'$ e $\varsigma'_A\colon A \otimes_K S' \to A \otimes_K S$ induzidos por $\varsigma\colon S \to S'$ e $\varsigma'\colon S' \to S$, respectivamente, tais que $\varsigma_A \rho = \rho'$ e $\varsigma'_A \rho' = \rho$, implicando $\varsigma'_A \varsigma_A \rho = \rho$. Da primeira parte da proposição, temos que o homomorfismo $\varsigma'_A \varsigma_A = Id_{A \otimes_K S}$ é induzido por $\varsigma' \varsigma$, ou seja, $\varsigma'_A \varsigma_A = (\varsigma' \varsigma)_A$ e consequentemente $\rho(r) = (\varsigma' \varsigma)_A \rho(r)$, para todo gerador r de R. Portanto todo coeficiente de $\rho(r)$, digamos s, será da forma $s = \varsigma' \varsigma(s)$. Como esses coeficientes, junto com 1, geram S, temos que $\varsigma' \varsigma$ é a aplicação identidade sobre S. Similarmente, $\varsigma \varsigma' = Id_{S'}$ e portanto ς, ς' são isomorfismos. Em particular, se $S \simeq S'$ então $\rho' = \varsigma_A \rho$, o que completa a prova da unicidade de S e ρ. □

A prova do Teorema 4.2.2 seguirá como consequência dos seguintes lemas.

Lema 4.2.7. *A álgebra livre $K\{X\}$ livremente gerada por um conjunto enumerável X satisfaz a A-aplicação universal.*

Demonstração. Seja $v_j = \sum_{i=1}^{n} a_i \otimes \xi_{ij}$, com $j \in \mathbb{N}$, um elemento genérico de A sobre K, ou seja, os elementos $\{\xi_{ij} \mid 1 \leqslant i \leqslant n\}$ são indeterminadas comutativas e associativas sobre K; eles são os coeficientes do elemento v_j sobre a álgebra de polinômios nas variáveis ξ_{ij}, denotado por $\Delta = K[\xi]$. Considerando $K\{v\}$ a álgebra gerada pelos v_j's, temos que $K\{v\} \subseteq A \otimes_K \Delta$. Consideremos o homomorfismo de álgebras $\psi\colon K\{X\} \to K\{v\}$ dado por $\psi(x_j) = v_j$. É claro que o par (Δ, ψ) satisfaz a condição (a) do Teorema 4.2.2, restando verificar o item (b). Para toda álgebra comutativa-associativa F e todo homomorfismo $\sigma\colon K\{X\} \to A \otimes_K F$ dado por $\sigma(x_i) = \sum a_i \otimes_K f_{ij}$, temos a existência de um homomorfismo

$\eta\colon \Delta \to F$ tal que $\eta(\xi_{ij}) = f_{ij}$ induzindo uma aplicação $\eta_A\colon A \otimes_K \Delta \to A \otimes F$ dada por

$$\eta_A(\sum a_i \otimes_K \xi_{ij}) = \sum a_i \otimes_K \eta(\xi_{ij}) = \sum a_i \otimes_K f_{ij},$$

um vez que Δ é a álgebra comutativa-associativa livre, livremente gerada pelo conjunto $\{\xi_{ij} \mid 1 \leqslant i \leqslant n_j \text{ e } j \in \mathbb{N}\}$. Note que

$$\eta_A\psi(x_j) = \eta_A(v_j) = \sum a_i \otimes_K \eta(\xi_{ij}) = \sum a_i \otimes_K f_{ij} = \sigma(x_j).$$

Portanto, o resultado está provado. $\square$

Lema 4.2.8. *Seja R uma álgebra em $\mathcal{V}$. Se (S,ρ) é a A-aplicação universal de R, então para todo ideal I de R existe J ideal de S tal que o par $(S/J, \rho')$ é a A-aplicação universal de R/I.*

Demonstração. Considere as projeções $\pi_I\colon R \to R/I$ e $\pi_{\rho(I)}\colon A \otimes_K S \to A \otimes_K (S/J)$, onde $(\rho(I)) = A \otimes_K J$, e observe que a boa definição desta última aplicação segue do Teorema 4.2.4. Denotando por $\mathcal{B}_R = \{r_i \mid i \in \Gamma\}$ um conjunto gerador da álgebra R, temos da definição de A-aplicação universal que os coeficientes dos elementos $\rho(r_i) = \sum\limits_j a_j \otimes_K \rho(r_i)_j$, junto com 1, geram S como álgebra. Denotemos tais elementos por $s_{ij} = \rho(r_i)_j$. Além disso, podemos considerar a aplicação composição:

$$R \xrightarrow{\rho} (A \otimes_K S) \xrightarrow{\pi_{\rho(I)}} (A \otimes_K S/J)\ , \tag{4.3}$$

dada por $\pi_{\rho(I)}\rho(r_i) = \sum\limits_i a_j \otimes_K (s_{ij} + J)$. Observamos que $I \subseteq Ker\pi_{\rho(I)}\rho$ e definimos $\rho'\colon R/I \to A \otimes_K (S/J)$ por $\rho'(r_i + I) = \sum\limits_i a_j \otimes_K (s_{ij} + J)$, implicando que o diagrama

$$\begin{tikzcd} R \arrow[r, "\rho"] \arrow[d, "\pi_I"'] & A \otimes_K S \arrow[d, "\pi_{\rho(I)}"] \\ R/I \arrow[r, "\rho'"'] & A \otimes_K (S/J) \end{tikzcd}\ , \tag{4.4}$$

é comutativo. É claro que S/J é gerado, como álgebra, pelos elementos $s_{ij} + J$ junto com $1 + J$, isto implica o item (a) do Teorema 4.2.2. Para provar o item (b) do mesmo teorema, tomemos uma álgebra comutativa-associativa F e um homomorfismo $\sigma\colon R/I \to A \otimes_K F$. Por (S,ρ) ser a A-aplicação universal para R, então existe um homomorfismo $\eta\colon S \to F$ que induz uma aplicação $\eta_A\colon A \otimes_K S \to A \otimes_K F$ de modo que a relação $\eta_A\rho = \sigma\pi_I$ seja válida. Temos de provar a existência de um homomorfismo $\bar{\eta}_A\colon A \otimes_K (S/J) \to A \otimes_K F$ de modo que o diagrama

$$\begin{tikzcd} R \arrow[r, "\rho"] \arrow[d, "\pi_I"'] & A \otimes_K S \arrow[d, "\pi_{\rho(I)}"] \arrow[dd, bend left=60, "\eta_A"] \\ R/I \arrow[r, "\rho'"] \arrow[dr, "\sigma"'] & A \otimes_K (S/J) \arrow[d, dashed, "\bar{\eta}_A"] \\ & A \otimes_K F \end{tikzcd}\ , \tag{4.5}$$

seja comutativo. Para isto é suficiente mostrar que $J \subseteq Ker\eta$, mas isto segue do fato que $\pi_I(I) = 0$, uma vez que $\eta_A\rho(I) = \sigma\pi_I(I) = 0$, concluindo a existência de um homomorfismo $\bar{\eta}\colon S/J \to F$. Consequentemente, a existência do homomorfismo $\bar{\eta}_A\colon A\otimes_K(S/J) \to A\otimes_K F$ dado por $\eta_A = \bar{\eta}_A\pi_{\rho(I)}$ é garantida por $\bar{\eta}$, ou seja, $\bar{\eta}_A$ é induzido por $\bar{\eta}$. Além disso,

$$\sigma(r_i + I) = \sigma(\pi_I(r_i)) = \eta_A\rho(r_i) = \bar{\eta}_A\pi_{\rho(I)}\rho(r_i) = \bar{\eta}_A\rho'\pi_I(r_i) = \bar{\eta}_A\rho'(r_i + I),$$

para todo $r_i \in \mathcal{B}_R$ e por $\mathcal{B}_R$ ser conjunto gerador de R (como álgebra), implica que $\sigma = \bar{\eta}_A\rho'$. Então segue o resultado. □

Demonstração do Teorema 4.2.2. Pelo Lema 4.2.7, o par (Δ, ψ) é a A-aplicação universal de $K\{X\}$. Considerando $\{r_i \mid i \in \Lambda\}$ um conjunto gerado para R, como álgebra, e o homomorfismo $\varphi\colon K\{X\} \to R$ dado por $\varphi(x_i) = r_i$. Podemos apresentar R como sendo $K\{X\}/I$, onde $I = Ker\varphi$. Denotando por P a imagem do ideal I por ψ, temos do Teorema 4.2.4 a existência de um ideal $\mathfrak{p}$ em Δ tal que $(P) = A \otimes_K \mathfrak{p}$ é um ideal de $A \otimes_K \Delta$. Concluímos a demonstração aplicando o Lema 4.2.8. □

Iremos agora listar uma série de consequências do Teorema 4.2.2.

