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

Identidade de Cayley-Hamilton para álgebras de matrizes

por

José Lucas Galdino da Silva †

sob orientação do

Prof. Dr. Claudemir Fidelis Bezerra Júnior

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

† Este trabalho contou com apoio financeiro da CAPES por meio do programa PICME.

Identidade de Cayley-Hamilton para álgebras de matrizes

por

José Lucas Galdino da Silva

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

Área de Concentração: Matemática

Aprovada por:

Alex R. Borges

Prof. Dr. Alex Ramos Borges - UPE

Prof. Dr. Charles Aparecido de Almeida - UFMG

Diogo Diniz P.S. Silva

Prof. Dr. Diogo Diniz Pereira da Silva e Silva - UFCG

Prof. Dr. Claudemir Fidelis Bezerra Júnior - UFCG

Orientador

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

Março/2020

Agradecimentos

"Isto é uma ordem: sê firme e corajoso. Não te atemorizes, não tenhas medo, porque o Senhor está contigo em qualquer parte para onde fores." (Josué 1, 9)

É utópico achar que neste espaço poderei expressar tudo o que sinto ao chegar aqui, bem como que irei lembrar de todas as pessoas e de cada momento específico. Todavia, o pouco que aqui será registrado demonstra uma parte do quanto meu coração sente-se grato a cada pessoa e a cada momento, seja bom ou ruim. Tudo, exatamente tudo, foi de extrema importância para chegar aqui.

Inicio agradecendo a mim, pois sei o quanto foi difícil. Ao escrever esses agradecimentos é impossível não lembrar dos dias em que fiquei mais de 10 horas seguidas estudando, das noites mal dormidas, tensões, medos, etc. Mas ver que com tudo isso pude alcançar esse momento, sinto-me imensamente orgulhoso.

Agradeço aos meus pais e minha irmã. Ao meu pai por sempre ter dado seu grande incentivo a mim. Desde criança quando ele buscava livros no lixo para que eu pudesse estudar, até mesmo no decorrer de minhas primeiras séries me dando pequenas aulas de inglês, com o básico que ele sabia, até hoje, onde mesmo sem entender nada que eu estudo, todos os dias me acordou bem cedo trazendo café com leite, e ainda ia me levar no ponto de ônibus. À minha mãe, pois mesmo já não tendo tanto amor pelos estudos devido à falta de condições financeiras quado era mais nova, ensinou-me sobre a maior riqueza que alguém pode ter: o conhecimento, pois ninguém nunca roubará isso de mim. Agradeço a ela por ter chorado junto comigo muitas vezes, por ter torcido, ter sido apoio, por ter estado ao meu lado. À minha irmã, por ter sido minha confidente em vários momentos, por até mesmo apostar dinheiro que eu passaria no mestrado e por ter sido alguém que sempre acreditou em meu potencial. Aproveito aqui para agradecer a Rafael, meu cunhado, por ter me ajudado sempre que precisei.

Quero aqui também agradecer a todos os meus professores, desde a minha primeira professora, Marlene, até os da Universidade. Sei que toda a base existente em mim hoje foi construída desde lá atrás, onde em aulas de diversas disciplinas pude aprender muito e tornar-me mais humano. Em particular, desejo agradecer aos meus professores na graduação, aqui desejo citar Lindomberg e Luiz Antônio, os quais foram meus tutores do PET Matemática e Estatística, por terem me incentivado a nunca desistir dos meus sonhos. Também agradeço a cada professor da pós-graduação Brandão, Leomarques, Marcelo, Diogo, Claudianor, que em suas aulas me fizeram apaixonar-me ainda mais pela Matemática. Agradeço, em particular, ao professor Brandão que no curso de verão 2019 me fez ganhar ainda mais gosto pela matemática e ao professor Diogo que com os seminários nos dois últimos períodos do mestrado me fez aumentar o meu conhecimento em Álgebra avançada.

Ao meu orientador, professor Claudemir, por ter desde os primeiros dias do mestrado me procurado e falado tão bem da Álgebra a ponto de ter me levado a mudar de área de estudo. Agradeço a ele por cada conversa, café, discussões (tanto de Matemática, quanto da vida), cresci muito nesse tempo e espero que nossa relação seja ainda mais intensa a partir de agora.

Agradeço a todos da UAMat, desde funcionários (limpeza, coordenação, secretaria, etc.) até aos alunos, em especial meus colegas de turma por todo o apoio de sempre, bem como pelas discussões matemáticas: Daniela, Geisa, Lucas, Oliverio, Renan, Caio, Ismael e Siebra. Cresci muito nesses 6 anos aqui (4 de graduação e 2 de mestrado) e espero nos próximos 4 de doutorado crescer ainda mais. Também acrescento aqui os alunos da graduação (por serem muitos, omitirei nomes) e do doutorado (Weiller, Pedro, Laíse, Franciélia, Geovany e Wallace) por cada discussão, risadas e apoio.