Corolário 4.2.9. *Sob as condições do Teorema 4.2.2, se R é finitamente gerada, então S também o é. Além disso, S é noetheriana.*

Demonstração. Segue diretamente da condição (a) do Teorema 4.2.2. □

Corolário 4.2.10. *A álgebra R pode ser mergulhada em $A \otimes_K F$ para alguma álgebra comutativa-associativa F se, e somente se, o homomorfismo $\rho\colon R \to A \otimes_K S$ do Teorema 4.2.2 for injetivo.*

Demonstração. Se ρ é um monomorfismo então é claro que R pode ser mergulhada em $A \otimes_K S$. Reciprocamente, se existir um mergulho $\sigma\colon R \to A \otimes_K F$ para alguma álgebra comutativa-associativa F. Por (S, ρ) ser a A-aplicação universal de R temos que o diagrama

$$\begin{tikzcd} R \arrow[r, "\sigma"] \arrow[d, "\rho"'] & A \otimes_K F \\ A \otimes_K S \arrow[ur, "\eta_A"'] & \end{tikzcd}$$

é comutativo, ou seja, $\sigma = \eta_A\rho$. Portanto, σ ser um monomorfismo implica que ρ é injetivo. □

Observação 4.2.11. *Uma condição necessária e suficiente para que o Corolário 4.2.10 seja válido é que exista um homomorfismo φ de $K\{v\}$ em R com $P = Ker\varphi$, implicando $(P) \cap K\{v\} = P$, onde $K\{v\}$ é a álgebra gerada pelos v_j's dados no Lema 4.2.7.*

Corolário 4.2.12. *Toda álgebra R contém um único ideal Q que satisfaz:*

(i) R/Q é mergulhada em $A \otimes_K S$;

(ii) Se Q_0 é um ideal de R tal que R/Q_0 é mergulhada em algum $A \otimes_K F$, então $Q \subseteq Q_0$.

Demonstração. Seja (S, ρ) a A-aplicação universal de R e considere $Q = Ker\rho$. Então ρ induz um mergulho de R/Q sobre $A \otimes_K S$. Suponha a existência de outro ideal Q_0 de R tal que $\sigma\colon R/Q_0 \to A \otimes_K F$ seja um monomorfismo, para alguma álgebra comutativa-associativa F. Pelo Teorema 4.2.2, temos a existência de $\eta_A\colon A \otimes_K S \to A \otimes_K F$ tal que $\eta_A\rho = \sigma\pi_{Q_0}$, onde $\pi_{Q_0}\colon R \to R/Q_0$ é a projeção canônica, e assim $0 = \eta_A\rho(x) = \sigma\pi_{Q_0}(x)$, para todo $x \in Q$. Isto implica que $x \in Q_0$, já que σ é injetivo. Portanto, $Q \subseteq Q_0$. A unicidade é óbvia, uma vez que se existir P ideal de R satisfazendo as condições do corolário, teremos $P \subseteq Q$ e $Q \subseteq P$, ou seja, $P = Q$. □

Sejam G o grupo dos automorfismos de A e (S, ρ) a A-aplicação universal de uma álgebra R, então podemos considerar a aplicação $\Phi_g\colon A \otimes S \to A \otimes S$ dada por $\Phi_g(a \otimes_K s) = (g \cdot a) \otimes_K s$, para todo $g \in G$. Por outro lado, existe uma aplicação estendendo $\eta^g\colon S \to S$ dado por

$$\eta_A^g\left(\sum_{i=1}^{n} a_i \otimes s_i\right) = \sum_{i=1}^{n} a_i \otimes \eta^g(s_i),$$

de modo que

$$\Phi_g \circ \rho = \eta_A^g \circ \rho, \tag{4.6}$$

isto é, o diagrama

$$\begin{tikzcd} R \arrow[r, "\rho"] \arrow[d, "\rho"'] & A \otimes_K S \arrow[r, "\Phi_g"] & A \otimes_K S \\ A \otimes_K S \arrow[urr, "\eta_A^g"'] & & \end{tikzcd} \tag{4.7}$$

é comutativo. Observamos a comutatividade entre as aplicações Φ_g e η_A^h, já que Φ_g e η_A^h fixam os elementos de S e A, respectivamente. Além disso, para todo $g, h \in G$ temos que

$$\eta_A^{gh} \circ \rho = \Phi_{gh} \circ \rho = \Phi_g \circ \Phi_h \circ \rho = \Phi_g \circ \eta_A^h \circ \rho = \eta_A^h \circ \Phi_g \circ \rho = \eta_A^h \circ \eta_A^g \circ \rho = (\eta^h\eta^g)_A \circ \rho,$$

implicando da Proposição 4.2.6 que $\eta^{gh} = \eta^h\eta^g$. Por fim, G não age somente sobre Δ, mas também sobre $A \otimes_K \Delta$, da seguinte maneira

$$\zeta\colon G \to GL(A \otimes_K \Delta)$$

dado por

$$\zeta_g\left(\sum_{i=1}^{n} a_i \otimes s_i\right) = \Phi_g \circ (\eta_A^g)^{-1}\left(\sum_{i=1}^{n} a_i \otimes s_i\right) = \sum_{i=1}^{n} g \cdot a_i \otimes \eta^{g^{-1}}(s_i),$$

para qualquer $g \in G$, e assim temos o seguinte resultado.

Proposição 4.2.13. *Seja (S,ρ) a A-aplicação universal de R. Então G ($= Aut_K A$) age, via a representação ζ_g, como um grupo de automorfismos de $A \otimes_K S$ e $\rho(R)$ está contido no anel de invariantes de $A \otimes_K S$.*

Corolário 4.2.14. *Seja (S,ρ) a A-aplicação universal de R. Para todo ideal J de S, a aplicação projeção $\pi_J\colon A \otimes_K S \to A \otimes_K (S/J)$ é G-equivariante.*

Demonstração. Seja I um ideal de R tal que $(\rho(I)) = A \otimes_K J$. Por abuso de notação iremos usar o mesmo símbolo Φ_g para denotar a aplicação $\Phi_g\colon A \otimes_K (S/J) \to A \otimes_K (S/J)$ dada por $\Phi_g(a \otimes \bar{s}) = (g \cdot a) \otimes \bar{s}$, para todo $g \in G$. Para demonstrar que a aplicação $\pi_{\rho(I)}$ é G-equivariante é suficiente provar que $\pi_{\rho(I)}\Phi_g(\eta_A^g)^{-1} = \Phi_g(\bar{\eta}_A^g)^{-1}\pi_{\rho(I)}$. Primeiramente, observamos que o diagrama

$$
\begin{tikzcd}
A \otimes_K S \arrow[r, "\Phi_g"] & A \otimes_K S \\
R \arrow[u, "\rho"] \arrow[r, "\rho"] \arrow[d, "\pi_I"'] & A \otimes_K S \arrow[u, "\eta_A^g"'] \arrow[d, "\pi_{\rho(I)}"] \\
R/I \arrow[r, "\rho'"'] \arrow[d, "\rho'"'] & A \otimes_K (S/J) \arrow[d, "\bar{\eta}_A^g"] \\
A \otimes_K (S/J) \arrow[r, "\Phi_g"'] & A \otimes_K (S/J)
\end{tikzcd}
$$

é comutativo, implicando

$$
\begin{aligned}
\pi_{\rho(I)}\Phi_g(\eta_A^g)^{-1}\rho &= \pi_{\rho(I)}(\eta_A^g)^{-1}\Phi_g\rho \\
&= \pi_{\rho(I)}\rho \\
&= \rho'\pi_I \\
&= (\bar{\eta}_A^g)^{-1}\Phi_g\rho'\pi_I \\
&= (\bar{\eta}_A^g)^{-1}\Phi_g\pi_{\rho(I)}\rho \\
&= \Phi_g(\bar{\eta}_A^g)^{-1}\pi_{\rho(I)}\rho.
\end{aligned}
$$

O resultado segue aplicando a Proposição 4.2.6. □

Como em [72], um caso particular importante da construção anterior ocorre quando R é a álgebra livre $K\{X\}$. Neste caso, S é o anel de polinômios em várias variáveis comutativas, como provado no Lema 4.2.7. Note que $\rho(x_j)$ é o "elemento genérico" cujo i-ésimo coeficiente será a variável ξ_{ij}. Assim, podemos considerar $\rho(x_j) = \sum_{i=1}^{n} a_i \otimes \xi_{ij}$, onde $\{a_1,\dots,a_1\}$ é uma base para A. Pela Igualdade (4.6), temos que

$$
\eta_A^g\left(\sum_{i=1}^{n} a_i \otimes \xi_{ij}\right) = \sum_{i=1}^{n} g \cdot a_i \otimes \xi_{ij},
$$

para $g \in G$. Considere $g \cdot a_i = \sum_{k=1}^{n} \alpha_{ki}(g)a_k$, temos que

$$\eta_A^g(v_j) = \eta_A^g\left(\sum_{i=1}^{n} a_i \otimes \xi_{ij}\right) = \sum_{i=1}^{n}\left(\sum_{k=1}^{n} \alpha_{ki}(g)a_k\right) \otimes \xi_{ij} = \sum_{k=1}^{n} a_k \otimes \left(\sum_{i=1}^{n} \alpha_{ki}(g)\xi_{ij}\right),$$

isto implica que $\eta^g(\xi_{rj}) = \sum_{i=1}^{n} \alpha_{ri}(g)\xi_{ij}$. Como $char K = 0$ então podemos considerar $f \in \Delta$ multilinear e o resultado segue por polarização completa. Então para todo polinômio $f(\xi_{i_1 j_j}, \ldots, \xi_{i_m j_m}) = f$ em Δ, teremos $f = \alpha \xi_{i_1 j_1} \ldots \xi_{i_m j_m}$, com $j_1 \leqslant \cdots \leqslant j_m$. Considerando o subespaço

$$P_m = span_K\{\xi_{i_1 j_1} \ldots \xi_{i_m j_m} \mid 1 \leqslant i_t \leqslant n; 1 \leqslant t \leqslant m\}$$

de Δ observamos que P_m é G-invariante, tem dimensão finita e contém f. Assim podemos assumir que $\{s_1, \ldots, s_t\}$ é uma base para o G-espaço P_m. Se $\eta_m \colon G \times P_m \to P_m$ denota a ação η restrita à P_m, então

$$\eta_m^g(s_i) = \sum_{j=1}^{t} m_{ij}(g)s_j.$$

Em outras palavras, a matriz η_m^g (relativa à base $\{s_1, \ldots, s_t\}$) é $(m_{ij}(g))$, além disso temos que tal representação de grupo é fiel. Isto significa que $\eta_m \colon G \to GL(P_m) \simeq GL_t(K)$, onde $\eta_m(g) = (m_{ij}(g))$, é um morfismo de grupos algébricos. De acordo com a Definição 1.10.11 temos que Δ é um G-módulo racional (ver [44, Seção 8.6, pág. 63]). Em resumo temos o seguinte resultado.

Corolário 4.2.15. *Sejam G o grupo de automorfismos de uma álgebra central simples de dimensão finita A na variedade $\mathcal{V}$. Então a representação ζ é racional.*

Demonstração. Pelos Exemplos 1.10.12 e 1.10.13, é suficiente mostrar que a representação $\eta \colon G \to GL(S)$ é racional, mas isto segue dos comentários anteriores. □

Podemos assim interpretar a ação do grupo G de modo diferente. Para isto, interpretaremos $A \otimes_K S$ como sendo o anel de aplicações polinomiais e um elemento dele será da forma $f \colon (A \otimes_K F)^k \to (A \otimes_K F)$ definido sobre K (onde F é uma álgebra comutativa-associativa qualquer), a ação de grupo é dada por $f^g(a_1, \ldots, a_k) = g \cdot f(g^{-1} \cdot a_1, \ldots, g^{-1} \cdot a_k)$ e $f = f^g$ significa que f é uma aplicação equivariante. Na próxima seção iremos fazer uso deste último comentário.

4.3 Resultado Principal

Recordamos que K é um corpo de característica zero. O objetivo desta seção é provar que dada uma álgebra A central simples de dimensão finita e uma álgebra R, ambas com traço e na variedade das álgebras de Jordan ou associativas sobre K, podemos mergulhar R na álgebra $A \otimes_K F$ para alguma álgebra comutativa-associativa F, se R satisfaz todas as identidades com traço de A. Podemos supor, sem perda de generalidade, que K é algebricamente fechado, uma vez que se o resultado é válido para $\bar{K}$ sendo o fecho algébrico de K. Então dada R uma álgebra nestas condições, temos que $R_{\bar{K}}$ pode ser mergulhada em $A_{\bar{K}} \otimes_{\bar{K}} F$ como $\bar{K}$-álgebras, e consequentemente,

$$R \hookrightarrow R \otimes_K \bar{K} \hookrightarrow (A \otimes_K \bar{K}) \otimes_{\bar{K}} F \simeq (A \otimes_K F) \otimes_{\bar{K}} \bar{K} \simeq A \otimes_K F,$$

ou seja, R também será mergulhado em $A \otimes_K F$ como K-álgebras.

Proposição 4.3.1. *Seja $m = m(x_1, x_2, \ldots, x_t)$ um monômio nas variáveis x_1, x_2, $\ldots$, x_t na álgebra livre $K\{X\}$ tal que m seja linear em pelo menos uma de suas variáveis, digamos x_t. Então existe m', monômio nas variáveis x_1, x_2, $\ldots$, x_{t-1}, em $K\{X\}$ tal que*

$$Tr(m) = Tr(m'x_t),$$

onde Tr é o traço formal sobre $K\{X\}$.

Demonstração. Como m é uma palavra em $K\{X\}$, então podemos escrevê-la da forma $m = uv$, onde u, v são monômios nas variáveis x_1, x_2, $\ldots$, x_t cujos graus são menores do que a de m. Se $u = x_t$ então não há o que fazer, o resultado segue colocando $m' = v$, e analogamente se $v = x_t$. Caso contrário, podemos supor que x_t é uma variável em v. Por $Tr((a, b, c)) = 0$ e escrevendo v da forma $v = v''v'$, teremos

$$Tr(m) = Tr(uv) = Tr(u(v''v')) = Tr((uv'')v') = Tr(u'v'),$$

se x_t estiver em v', ou

$$Tr(m) = Tr(uv) = Tr((v''v')u) = Tr(v''(v'u)) = Tr(v''u'),$$

se x_t estiver em v'', onde $u' = uv''$ ou $v'u$, respectivamente. Tal processo se repete uma quantidade finita de etapas e assim podemos supor que $v = x_t$. Portanto, o resultado segue. □

Como consequência imediata da proposição anterior temos o seguinte resultado.