Agradeço a Bruna e Yasmim, as quais foram minhas diretoras por 3 anos na Escola Estadual Antônio Galdino Filho. Sou eternamente grato por todo ensinamento que obtive lá. Em muitos momentos ver o que quanto todo o corpo daquela escola acreditava em mim, me deu forças para lutar. Aqui também não posso deixar de agradecer aos meus alunos (agora ex-alunos), por muitas das vezes acreditarem em mim mais do que eu mesmo. Eles me fizeram em vários momentos rir, mesmo quando passava por dificuldades. Em especial cito Joelson, Alfredo, Isaac, Sabrina, Mengla, Viviane e Beatriz, estes são ex-alunos que hoje cursam matemática na UFCG (exceto uma que é na UEPB e uma que estuda Estatística na UEPB). Vê-los seguindo o caminho da Matemática me motiva ainda mais a estudá-la.

Agradeço aos integrantes do Grupo de Oração Rosa Mística, estiveram comigo desde o Ensino Médio e até hoje estão. Sou grato a cada um que rezou por mim e me deu grande apoio durante todos os momentos do mestrado. Jamais nego: a garra que tenho, a pessoa que sou devo, em sua grande maioria, a esse Grupo de Oração. Aqui abro um parêntese para agradecer a Gracilene, Edna, Assunção, Carla, Thaisa, Angela e Glazy, estas integraram a coordenação junto comigo durante um tempo e foram as que compartilhei minhas dores, aflições, angústias e medos. Obrigado por terem sido um grande apoio e suporte para mim.

Aqui cito também alguns amigos que a vida foi me dando. Rennaly, uma grande irmã que tenho, com seu exemplo e empenho na vida acadêmica me incentiva a não desistir dos meus sonhos, por mais difícil que seja lutar por eles. Agradeço a Jorge, meu amigo e professor de Inglês, por cada discussão, conversa, bate boca, etc. Somos extremamente reflexivos e ele me ajudou a sair de vários fundos do posso em nossas ligações. Também agradeço a Padre Saulo pelas vezes em que ouviu meus desabafos durante a seleção do doutorado e por sempre dizer que acreditava em meu potencial, aqui abro um espaço para agradecer a ele pela oportunidade de estar a frente do coral em sua paróquia, pois em cada ensaio eu me desestressava e ganhava ânimo para estudar ainda mais.

Além dos já citados no parágrafo anterior, me aproximei de Luciana (minha tia), por ver nela uma grande modelo de amor pela profissão. Ela para mim é um exemplo, uma vez que foi a primeira da minha família a concluir uma graduação. Ademais, agradeço também a Ênnia, com a qual fiz terapia durante 2 meses. Seus conselhos estou pondo em prática e desejo pô-los para a vida inteira.

Além disso, não posso jamais me esquecer do GOU (Grupo de Oração Universitário) da UFCG. Durante a graduação foi um grande suporte para mim, muitas amizades que ali tive me estimularam a seguir a carreira acadêmica.

Sei que já citei o nome de colegas de turma, mas neste parágrafo enfatizo duas grandes amigas que o mestrado me proporcionou: Daniela e Geisa. Muitas conversas, fofocas, risadas, choros, etc., foram compartilhados juntos. Obrigado a vocês por sempre me darem força e por acreditarem em mim. Os seus conselhos levarei para a vida inteira.

Agradeço ao professor Dr. Charles Aparecido de Almeida, ao professor Dr. Alex

Ramos Borges e ao professor Dr. Diogo Diniz Pereira da Silva e Silva por terem aceitado participar da banca.

À Capes, através do programa PICME, por todo o apoio financeiro.

Por fim, uma vez que os últimos são os primeiros, finalizo agradecendo ao Ser mais importante de minha vida, aquele que me deu a vida e me sustentou cada segundo desde o dia 12 de março, em que comecei o mestrado. Sem Ele, não teria chegado aqui. Obrigado meu Deus por ter me sustentado, quando caí. Por ter me orientado e me guiado, mesmo quando não sabia o que fazer, nem o que dizer, nem para onde ir. Sem dúvidas, esse mestrado é graça tua! Toda honra e toda glória sejam dadas a Ti.

“Ontem o menino que brincava me falou
Que hoje é semente do amanhã
Para não ter medo que esse tempo vai passar
Não se desespere, nem pare de sonhar
Nunca se entregue, nasça sempre com as manhãs
Deixe a luz do sol brilhar no céu do seu olhar
Fé na vida, fé no homem, fé no que virá
Nós podemos tudo
Nós podemos mais
Vamos lá fazer o que será.”
(Sementes do Amanhã - Erasmo Carlos)

Dedicatória

Aos meus pais, Lúcia de Fátima e Antônio Antero (Tota), e a minha irmã, Ana Lívia.