Corolário 4.3.2. *Se $g \in G\{X\}$ é um polinômio generalizado nas variáveis x_1, x_2, $\ldots$, x_{t+1} linear em pelo menos uma das variáveis, digamos x_{t+1}, então existe $f \in G\{X\}$ tal que*

$$Tr(g(x_1, x_2, \ldots, x_{t+1})) = Tr(f(x_1, x_2, \ldots, x_t)x_{t+1}).$$

Recordaremos que existe um traço genérico em A, denotado por Trd (Ver Seção 1.6). Pelo comentário feito no fim da seção anterior, podemos considerar a álgebra $A \otimes_K \Delta$ como sendo a álgebra de aplicações polinomiais $A^\infty \to A$, com $F = K$ e A^∞ sendo o espaço das sequências quase todas nulas $(a_1, a_2, \dots)$ de elementos de A. Além disso, denotaremos por X_i as projeções equivariantes $(a_1, a_2, \dots) \mapsto a_i$. Como A possui identidade, podemos considerar que $K \subseteq A$ e para todo $p \in A \otimes_K \Delta$ temos que a composição $Trd(p) = Trd \circ p$ é um elemento central em $A \otimes_K \Delta$, definindo um traço sobre $A \otimes_K \Delta$ o qual denotaremos por Tr. Consideraremos a ação do grupo dos automorfismos de A dado de forma natural $f^g((x_i)_{i\in I})) = g \cdot f((g^{-1} \cdot x_i)_{i\in I})$ e $f = f^g$ significa que f é uma aplicação equivariante. Ainda denotaremos por $\mathcal{T}$ a subálgebra de $A \otimes_K \Delta$ gerada pelas aplicações equivariantes, ou seja, $\mathcal{T} = (A \otimes \Delta)^G$. Observe que $X_i \in \mathcal{T}$, para todo i.

Observação 4.3.3. *Considerando A uma álgebra central simples de dimensão finita com traço genérico Trd não degenerado, temos que as álgebras com traço $(A \otimes_K \Delta, Tr)$ e (A, Trd) satisfazem as mesmas identidades com traço. De fato, é claro que $Id_{Tr}(A \otimes_K \Delta) \subseteq Id_{Tr}(A)$, faltando mostrar apenas a inclusão oposta. Para isto tome $f \in Id_{Tr}(A)$; por K ter característica zero, podemos supor que $f = f(x_1, \dots, x_n)$ é multilinear. Assim substituímos Tr (traço formal) por Tr (Traço em $A \otimes_K \Delta$) e obtemos*

$$f(p_1, \dots, p_n)(a_1, a_2, \dots) = f(p_1(a_1, a_2, \dots), \dots, p_n(a_1, a_2, \dots)) = 0,$$

para toda substituição por elementos $(p_1, \dots, p_n)$ de $A \otimes_K \Delta$ e quaisquer elementos a_j em A, para todo j. Portanto, $f \in Id_{Tr}(A \otimes_K \Delta)$.

Teorema 4.3.4. *Sejam A uma álgebra central simples de dimensão finita com traço genérico não degenerado que satisfaça a Conjectura 4.1.5 e G o grupo dos automorfismos de A. Então $\mathcal{T}$ é gerada, como álgebra, pelos elementos X_i e os $\mathrm{Tr}\, m(X_1, \dots, X_n)$, onde $m(x_1, \dots, x_n)$ é um monômio na álgebra livre unitária $K\{X\}$ e Tr é o traço definido sobre $A \otimes_K \Delta$.*

Demonstração. Denotemos por T a álgebra gerada pelos elementos x_i e $Tr(v(x_{i_1}, \dots, x_{i_l}))$, onde v é um monômio em $K\{X\}$ e Tr é o traço formal sobre $K\{X\}$. Consideremos uma aplicação equivariante $f\colon A^k \to A$, então é possível construir um invariante $\bar{f}\colon A^{k+1} \to K$ dado da seguinte forma

$$\bar{f} = Tr(f \cdot x_{k+1}).$$

Por A satisfazer a Conjectura 4.1.5, temos que $\bar{f}$ são somas de produtos de polinômios da forma $Tr(v(x_{i_1}, \dots, x_{i_l}))$, que é linear em x_{k+1}. Do Corolário 4.3.2, temos

$$\bar{f} = Tr(f' \cdot x_{k+1}),$$

para algum $f' \in T$. Portanto, o resultado segue do fato que o traço genérico Trd sobre A, como uma forma bilinear, é não degenerado. □

Da Observação 1.8.10, a álgebra A satisfaz a identidade de Cayley–Hamilton de grau s, então podemos enunciar o Teorema 4.3.4 do seguinte modo.

Teorema 4.3.5. *Sejam A uma álgebra central simples de dimensão finita com traço genérico não degenerado que satisfaça a Conjectura 4.1.5 e G o grupo dos automorfismos de A. Se A satisfaz a identidade de Cayley-Hamilton de grau s, então:*

(i) $Tr' = \bigcup_{k>0} Tr'_k$ *é gerada, como álgebra, pelos elementos da forma* $\mathrm{Tr}\ m(X_{j_1}, \ldots, X_{j_r})$, *onde* $m(x_1, \ldots, x_r)$ *são monômios na álgebra livre de grau* $r \leqslant 2^s$.

(ii) $\mathcal{T}$ *é gerada, como* Tr'*-álgebra, pelos elementos da forma* $n(X_{j_1}, \ldots, X_{j_r})$, *onde* $n(x_1, \ldots, x_r)$ *são monômios na álgebra livre de grau* $r \leqslant 2^s - 1$.

Demonstração. No caso em que A é associativa, o resultado segue de [71, Teorema 3.2]. Já no caso em que A é uma álgebra de Jordan, a demonstração segue passos análogos aos que foram feitos no caso associativo, aplicando o Teorema 1.7.23 em vez do Teorema de Nagata e Higman [49, pág. 274]. $\square$

Teorema 4.3.6. *Sejam A uma álgebra central simples de dimensão finita com traço genérico não degenerado que satisfaça a Conjectura 4.1.5 e G o grupo dos automorfismos de A. Então $\mathcal{T}$ é a álgebra livre com traço módulo o T_{Tr}-ideal de A.*

Demonstração. Devemos mostrar que $\mathcal{T} \simeq G\{X\}/Id_{Tr}(A)$. Inicialmente, observe que $\mathcal{T}$ é uma subálgebra de $A \otimes_K \Delta$ e que $Id_{Tr}(A \otimes_K \Delta) = Id_{Tr}(A)$. Portanto se considerarmos o epimorfismo com traço φ de $G\{X\}$ em $\mathcal{T}$ dado por $\varphi(x_i) = X_i$, temos que $Id_{Tr}(A) \subseteq Ker\varphi$. Por outro lado, seja f um elemento de $Ker\varphi$, então para quaisquer projeções equivariantes $X_1, \ldots, X_n$ em $A \otimes_K \Delta$ temos que $f(X_1, \ldots, X_n) = 0$, e assim para toda n-upla $(a_1, \ldots, a_n)$ de elementos em A temos que $0 = (f(X_1, \ldots, X_n))(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$, portanto f é uma identidade com traço para A e consequentemente $Ker\varphi = Id_{Tr}(A)$. $\square$

Considerando que G é semissimples, então todo G-módulo racional é completamente redutível. Suponha que M seja um G-módulo racional então M contém uma único submódulo maximal M_G tal que $M = M^G \oplus M_G$ e $(M_G)^G = (0)$. Além disso, M_G é o único G-complemento de M^G em M, para maiores detalhes ver [41, Lema 5.2, pág. 155]. Isso motiva fazer a seguinte definição.

Definição 4.3.7. *A projeção canônica $\pi_M^G \colon M \to M^G$ é usualmente chamada de* ***operador de Reynolds****.*

O operador de Reynolds π^G é realmente um functor definido sobre a categoria de G-módulos racionais no sentido que dados dois G-módulos M, M' e uma aplicação

G-linear $f\colon M \to M'$ tem-se o diagrama

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle \pi_M^G}\downarrow & & \downarrow{\scriptstyle \pi_{M'}^G} \\ M^G & \xrightarrow[f|_{M^G}]{} & M'^G \end{array}$$

comutativo, ou seja, $f \circ \pi_M^G = \pi_{M'}^G \circ f$. para maiores detalhes ver [41, Seção V-2].

Em particular, podemos considerar M uma álgebra com traço, $M' = \mathcal{Z}(M)$, $f = tr\colon M \to \mathcal{Z}(M)$ a aplicação traço de M e $G = Aut_K M$ semissimples. Então as seguintes relações serão válidas:

(i) Se $a \in M^G$ e $b \in M$ então $\pi_M^G(ab) = a\pi_M^G(b)$ e $\pi_M^G(ba) = \pi_M^G(b)a$;

(ii) $\pi_M^G(tr(a)) = tr(\pi_M^G(a))$, para todo $a \in M$.

Lema 4.3.8. *Sejam (A, τ) uma álgebra com traço e $G = Aut_K A$. Se I é um ideal de A^G, então (I) é um ideal com traço.*

Demonstração. É suficiente provar que (I) é invariante pela aplicação traço τ de A, já que (I) é o ideal de A gerado pelo conjunto I. Seja $\varphi\colon KTR\{X\} \to A$ o homomorfismo com traço dado por $\varphi(x_i) = a_i$ e $\varphi(Tr(x_{i_1} \cdots x_{i_t})) = \tau(a_{i_1} \cdots a_{i_t})$, então representaremos a álgebra A como $KTR\{X\}/J$ onde $J = Ker\varphi$. Pela correspondência biunívoca, existe P um subespaço de $KTR\{X\}$ que contém J tal que $P/J \simeq I$, já que $I \neq \{0\}$. Observamos que $(I) \simeq (P)/J$ e pela Proposição 1.4.7, (P) é soma de produtos, em qualquer associação de elementos de $KTR\{X\}$ desde que pelo menos um de seus elementos esteja em P. Assim podemos tomar $m = \sum_i m_i(y_{1i}, \ldots, y_{k_i i})$ um elemento em (P), onde pelo menos um dos y_{ji}'s está em P, digamos $y_{k_i i}$. Considere $m_i = m_i(y_{1i}, \ldots, y_{k_i i})$, da Proposição 4.3.1 existe $m_i'(y_{1i}, \ldots, \widehat{y}_{k_i i})$ tal que

$$Tr(m_i(y_{1i}, \ldots, y_{k_i i})) = Tr(m_i'(y_{1i}, \ldots, \widehat{y}_{k_i i}) \cdot y_{k_i i}).$$

Fazendo o homomorfismo projeção e aplicando o operador de Reynolds, temos que

$$Tr(m_i(\bar{y}_{1i}, \ldots, \bar{y}_{k_i i})) = Tr(\pi_A^G(m'(\bar{y}_{1i}, \ldots, \widehat{\bar{y}}_{k_i i})) \cdot \bar{y}_{k_i i}) \in I,$$

uma vez que $\pi_A^G(m'(\bar{y}_{1i}, \ldots, \widehat{\bar{y}}_{k_i i})) \in A^G$ e I é um ideal de A^G invariante pela aplicação traço, o resultado segue. $\square$

O teorema a seguir é o resultado principal desta seção.

Teorema 4.3.9. *Seja A uma álgebra central simples com traço, de dimensão finita na variedade $\mathcal{V}$ das álgebras associativas ou de Jordan, satisfazendo a Conjectura 4.1.5 e* *seja $G = Aut_K A$. Se R é uma álgebra com traço na variedade $\mathcal{V}$ que satisfaz todas as identidades com traço de A, então R pode ser mergulhada em $A \otimes_K S$ como uma K-álgebra, onde (S, ρ) é a A-aplicação universal de R. Além disso, $\rho(R) = (A \otimes_K S)^G$.*

Demonstração. Como R satisfaz todas as identidade com traço da álgebra A apresentaremos R como $\mathcal{T}/I$, onde $\mathcal{T}$ é a álgebra livre na categoria das álgebras que satisfazem todas as identidades com traço da álgebra A. Observe que $\mathcal{T} \subseteq A \otimes_K \Delta$. Assumimos por razões técnicas que $\mathcal{T}$ é gerado, como álgebra com traço, por um conjunto infinito de projeções equivariante (porém enumerável). Por I ser um ideal de $\mathcal{T}$, podemos considerar o ideal (I) de $A \otimes_K \Delta$ gerado pelo conjunto G-invariante I. Pelo Teorema 4.2.4, existe um ideal G-invariante J de Δ tal que $A \otimes_K J = (I)$. Por fim, denotaremos por ψ_R a aplicação induzida

$$R = \mathcal{T}/I \to (A \otimes_K \Delta)/(I) = (A \otimes_K \Delta)/(A \otimes_K J) \simeq A \otimes_K (\Delta/J).$$

Afirmamos que $(\Delta/J, \psi_R)$ é a A-aplicação universal de R. De fato, se considerarmos (Δ, ψ) a A-aplicação universal de $G\{X\}$ (análogo ao que foi obtido no Lema 4.2.7) observamos que $\psi(Id_{Tr}(A)) = (0)$. Do Lema 4.2.8, temos que (Δ, ψ') é a A-aplicação universal de $\mathcal{T}$ e como $\psi' \colon \mathcal{T} \to A \otimes_K \Delta$ satisfaz as condições do Teorema 4.2.2, temos que a conclusão da afirmação segue aplicando novamente o Lema 4.2.8.

Seja $\pi_{(I)} \colon A \otimes_K \Delta \to (A \otimes_K \Delta)/(I) = A \otimes_K (\Delta/J)$ a projeção canônica, segue da Proposição 4.2.13 que $\pi_{(I)}$ é uma aplicação G-linear. Como G é semissimples, temos que $\pi_{(I)}$ levará subanel invariante de $A \otimes_K \Delta$ em subanel invariante de $A \otimes_K (\Delta/J)$, ou seja, $\mathcal{T}$ é enviado sobrejetivamente em $(A \otimes_K (\Delta/J))^G$. Como I é o núcleo dessa aplicação, temos que $\psi_R(R) = (A \otimes_K (\Delta/J))^G$.

Resta provar que ψ_R é injetivo, ou seja, $(I) \cap \mathcal{T} = I$. É óbvio que I está contido em $(I) \cap \mathcal{T}$. Como em [72], utilizaremos o operador de Reynolds para provar a inclusão oposta. Seja a um elemento em $(I) \cap \mathcal{T}$, então existem $m_i \in (I)$ de modo que para cada i há pelo menos um $u_i \in I$ (em qualquer associação de parênteses em A) elemento em m_i. Pelo Corolário 4.3.2 podemos escolher uma variável x que não aparece em nenhum m_i e assim

$$Tr(ax) = Tr\left(\left(\sum_i m_i\right) x\right) = Tr\left(\sum_i (m_i' m_i'' u_i)\right),$$

onde o monômio $m_i' m_i''$ é linear na variável x, para cada i. Aplicando o operador de Reynolds π^G obtemos

$$Tr(ax) = Tr\left(\sum_i \pi^G(m_i' m_i'') u_i\right).$$

Agora, fixando um i qualquer temos que $\pi^G(m_i' m_i'')$ é uma equivariante linear em x. Pelo Teorema 4.3.6 e Corolário 4.3.2 temos

$$\pi^G(m_i' m_i'') = \sum_s Tr(a_{is} x) t_{is} + \sum_k \bar{x}_{ik} w_{ik},$$

onde $t_{is}, w_{ik} \in \mathcal{T}$ e $a_{is}, \bar{x}_{ik}$ são monômios em $K\{X\}$ e x é uma variável em $\bar{x}_{ik}$. Podemos aplicar novamente o Corolário 4.3.2 e teremos

$$\begin{aligned} Tr(ax) &= Tr\left(\sum_i \left(\sum_s (Tr(a_{is}x)t_{is} + \sum_k \bar{x}_{ik}w_{ik}\right) u_i\right) \\ &= Tr\left(\sum_i \left(\sum_s (Tr(t_{is}u_i)a_{is} + \sum_k w_{ik}u_i\bar{x}'_{ik}\right) x\right), \end{aligned}$$

onde $\bar{x}'_{ik}$ é um monômio obtido de $\bar{x}_{ik}$ usando argumentos análogos da demonstração da Proposição 4.3.1 que não tem x como variável. A forma $tr(xy)$ é não degenerada, portanto

$$a = \sum_{i,s}(Tr(t_{is}u_i)a_{is}) + \sum_{i,k} u_i\bar{x}'_k w_{ik}.$$

Como o conjunto I é fechado pela aplicação traço segue que $a \in I$. Portanto, isto completa a prova do teorema. □