Resumo

Sobre um corpo K de característica zero, estudamos nesta dissertação a álgebra das matrizes, $M_n(K)$, sob dois pontos de vista: primeiramente as suas identidades com traço (usando por base a teoria de invariantes) e, em um segundo momento, vemos condições para a realização de mergulhos nesta álgebra, vendo-a como um anel. Sendo mais específicos, estudamos a natureza do anel das invariantes de $M_n(K)$, sob a ação diagonal do grupo geral linear, bem como, a caracterização deste anel como aplicações que dependem do traço. Por conseguinte, provaremos que todas as identidades com traço para $M_n(K)$ podem ser obtidas de um polinômio denominado "polinômio de Cayley-Hamilton de grau n", além do mesmo satisfazer a propriedade de Specht. Por fim, utilizando uma certa aplicação universal, estabelecemos uma condição de existência de mergulho sobre o anel de matrizes de ordem n. Com esses estudos concluídos, obtemos que toda álgebra nil de índice limitado n é subanel de $M_n(C)$, para algum anel comutativo C.

Palavras-chave: Álgebra com traço, identidades polinomiais com traço, mergulho, invariantes de matrizes, polinômio de Cayley-Hamilton.

Abstract

Over a field K of characteristic zero, we study in this dissertation the matrix algebras, $M_n(K)$, from two points of view: firstly its trace identities - using the Invariant Theory as a basis - and, secondly, we provide the conditions for the realization of embeddings in this algebra, seeing it as a ring. Being more specific, we study the nature of the invariants of $M_n(K)$, under the diagonal action of the general linear group, as well as the characterization of this ring as applications that depend of trace maps. Furthermore, we prove that all trace identities can be obtained by one called the "Cayley-Hamilton polynomial of degree n", and also we prove that this ideal satisfies the Specht property. Lastly, using certain universal maps, we establish a condition for the existence of embeddings on the ring matrix of order n. With these results, we conclude that every nil algebra of bounded index n is a subring of $M_n(C)$, for some commutative ring C.

Keywords: Trace algebras, trace identities, trace preserving embedding, invariants of matrices, Cayley-Hamilton polynomial.

Conteúdo

Introdução

O estudo das PI-álgebras, ou álgebras com identidades polinomiais, é bastante amplo e de rápida expansão na matemática. 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 $f(a_1, \ldots, a_n) = 0$. Se existir um polinômio f não nulo com esta propriedade, 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.

O estudo das PI-álgebras foi iniciado por volta de 1930 com os trabalhos de Dehn [11] e Wagner [41]. Nestes, embora implícito, aparecem identidades polinomiais para álgebras das matrizes de ordem 2. O termo "identidade polinomial" foi escrito de modo explícito no trabalho de Kaplansky [24] em 1948. Neste trabalho, Kaplansky demonstrou que qualquer PI-álgebra primitiva é central simples e de dimensão finita sobre seu centro, tal resultado ficou conhecido como "O Teorema de Kaplansky". Em 1950, Amitsur e Levitzki [3] provaram que o polinômio dito "Standard" de grau $2n$ é uma identidade de grau mínimo para a álgebra de matrizes de ordem n. No mesmo ano Specht [38] 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. O problema de Specht pode ser enunciado de outras maneiras equivalentes, como por exemplo: todo ideal de identidades polinomiais na álgebra associativa livre é finitamente gerado como ideal de identidades, ou, de forma equivalente, se toda cadeia ascendente de ideais de identidades estabiliza. Observamos que tal forma do problema de Specht se assemelha à propriedade Noetheriana da álgebra dos polinômios comutativos nas variáveis x_1, $\ldots$, x_n. Este passou a ser um problema central na teoria, motivando boa parte do seu desenvolvimento.

Em [26, 25], 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. Por este motivo, se vê nas últimas décadas que várias generalizações do conceito de identidade polinomial têm sido estudadas tais como: identidades polinomiais graduadas, com involução, com involução graduada, entre outras. Uma dessas ramificações que merece destaque neste trabalho são as identidades polinomiais com traço por sua íntima interligação com a Teoria de Invariantes. Tais identidades foram estudadas com detalhes por Procesi [29] e Razmyslov [32] de forma independente, embora quase simultaneamente; como consequência dos resultados obtidos, Razmyslov deu uma nova demonstração do Teorema de Amitsur e Levitzki.

Iremos agora comentar as relações entre a teoria de invariantes e as identidades com traço. Em 1969, Artin conjecturou um problema sobre a natureza das invariantes em álgebra de matrizes de ordem n sobre um corpo de característica zero. Mais precisamente, considerando o grupo geral linear, Artin conjecturou que o anel dos invariantes das Matrizes, sob a ação diagonal deste grupo, são aplicações polinomiais que dependem da aplicação traço usual [4]. Para $n = 2$, tal resultado é clássico ([19]); e, Spencer e Rivlin ([35, 36, 37]) provaram tal resultado para invariantes ortogonais de matrizes simétricas de ordem 3. No caso geral, Procesi [29] dá uma resposta afirmativa para tal conjectura e tal resultado é um dos objetos de estudo desta dissertação.