Observação 4.3.10. *A hipótese de A ser uma álgebra de dimensão finita associativa ou de Jordan é utilizada para argumentar que a forma $tr(xy)$ é não degenerada (ver Teorema 1.6.4), uma vez que todas as aplicações traço trabalhadas em álgebras de Jordan centrais simples de dimensão finita são obtidas por um traço genérico. Além disso, nessas condições podemos garantir que o grupo dos automorfismo é semisimples (ver Teorema 1.10.21).*

4.4 Aplicação do Teorema 4.3.9: Mergulho em Álgebras de Jordan de uma Forma Bilinear

Em [72], Procesi mostrou que se uma álgebra associativa satisfaz todas as identidades com traço das matrizes $n \times n$, esta álgebra pode ser mergulhada, respeitando o traço, em matrizes $n \times n$. Como as identidades com traço das matrizes $n \times n$ são todas consequências do polinômio de Cayley-Hamilton, o artigo de Procesi teve no seu título a frase "inversa formal do teorema de Cayley-Hamilton". Berele, em [19], obteve um resultado similar para o caso em que A é a álgebra com involução $(M_n(K), *)$. A técnica utilizada na demonstração do teorema principal da seção anterior é muito similar aos métodos empregados por Procesi e Berele em seus resultados, porém generalizamos e provamos para o caso da álgebra de Jordan central simples. Nesta seção iremos focar na aplicação do Teorema 4.3.9 para o caso de álgebra de Jordan de uma forma bilinear.

Denotamos $A = B_n(K)$ a álgebra de Jordan de uma forma bilinear simétrica e não degenerada f sobre um espaço vetorial V de dimensão finita n, sobre um corpo algebricamente fechado de característica zero. Consideramos os polinômios com traço

$$f_2(x) = x^2 - Tr(x)x + (1/2)(Tr(x)^2 - Tr(x^2)) \quad (4.8)$$

$$L_{n+1} = \sum_{\sigma \in S_{n+1}} (-1)^\sigma (x_{\sigma(n+1)} - (1/2)Tr(x_{\sigma(n+1)})) \prod_{k=1}^{n+1} H(x_{\sigma(k)}, y_k), \quad (4.9)$$

onde $L_{n+1} = L(x_1, \cdots, x_n, x_{n+1}, y_1, \cdots, y_n)$ com $n = 2, 3, \cdots$ e

$$H(x, y) = Tr(xy) - (1/2)Tr(x)Tr(y).$$

Em [94], Vasilovskii provou que todas as identidades com traço da álgebra A seguem dos polinômios (4.8) e (4.9). Além disso, na demonstração deste resultado observamos que qualquer polinômio com traço pode ser representado, módulo f_2, na forma

$$\sum \alpha_{\hat{0},1,\ldots,s} \hat{a}_0 Tr(a_1) \cdots Tr(a_s), \tag{4.10}$$

onde a_0, a_1, ..., a_s (com $s \geqslant 0$) são monômios em $K\{X\}$ com a seguinte restrição em seus graus: $deg(a_0) \leqslant 1$, $deg(a_1) \leqslant 2$, para $i = 1, 2, \ldots, s$.

Seja G o grupo dos automorfismos de A, ele é isomorfo ao grupo ortogonal de V relativo a forma f (ver Exemplo 1.7.15). Por fim, os invariantes ortogonais $\varphi\colon V^i \to K$ compatíveis com a forma bilinear canônica $(x, y) = \sum_i x_i y_i$, onde $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$, são expressos em termos desse produto escalar. Mais precisamente, temos o **Primeiro Teorema Fundamental**.

Teorema 4.4.1. *[25, Teorema 5.6] Todo invariante ortogonal de m vetores x_1, ..., x_m pode ser expresso em termos dos m^2 produtos escalares (x_i, x_j).*

Retornamos à discussão do Exemplo 4.1.3 sobre o primeiro teorema fundamental para o caso da álgebra de Jordan A. Queremos descrever a álgebra das funções polinomiais $A^k \to K$ invariantes sob a ação de G. Consideremos uma aplicação polinomial multilinear dada por $\psi\colon A^k \to K$. Temos que

$$\psi(\alpha_1 + v_1, \ldots, \alpha_k + v_k) = \sum \bar{\alpha}_i \psi_i(v_1, \ldots, v_k),$$

onde $\bar{\alpha}_i$ é obtido como produto dos escalares $\alpha_1, \ldots, \alpha_k$. Afirmamos que se ψ é um invariante ortogonal de A, então ψ_i são invariantes ortogonais de V, para todo i. De fato, ψ um invariante ortogonal sobre A implicará

$$\sum \bar{\alpha}_i \psi_i(v_1, \ldots, v_k) = \sum \bar{\alpha}_i \psi_i^g(v_1, \ldots, v_k), \text{ ou seja }, \sum \bar{\alpha}_i(\psi_i - \psi_i^g) = 0$$

para todo $g \in Aut_K(V)$. Por K ser infinito temos a afirmação. Do Teorema 4.4.1, os invariantes ortogonais de V são expressos em termos de produtos escalares de (v_i, v_j) de vetores em V. Além disso, segue da definição do traço e do produto em A que dados $\alpha + v_\alpha$ e $\beta + v_\beta$ elementos em A, teremos $tr(\alpha + v_\alpha) = 2\alpha$ e $(v_\alpha, v_\beta) = (1/2)H(\alpha + v_\alpha, \beta + v_\beta)$.

Deste comentário e da Expressão (4.10), temos que os invariantes $K[A^k]^G$ podem ser expressos em temos dos invariantes Tr X_i e Tr X_iX_j, onde X_i é a projeção equivariante sobre A na i-ésima coordenada. Assim temos o seguinte resultado.

Lema 4.4.2. *A álgebra de Jordan $B_n(K)$ satisfaz a Conjectura 4.1.5.*

Concluímos o objetivo final deste capítulo que podemos enunciar no seguinte teorema. A sua demonstração segue do Teorema 4.3.9 e do Lema 4.4.2.

Teorema 4.4.3. *Seja $A = B_n(K)$ a álgebra de Jordan de uma forma bilinear simétrica e não degenerada f sobre um espaço vetorial V de dimensão finita. Se R é uma álgebra com traço que satisfaça as Identidades (4.8) e (4.9), então R pode ser mergulhada em $A \otimes_K F$, para alguma álgebra comutativa-associativa F. Além disso, se (S, ρ) é a A-aplicação universal de R, então $\rho(R) = (A \otimes S)^G$, onde $G = Aut_K V$.*

Referências

[1] ALJADEFF, E.; HAILE, D.; NATAPOV, M. Graded Identities of Matrix Algebras and the Universal Graded Algebra. **Transactions of the American Mathematical Society**, v. 362, n. 6, p. 3125–3147, 2010.

[2] ALJADEFF, E.; KANEL-BELOV, A. Representability and Specht Problem for G-Graded Algebras. **Advances in Mathematics**, v. 225, n. 5, p. 2391–2428, 2010.

[3] ALJADEFF, E.; KARASIK, Y. Crossed Products and their Central Polynomials. **Journal of Pure and Applied Algebra**, v. 217, n. 9, p. 1634–1641, 2013.

[4] ALJADEFF, E.; DAVID, O. On Regular G-Gradings. **Transactions of the American Mathematical Society**, v. 367, n. 6, p. 4207–4233, 2015.

[5] ALVES, S. M.; BRANDAO JR, A. P.; KOSHLUKOV, P. Graded Central Polynomials for T-prime Algebras. **Communications in Algebra**, v. 37, n. 6, p. 2008–2020, 2009.

[6] AMITSUR, S. A.; LEVITZKI, J. Minimal Identities for Algebras. **Proceedings of the American Mathematical Society**, v. 1, n. 4, p. 449–463, 1950.

[7] AMITSUR, S. A. Identities in Rings with Involutions. **Israel Journal of Mathematics**, v. 7, n. 1, p. 63–68, 1969.

[8] ______.A Noncommutative Hilbert Basis Theorem and Subrings of Matrices. **Transactions of the American Mathematical Society**, v. 149, n. 1, p. 133–142, 1970.

[9] ______. Embeddings in Matrix Rings. **Pacific Journal of Mathematics**, v. 36, n. 1, p. 21–29, 1971.

[10] ARTIN, M. On Azumaya Algebras and Finite Dimensional Representations of Rings. **Journal of Algebra**, v. 11, n. 4, p. 532–563, 1969.

[11] BAHTURIN, Y. A.; SEHGAL, S. K.; ZAICEV, M. V. Group Gradings on Associative Algebras. **Journal of Algebra** v. 241, n. 2, p. 677–698, 2001.

[12] BAHTURIN, Y. A.; DRENSKY, V. Graded Polynomial Identities of Matrices. **Linear Algebra and its Applications**, v. 357, n. 1–3, p. 15–34, 2002.

[13] BAHTURIN, Y. A.; REGEV, A. Graded Tensor Products. **Journal of Pure and Applied Algebra**, v. 213, n. 9, p. 1643–1650, 2009.

[14] BAHTURIN, Y. A.; DINIZ, D. Graded Identities of Simple Real Graded Division Algebras. **Journal of Algebra**, 2017.

[15] BAHTURIN, Y. A.; ZAICEV, M. Graded Algebras and Graded Identities. **Lecture Notes in Pure and Applied Mathematics**, p. 101–140, 2003.

[16] ______. Simple Graded Division Algebras over the Field of Real Numbers. **Linear Algebra and its Applications**, v. 490, p. 102–123, 2016.

[17] ______. Graded Division Algebras over the Field of Real Numbers. **arXiv preprint arXiv:1611.04000**, 2016. - to appear

[18] BELOV, A. Y. No Associative PI-Algebra Coincides with its Commutant. **Siberian Mathematical Journal**, v. 44, n. 6, p. 969–980, 2003.

[19] BERELE, A. Matrices with Involution and Invariant Theory. **Journal of Algebra**, v. 135, n. 1, p. 139–164, 1990.

[20] BRANDÃO JR., A. P.; KOSHLUKOV, P. Central Polynomials for $\mathbb{Z}_2$-Graded Algebras and for Algebras with Involution. **Journal of Pure and Applied Algebra**, v. 208, n. 3, p. 877–886, 2007.

[21] BRANDÃO JR., A. P.; KOSHLUKOV, P.; KRASILNIKOV, A.; SILVA, É. A. da. The Central Polynomials for the Grassmann Algebra. **Israel Journal of Mathematics**, v. 179, n. 1, p. 127–144, 2010.

[22] CHEVALLEY, C. Classification des Groupes de Lie Algébriques, **Seminaire**, Ecole Normale Superieur, 1956–1958, 2 Vols. (mimeographed).

[23] COLOMBO, J.; KOSHLUKOV, P. Central Polynomials in the Matrix Algebra of Order Two. **Linear Algebra and its Applications**, v. 377, p. 53–67, 2004.

[24] CURTIS, C. W.; REINER, I. **Representation Theory of Finite Groups and Associative Algebras**. American Mathematical Society, v. 356, 1966.

[25] DE CONCINI, C.; PROCESI, C. A Characteristic Free Approach to Invariant Theory. **Advances in Mathematics**, v. 21, n. 3, p. 330–354, 1976.

[26] DEHN, M. Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme. In: **Festschrift David Hilbert zu Seinem Sechzigsten Geburtstag am 23. Januar 1922**. Berlin, Heidelberg, 1922. p. 184–194.

[27] DI VINCENZO, O. M. On the Graded Identities of $M_{1,1}(E)$. **Israel Journal of Mathematics**, v. 80, n. 3, p. 323–335, 1992.

[28] DI VINCENZO, O. M.; NARDOZZA, V. Graded Polynomial Identities for Tensor Products by the Grassmann Algebra. **Communications in Algebra**, v. 31, n. 3, p. 1453–1474, 2003.

[29] DI VINCENZO, O. M.; DA SILVA, V. R. T. On $\mathbb{Z}_2$-Graded Polynomial Identities of the Grassmann Algebra. **Linear Algebra and its Applications**, v. 431, n. 1–2, p. 56–72, 2009.

[30] DINIZ, D. **Identidades Graduadas em Álgebras Não-Associativas**. 2010. Tese de Doutorado (Doutorado em Matemática) - Departamento de Matemática, UNICAMP, Campinas, 2010.

[31] ______. A Primeness Property for Central Polynomials of Verbally Prime PI-Algebras. **Linear and Multilinear Algebra**, v. 63, n. 11, p. 2151–2158, 2015.

[32] DINIZ, D.; DE MELLO, T. C. Graded Identities of Block-Triangular Matrices. **Journal of Algebra**, v. 464, p. 246–265, 2016.

[33] DINIZ, D.; BEZERRA JR., C. F. Primeness Property for Graded Central Polynomials of Verbally Prime Algebras. **Journal of Pure and Applied Algebra**, 2017.

[34] DINIZ, D.; BEZERRA JR., C. F.; MOTA, S. Identities and Central Polynomials of Real Graded Division Algebras. **International Journal of Algebra and Computation**, 2017.

[35] DRENSKY, V. S. A Minimal Basis of Identities for a Second-Order Matrix Algebra over a Field of Characteristic 0. **Algebra and Logic**, v. 20, n. 3, p. 188–194, 1981.

[36] ______. **Free Algebras and PI-Algebras: Graduate Course in Algebra**. Springer Verlag, 2000.

[37] DRENSKY, V.; KOSHLUKOV, P. Weak Polynomial Identities for a Vector Space with a Symmetric Bilinear Form, **Mathematics and Education in Mathematics**. p. 213–219, 1987.

[38] ______. Polynomial Identities for Jordan Algebras of Degree Two. **Journal Indian Mathematical Society**, v. 55, n. 7, p. 1–30, 1990.

[39] DRENSKY, V.; FORMANEK, E. **Polynomial Identity Rings**. Birkhäuser, 2012.

[40] ELDUQUE, A.; KOCHETOV, M. **Gradings on Simple Lie Algebras**. Providence, RI: American Mathematical Society, v. 189. 2013.

[41] FOGARTY, J. **Invariant Theory**. WA Benjamin, 1969.

[42] FORMANEK, E. Central Polynomials for Matrix Rings. **Journal of Algebra**, v. 23, n. 1, p. 129–132, 1972.

[43] GIAMBRUNO, A.; ZAICEV, M. **Polynomial Identities and Asymptotic Methods**. American Mathematical Society, 2005.

[44] HUMPHREYS, J. E. **Linear Algebraic Groups**. Springer Science & Business Media. v. 21, 2012.

[45] ILTYAKOV, A. V. Specht Ideals of Identities of Certain Simple Nonassociative Algebras. **Algebra and Logic**, v. 24, n. 3, p. 210–228, 1985.

[46] ______. Trace Polynomials and Invariant Theory. **Geometriae Dedicata**, v. 58, n. 3, p. 327–333, 1995.

[47] ______. On Invariants of the Group of Automorphisms of Albert Algebras. **Communications in Algebra**, v. 23, n. 11, p. 4047–4060, 1995.

[48] ______. **On Generators of the Algebra of Polynomial Invariants of Group F_4**. University of Sydney. School of Mathematics and Statistics, 1997.

[49] JACOBSON, N. **Structure of Rings**. American Mathematical Society Colloquium Publications. v. 37, 1956.

[50] ______. **Structure and Representations of Jordan Algebras**. American Mathematical Society Colloquium Publications. v. 39, 1968.

[51] ______. **Lie Algebras**. Courier Corporation, 1979.

[52] ______. Some Groups of Transformations Defined by Jordan Algebras, II. Groups of type F_4. In: **Nathan Jacobson Collected Mathematical Papers**. Birkhäuser Boston. p. 406–430, 1989.