Assim, as identidades com traço nas álgebras matriciais foram estudadas e descritas independentemente por Procesi [29] e Razmyslov [32]. 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. Neste contexto, 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. A respeito do uso da teoria de invariantes podemos citar o uso dessas técnicas pelos autores: Berele [6, 5, 7, 8]; o próprio Procesi em [29] e [30], citamos novamente [29] por se tratar da descrição das invariantes e identidades com traço para álgebra de matrizes com involução; e no artigo recente [15] dos autores Fidelis, Diniz e Koshlukov.

Além dos já citados problemas que envolvem teoria de anel e invariantes, temos questões que envolvem caracterizações de subanéis de um anel dado. Uma importante questão que vem intrigando muitos matemáticos é a caracterização de subanéis de anéis de matrizes. Mais precisamente: "Qual condição é necessária para que um anel seja subanel de $M_n(C)$, a álgebra das matrizes de ordem n sobre um anel comutativo C, para algum $n \in \mathbb{N}$?". Sabe-se há muito tempo que as PI-álgebras não precisam ser imersas em $M_n(C)$, 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 [1] e Small [34] produziram contra-exemplos para a última afirmação.

Uma resposta completa para o problema de mergulho anterior não é conhecida, porém Procesi [30] 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 [6] obteve um resultado análogo ao de Procesi 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.

Recentemente Fidelis, Diniz e Koshlukov [15] generalizaram os resultados de Berele e Procesi e os ampliaram para as álgebras de Jordan de uma forma bilinear não degenerada. Tais resultados estão relacionados à teoria dos grupos algébricos lineares e, portanto, considerar o corpo base sendo de característica zero é essencial.

Esta dissertação contém três capítulos. No primeiro capítulo serão introduzidos conceitos base para toda a leitura do nosso trabalho. Iniciamos com a definição de

Álgebra e Módulo e, posteriormente, incluímos as definições básicas da PI teoria. Tendo em vista que o capítulo dois utiliza a Teoria de Invariantes, trazemos alguns conceitos básicos dessa teoria como o processo de polarização e restituição, ação de grupo e a definição de funções polinomiais invariantes.

No capítulo dois, tomando por base o artigo [29] de autoria de C. Procesi intitulado "The Invariant theory of $n \times n$ Matrices", estudamos a natureza das invariantes das matrizes de ordem n. Além disso, estabeleceremos uma relação entre as invariantes e as concomitantes de matrizes de ordem n sobre um corpo de característica zero. E, ao final deste capítulo, mostraremos que todas as identidades com traço da álgebra das matrizes de ordem n são consequência do polinômio chamado "Cayley-Hamilton", e consequentemente obtemos tais relações entre invariantes e concomitantes.

No último capítulo deste trabalho de dissertação, tendo por base os artigos [2] e [30], estudaremos com mais detalhes o problema de mergulhos de álgebras em $M_n(C)$, onde C é um anel comutativo. Aqui iremos considerar a classe das álgebras associativas com traço. Como consequência do capítulo dois, obteremos que uma condição suficiente para que haja o mergulho é que tal anel satisfaça a identidade de Cayley-Hamilton de grau n. Um resultado que responde, de maneira parcial, o caso geral é que toda álgebra nil de índice limitado n é subálgebra de álgebra de matrizes de ordem n sobre algum anel comutativo. Não podemos esquecer de mencionar que, baseado no artigo [15], obtemos que todo T-ideal que preserva traço formal que possui a identidade de Cayley-Hamilton possui base finita. Esse resultado é um análogo do problema de Specht para o ideal de todas as identidades com traço para $M_n(K)$.

Por fim, é importante mencionar novamente que os resultados obtidos nos Capítulos 2 e 3 são sobre um corpo de característica zero, e tal condição é necessária para que os resultados da teoria funcionem de modo satisfatório. Embora tais resultados sejam da década de 70, podemos informar que esses ainda trazem ferramentas importantes fortemente utilizadas em ambas teorias. Com isso, acreditamos que este trabalho será uma forte fonte de consulta para estudos futuros na área.

Capítulo 1

Preliminares

Neste capítulo estabeleceremos a linguagem que será adotada no decorrer deste trabalho e, para isso, apresentaremos conceitos básicos e resultados que serão a base do mesmo. Em vista de uma melhor organização do texto, assumiremos que o leitor conheça os conceitos e resultados básicos de Álgebra Linear, bem como da teoria de grupos, anéis e corpos. Para um leitor interessado em um estudo mais detalhado desses conceitos e resultados, indicamos as referências [16], [20] e [21].

Neste capítulo teremos nove seções, as quais podemos dividir em duas partes, onde a primeira será uma espécie de preliminar geral para toda dissertação e a segunda uma introdução a teoria de invariantes, sendo base especialmente para o Capítulo 2.

Inicialmente estudaremos o conceito de álgebras e de módulos sobre álgebras, vendo seus exemplos e resultados mais importantes para o nosso texto. Posteriormente, faremos uma pequena exposição da teoria de Young, onde definiremos o simetrizador de Young e ainda apresentaremos os conceitos de álgebra livre, identidades polinomiais e álgebra com traço. Além disso, estudaremos as identidades de Newton, tomando por base o livro [18].

Da seção seis à seção nove, teremos como texto base o livro [31] e nelas recordaremos a definição de ação de grupos, dando exemplos de ações que irão ser utilizadas aqui, e definiremos o conceito de funções invariantes. Ainda, utilizando tal material, faremos um rápido aprofundamento de métodos bastante usados na teoria de invariantes, que são: a polarização e a restituição.

No decorrer de todo texto, K denotará um corpo e, a menos que seja mencionado o contrário, todas as álgebras e espaços vetoriais serão definidos sobre K. Além disso, $charK$ denotará a característica do corpo K.

1.1 Álgebras

Nosso objetivo nesta seção será definir uma estrutura chamada de **álgebra** e estudar suas propriedades básicas, uma vez que nela construiremos o ambiente base de nosso trabalho.

Definição 1.1.1 *Dado A um espaço vetorial, dizemos que o par $(A, *)$ é uma* ***álgebra*** *(ou K-álgebra) se $*$ é uma forma bilinear, ou seja, $* : A \times A \to A$ satisfaz:*

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

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

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

para quaisquer $a, b, c \in A$ e $\lambda \in K$. Neste caso, "$*$" é uma operação em A.

Observação 1.1.2 *A fim de simplificar as nossas notações, denotaremos a álgebra $(A, *)$ simplesmente por A, o produto $a * b$, para $a, b \in A$, por ab e, por fim, iremos utilizar simplesmente o termo álgebra ao invés de K-álgebra.*

A operação $*$ definida acima é chamada multiplicação e definimos a multiplicação de três elementos como $a_1a_2a_3 = (a_1a_2)a_3$ e, indutivamente, o produto de $n + 1$ elementos de A da seguinte maneira:

$$a_1a_2 \cdots a_na_{n+1} = (a_1a_2 \cdots a_n)a_{n+1}, \text{ para } a_i \in A.$$

Neste momento é natural indagarmos se todo espaço vetorial pode ser visto como uma álgebra. Podemos responder de modo afirmativo, bastando muni-lo do "produto trivial", isto é, se $ab = 0$ para quaisquer $a, b \in A$. Ademais, todo corpo K pode ser visto como uma álgebra, munido da soma e a multiplicação que o definimos como corpo, daí segue que os conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ podem ser vistos como álgebras sobre si próprios.

Definição 1.1.3 *Um subconjunto β da álgebra A é dito* ***base*** *se β é uma base de A como espaço vetorial, e definimos a* ***dimensão*** *de A como sendo sua dimensão como espaço vetorial.*

Definição 1.1.4 *Dizemos que uma álgebra A é:*

a) ***associativa*** *se o produto de A é associativo, isto é, se $(ab)c = a(bc)$, para todo a, b e $c \in A$;*

b) ***comutativa*** *se o produto de A é comutativo, isto é, se $ab = ba$, para todo $a, b \in A$;*

c) ***unitária (ou com unidade)*** *se o produto de A possui elemento neutro, isto é, se existe $1_A \in A$, tal que $1_A a = a 1_A = a$, para todo $a \in A$;*

d) ***nil*** *se todo elemento $a \in A$ é nilpotente, isto é, para cada $a \in A$ existe um número natural n (que pode depender de a), tal que $a^n = 0$. O menor natural com tal propriedade é chamado de grau ou índice de nilpotência do elemento a. Uma álgebra é nil de grau limitado se existe um número natural n fixo, tal que $a^n = 0$, para todo $a \in A$;*

e) ***nilpotente*** *se existe um número natural n fixo, tal que o produto de quaisquer n elemento de A é igual a zero, isto é, $A^n = 0$. O menor número n com esta propriedade é chamado grau ou índice de nilpotência da álgebra A.*

Se A é uma álgebra com unidade, identificamos cada escalar λ no corpo K por $\lambda 1_A$ de A, e, consequentemente, o corpo K será denotado pelo conjunto $\{\lambda 1_A \mid \lambda \in K\}$ (o subespaço de A gerado por 1_A).