[53] ______. **Basic Algebra I**. Courier Corporation, 2012.

[54] ______. **Basic Algebra II:** Second Edition. Dover Publications, 2012. (Dover Books on Mathematics).

[55] KAPLANSKY, I. Rings with a Polynomial Identity. **Bulletin of the American Mathematical Society**, v. 54, n. 6, p. 575–580, 1948.

[56] ______. Problems in the Theory of Rings. **Report of a Conference on Linear Algebras**, Long Island, New York, June, 1956, National Academy of Sciences. National Research Council Publication 502, pp. 1–3.

[57] KEMER, A. R. Varieties and $\mathbb{Z}_2$-Graded Algebras. **Mathematics of the USSR-Izvestiya**, v. 25, n. 2, p. 359–374, 1985.

[58] ______. Finite Basis Property of Identities of Associative Algebras. **Algebra and Logic**, v. 26, n. 5, p. 362–397, 1987.

[59] ______. **Ideals of Identities of Associative Algebras**, Translations of Mathematical Monographs, v. 87 of In: American Mathematical Society, Providence, RI, 1991.

[60] KNUS, M.-A.; MERKURJEV, A.; ROST, M.; TIGNOL, J.-P. **The Book of Involutions**. v. 44 of In: American Mathematical Society Colloquium Publications, Providence, 1998.

[61] KOSHLUKOV, P. Polynomial Identities for a Family of Simple Jordan Algebras. **Communications in Algebra**, v. 16, n. 7, p. 1325–1371, 1988.

[62] ______. Basis of the Identities of the Matrix algebra of Order Two Over a Field of Characteristic $p \neq 2$. **Journal of Algebra**, v. 241, n. 1, p. 410–434, 2001.

[63] KOSHLUKOV, P.; DINIZ, D. 2-Graded Polynomial Identities for the Jordan Algebra of the Symmetric Matrices of Order Two. **Journal of Algebra**, v. 327, n. 1, p. 236–250, 2011.

[64] LATYSHEV, V. N. On the Choice of Basis in a T-ideal. **Sibirskii Matematicheskii Zhurnal**, v. 4, n. 5, p. 1122–1126, 1963.

[65] MAKAR-LIMANOV, L. On Grassmann Algebras of Graphs. **Journal of Algebra**, v. 87, n. 2, p. 283–289, 1984.

[66] NASTASESCU, C.; VAN OYSTAEYEN, F. **Methods of Graded Rings**. Springer, 2004.

[67] OKHITIN, S. Central Polynomials of an Algebra of Second-Order Matrices. (Russian), Vestnik Moskovskogo Universiteta, Seriya I Matematika, Mekhanika 1988, no. 4, 61–63; English translation: **Moscow University Mathematics Bulletin**, v. 43, p. 49–51, 1988.

[68] PLATONOV, V. P.; RAPINCHUK, A. S.; ROWEN, R. **Algebraic Groups and Number Theory**. Academic Press, v. 139, 1993.

[69] POPOV, A. P. Identities of the Tensor Square of the Grassman Algebra. **Algebra and Logic**, v. 21, n. 4, p. 296–316, 1982.

[70] POPOV, V. L. An Analogue of M. Artin's Conjecture on Invariants for Nonassociative Algebras. **Translations of the American Mathematical Society-Series 2**, Providence, v. 169, p. 121–144, 1995.

[71] PROCESI, C. The Invariant Theory of $n \times n$ Matrices. **Advances in Mathematics**, v. 19, n. 3, p. 306–381, 1976.

[72] ______. A Formal Inverse to the Cayley-Hamilton Theorem. **Journal of Algebra**, v. 107, n. 1, p. 63–74, 1987.

[73] RAZMYSLOV, J. P. On a Problem of Kaplansky. **Mathematics of the USSR-Izvestiya**, v. 7, n. 3, p. 479–496, 1973.

[74] ______. Trace Identities of Full Matrix Algebras Over a Field of Characteristic Zero. **Mathematics of the USSR-Izvestiya**, v. 8, n. 4, p. 727–760 , 1974.

[75] RAZMYSLOV, Yu P. Finite Basing of the Identities of a Matrix Algebra of Second Order Over a Field of Characteristic Zero. **Algebra and Logic**, v. 12, n. 1, p. 47–63, 1973.

[76] ______. Trace Identities and Central Polynomials in the Matrix Superalgebras $M_{n,k}$. **Sbornik: Mathematics**, v. 56, n. 1, p. 187–206, 1987.

[77] ______. **Identities of Algebras and Their Representations**. Translations of Mathematical Monographs, American Mathematical Society, Providence, 1994. v. 138.

[78] REGEV, A. A Primeness Property for Central Polynomials. **Pacific Journal of Mathematics**, v. 83, n. 1, p. 269–271, 1979.

[79] REGEV, A.; SEEMAN, T. Z_2-Graded Tensor Products of PI-Algebras. **Journal of Algebra**, v. 291, n. 1, p. 274–296, 2005.

[80] ROBINSON, D. **A Course in the Theory of Groups**. Springer Science & Business Media, 2012. v. 80.

[81] RODRIGO-ESCUDERO, A. Classification of Division Gradings on Finite-Dimensional Simple Real Algebras. **Linear Algebra and its Applications**, v. 493, p. 164–182, 2016.

[82] ROWEN, L. H. **Polynomial Identities in Ring Theory**. Academic Press, 1980. v. 84.

[83] SAMOILOV, L. M. On the Primality Property of Central Polynomials of Prime Varieties of Associative Algebras. **Mathematical Notes**, v. 99, n. 3–4, p. 413–416, 2016.

[84] SANTOS, W. F.; RITTATORE, A. **Actions and Invariants of Algebraic Groups**. Chapman & Hall/CRC Press. v. 269, 2005.

[85] SCHARLAU, W. **Quadratic and Hermitian Forms**. Springer Science & Business Media, 2012. v. 270.

[86] SCHEUNERT, M. Generalized Lie Algebras. **Journal of Mathematical Physics**, v. 20, n. 4, p. 712–720, 1979.

[87] SCHWARZ, G. W. Invariant Theory of G_2. **Bulletin (New Series) of the American Mathematical Society**, v. 9, n. 3, p. 335–338, 1983.

[88] SMALL, L. W. An Example in PI-Rings. **Journal of Algebra**, v. 17, n. 3, p. 434–436, 1971.

[89] SPECHT, W. Gesetze in Ringen. I. **Mathematische Zeitschrift**, v. 52, n. 1, p. 557–589, 1950.

[90] STEWART, I. Tensorial Extensions of Central Simple Algebras. **Journal of Algebra**, v. 25, n. 1, p. 1–14, 1973.

[91] SVIRIDOVA, I. Identities of PI-Algebras Graded by a Finite Abelian Group. **Communications in Algebra**, v. 39, n. 9, p. 3462–3490, 2011.

[92] VASILOVSKY, S. Yu. Basis of Identities of a Three-Dimensional Simple Lie Algebra over an Infinite Field. **Algebra and Logic**, v. 28, n. 5, p. 355–368, 1989.

[93] ______. A Finite Basis for Polynomial Identities of the Jordan Algebra of a Bilinear Form. **Siberian Advances in Mathematics**, v. 1, n. 4, p. 1–45, 1991.

[94] ______. Trace Identities of the Jordan Algebra of a Bilinear form. **Siberian Mathematical Journal**, v. 32, n. 6, p. 19–23, 1991.

[95] WAGNER, W. Über Die Grundlagen der Projektiven Geometrie und Allgemeine Zahlensysteme. **Mathematische Annalen**, v. 113, n. 1, p. 528–567, 1937.

[96] WALL, C. T. C. Graded Brauer Groups. **Journal für die reine und angewandte Mathematik**, v. 213, n. 2013, p. 187–199, 1964.

[97] ZHEVLAKOV, K. A.; SLIN'KO, A. M.; SHESTAKOV, I.P.; SHIRSHOV, A. I.; **Rings that are Nearly Associative**. v. 104, Academic Press, Inc., 1982.