Observação 1.1.5 *Por simplicidade de notação, denotaremos por 1 a unidade da álgebra, em vez de 1_A, quando A for unitária. Tal opção não permite confusão com a unidade do corpo K, pois ambas serão a mesma.*

Exemplo 1.1.6 (Álgebra das Matrizes de ordem n) *Fixado $n \in \mathbb{N}$, o espaço vetorial $M_n(K)$ de todas as matrizes de ordem n com entradas em K, munido do produto usual de matrizes, é uma álgebra associativa com unidade de dimensão n^2. Uma base desta álgebra é o conjunto formado pelas matrizes elementares E_{ij}, para $1 \leq i, j \leq n$, onde E_{ij} é a matriz cuja entrada na i-ésima linha e j-ésima coluna é 1 e as demais são nulas. De modo geral, se A é uma álgebra, ao munir o espaço vetorial $M_n(A)$ com o produto análogo ao de $M_n(K)$ temos uma estrutura de álgebra em $M_n(A)$.*

Exemplo 1.1.7 *Dado V um espaço vetorial, o espaço vetorial $End(V)$ munido da operação de composição é uma álgebra associativa e unitária.*

Exemplo 1.1.8 ***(Álgebra de Grassmann)*** *Seja V um espaço vetorial de dimensão infinita enumerável, com base $\{e_1, e_2, e_3, \ldots\}$. A álgebra de Grassmann $E = E(V)$ de V*

é a álgebra associativa e unitária gerada por $\{1, e_{i_1}e_{i_2}\cdots e_{i_k} \mid i_1 < i_2 < \ldots < i_k; k \geq 1\}$ *que satisfaz a seguinte relação:*

$$e_ie_j = -e_je_i, \forall i, j \in \mathbb{N}^*.$$

Na álgebra de Grassmann E *é importante destacar os seguintes subespaços:*

- E_0*, gerado pelo conjunto* $\{1, e_{i_1}e_{i_2}\cdots e_{i_k} \mid k \text{ é par}\}$*;*
- E_1*, gerado pelo conjunto* $\{e_{i_1}e_{i_2}\cdots e_{i_k} \mid k \text{ é ímpar}\}$*.*

Neste caso $E = E_0 \oplus E_1$*, visto como espaço vetorial, e* $E_0 \cup E_1$ *é a base canônica de* E*. Nestas condições* $ab = (-1)^{\alpha\beta}ba$*, para todo* $a \in E_\alpha$ *e* $b \in E_\beta$*.*

Na teoria de álgebra linear vemos a importância da base de um dado espaço vetorial, por exemplo, quando desejamos ver se uma determinada aplicação é ou não uma transformação linear, já que uma transformação linear fica completamente determinada por sua restrição a uma base. De modo similar, a base torna-se uma ferramenta importante para a construção de álgebras, uma vez que definindo um produto para os seus elementos da base é possível obter uma estrutura de álgebra a partir dele. Isso é garantido pelo próximo resultado, o qual é canônico no estudo das álgebras. Sua demonstração pode ser encontrada em [9, pág. 13].

Proposição 1.1.9 *Seja* A *um espaço vetorial com base* β*. A aplicação* $f : \beta \times \beta \to A$ *pode ser estendida a uma única aplicação bilinear* $* : A \times A \to A$ *tal que*

$$u_1 * u_2 = f(u_1, u_2),$$

para quaisquer $u_1, u_2 \in \beta$*.*

Um exemplo clássico de uma álgebra obtida através da proposição acima é a álgebra de grupo. Vejamos no exemplo a seguir.

Exemplo 1.1.10 *Seja* S *um conjunto não-vazio. Consideremos o conjunto* KS *de todas as somas formais*

$$\sum_{s\in S} \lambda_s s \text{ , onde } \lambda_s \in K \text{ e } \{s \in S, \lambda_s \neq 0\} \text{ é finito.}$$

Dados dois elementos $\sum_{s\in S} \lambda_s s$ *e* $\sum_{s\in S} \gamma_s s$ *em* KS*, dizemos que são iguais se para cada* $s \in S$*, tem-se* $\lambda_s = \gamma_s$*. Definimos as operações soma e produto escalar da seguinte forma:*

$$\sum_{s\in S} \lambda_s s + \sum_{s\in S} \gamma_s s = \sum_{s\in S} (\lambda_s + \gamma_s) s$$

e

$$\gamma \sum_{s \in S} \lambda_s s = \sum_{s \in S} (\gamma \lambda_s) s$$

respectivamente. Munidos destas operações, vemos facilmente que KS é um K-espaço vetorial, chamado de K-espaço vetorial de base S.

*Se "$*$" é uma operação em S, pela Proposição 1.1.9, podemos estender a uma única operação bilinear em KS, a qual denotaremos também por $*$. Assim, $(KS, *)$ tem uma estrutura de Álgebra. Em particular, tomando um grupo G, em vez de um conjunto S qualquer e $*$ a operação de G, obtemos a álgebra KG, chamada de **Álgebra de Grupo**. Como a operação de G é associativa e possui elemento neutro, facilmente se mostra que KG é associativa e possui unidade. E, caso G seja abeliano, a álgebra de grupo KG será comutativa.*

Outras duas álgebras que tem grande importância no decorrer deste trabalho são a álgebra de polinômios e a tensorial.

Exemplo 1.1.11 *Seja $K[x]$ o espaço dos polinômios na indeterminada x. Esse espaço munido do produto usual de polinômios é uma álgebra. De maneira geral, se X é um conjunto (não necessariamente finito, mas enumerável) de indeterminadas comutativas, então o anel de polinômios $K[X]$, munido de suas operações usuais, é uma álgebra.*

Observação 1.1.12 *Na verdade, todo anel sobre um corpo K é um álgebra. O inverso não é verdade, basta considerar o espaço $\mathbb{R}^3$ munido do produto vetorial.*

Exemplo 1.1.13 *Sejam V e W espaços vetoriais. Consideremos o espaço vetorial $K(V \times W)$ com base $V \times W$ e o subespaço $\mathcal{U}$ gerado pelos elementos dos tipos*

$$\begin{aligned} (v_1 + v_2, w) - (v_1, w) - (v_2, w) \\ (v, w_1 + w_2) - (v, w_1) - (v, w_2) \\ (\lambda v, w) - \lambda(v, w) \\ (v, \lambda w) - \lambda(v, w), \end{aligned}$$

*onde $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ e $\lambda \in K$. Daí, obtemos um espaço vetorial quociente $\dfrac{K(V \times W)}{\mathcal{U}}$, denotado por denotado por $V \otimes W$, o qual é chamado de **produto tensorial** entre os espaços V e W. Os elementos $\overline{(v, w)}$ são chamados de tensores (ou tensores decomponíveis) e são denotados por $v \otimes w$.*

Considerando os elementos que geram $\mathcal{U}$, obtemos que dados $\lambda \in K$, $v, v_1, v_2 \in V$ e $w, w_1, w_2 \in W$, valem:

(i) $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$;

(ii) $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$;

(iii) $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$.

Enunciaremos agora uma propriedade muito importante e que será muito usada no Capítulo 3 e cuja demonstração pode ser encontrada em [10, pág. 61]

Teorema 1.1.14 (Propriedade Universal) *Sejam V, W e U espaços vetoriais sobre um corpo K e $f\colon V \times W \to U$ uma aplicação linear. Então existe uma única transformação linear $T_f\colon V \otimes W \to U$, tal que $T_f(v \otimes w) = f(v, w)$, para quaisquer $v \in V$ e $w \in W$.*

Observação 1.1.15 (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 $V \otimes_K W$. A demonstração desse resultado é obtida como aplicação direta do teorema anterior.*

Um fato importante a considerar é que se S_1 e S_2 são conjuntos geradores de V e W, respectivamente, então $\{u_1 \otimes u_2 \mid u_1 \in S_1, u_2 \in S_2\}$ é um conjunto gerador de $V \otimes W$. Nestas condições é fácil perceber que $dim(V \otimes W) = dimV \cdot dimW$. Ademais, considerando V e W como álgebras, podemos definir a aplicação

$$\begin{array}{rcl} \cdot\colon (V \otimes W) \times (V \otimes W) & \to & V \otimes W \\ (v_i \otimes w_j, v_l \otimes w_m) & \mapsto & v_i v_l \otimes v_j v_m. \end{array}$$

Tal aplicação é uma operação em $V \otimes W$. Dessa forma, $V \otimes W$ é uma álgebra, conhecida como Álgebra tensorial.

Existem algumas estruturas comumente utilizadas dentro do estudo das álgebras, e dentre elas destacamos aqui as subálgebras e os ideais.

Definição 1.1.16 *Dada A uma álgebra, dizemos que um subespaço vetorial B de A é uma **subálgebra** se B é multiplicativamente fechado, isto é, $b_1 b_2 \in B$ para quaisquer $b_1, b_2 \in B$. Caso A seja unitária, exigimos que $1_A \in B$. Ademais, dizemos que um subespaço vetorial I de A é um* **ideal** *(bilateral) de A se $AI \subseteq I$ e $IA \subseteq I$, isto é, $ax, xa \in I$ para quaisquer $x \in I$ e $a \in A$.*

Exemplo 1.1.17 *Dada A uma álgebra, definimos o centro $Z(A)$ da álgebra A como sendo o conjunto dos elementos que comutam, com relação ao produto, com todos os elementos da álgebra. Isto é, o centro é dado em símbolos por:*

$$Z(A) = \{a \in A \mid ab = ba, \forall b \in A\}.$$

É claro que $Z(A)$ é uma subálgebra de A que não é, em geral, um ideal. No caso da álgebra das matrizes $M_n(K)$, temos que $Z(M_n(K))$ é formado pelas matrizes múltiplas escalares da identidade. Além disso, para uma álgebra qualquer A é possível provar de forma similar ao caso da álgebra $M_n(K)$ que $Z(M_n(A)) = \{aI_n \mid a \in Z(A)\}$.

Exemplo 1.1.18 *A álgebra $M_{a+b}(E)$ possui uma subálgebra, denotada 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.

Definição 1.1.19 *Definimos o radical de Jacobson de uma álgebra A, denotado por $r(A)$, como a interseção de todos os ideais maximais de A.*

Definição 1.1.20 *Uma álgebra A de dimensão finita é chamada de semissimples se $r(A) = 0$.*

Definiremos uma estrutura muito útil denominada "Álgebra quociente". Seja A uma álgebra, I um ideal de A e consideremos o espaço vetorial quociente A/I. Daí, temos uma classe de equivalência dada por: para todo $a, b \in A$, a é dito **congruente a** b **módulo** I, se $a - b \in I$ e denotaremos por $a \equiv b(\mathrm{mod} I)$.

Consideremos agora o produto no espaço A/I dado por:

$$\begin{aligned} \cdot : A/I \times A/I &\rightarrow A/I \\ (\bar{a}, \bar{b}) &\mapsto \bar{a}.\bar{b} = \overline{ab}. \end{aligned}$$

Um exercício padrão é verificar que este produto está bem definido. Além disso, esse produto é bilinear, logo A/I munido dele é uma álgebra chamada de **álgebra quociente de A por I**.

Definição 1.1.21 *Sejam A e B duas álgebras. Uma transformação linear $\varphi : A \rightarrow B$ é dita um homomorfismo de álgebras se $\varphi(xy) = \varphi(x)\varphi(y)$, para quaisquer $x, y \in A$. Além disso, se as álgebras são unitárias, exigiremos que $\varphi(1_A) = 1_B$.*

Temos alguns tipos especiais de homomorfismos de álgebras, os quais recebem nomes específicos. Chamamos de:

- **mergulho** (ou monomorfismo) um homomorfismo injetivo;
- **epimorfismo** um homomorfismo sobrejetivo;
- **isomorfismo** um homomorfismo bijetivo;
- **endomorfismo** um homomorfismo de A em A;

- **automorfismo** um endomorfismo bijetivo.

Denotamos por End$A$ e Aut$A$ os conjuntos dos endomorfismos e automorfismos, respectivamente, da álgebra A. Além disso, dizemos que duas álgebras A e B são isomorfas, e denotamos por $A \simeq B$ quando existe um isomorfismo entre elas. O próximo resultado determina um critério para a existência de um homomorfismo de álgebra.

Proposição 1.1.22 *Sejam A e B álgebras e S um conjunto gerador de A como espaço vetorial. Seja $\varphi : A \to B$ uma transformação linear (satisfazendo $\varphi(1_A) = 1_B$ se A e B têm unidade). Então, φ é um homomorfismo de álgebras se, e somente se, $\varphi(xy) = \varphi(x)\varphi(y)$ para quaisquer $x, y \in S$.*

Demonstração: Basta usar o fato de que φ é uma transformação linear e também usar a bilinearidade do produto em A e em B. ■

Exemplo 1.1.23 *Sejam A uma álgebra e I um ideal de A. A aplicação*

$$\begin{array}{rcl} \varphi : A & \to & A/I \\ a & \mapsto & \bar{a} = a + I \end{array}$$

é chamada de projeção canônica. Não é difícil ver que ela é um epimorfismo de álgebras.

Exemplo 1.1.24 *Seja A uma álgebra 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. Tomando $r \in U(A)$, podemos considerar a aplicação*

$$\begin{array}{rcl} \varphi : A & \to & A \\ x & \mapsto & \varphi(x) = r^{-1}xr. \end{array}$$

Facilmente verifica-se que φ é um automorfismo de A, chamado de ***automorfismo interno determinado por*** *r.*

No decorrer de nosso trabalho, muitas das vezes será conveniente trabalhar com produto tensorial. No exemplo abaixo, temos uma identificação entre a álgebra de matrizes com a álgebra tensorial que iremos no Capítulo 3 usar frequentemente.

Exemplo 1.1.25 *Dada A uma K-álgebra e $M_n(K)$ a álgebra de matrizes, facilmente vemos que $M_n(K) \otimes A \simeq M_n(A)$. Considere a aplicação linear $f : M_n(K) \otimes A \to M_n(A)$*

induzida por $(E_{ij}, a) \mapsto aE_{ij}$. *Verifica-se que* f *é um isomorfismo de álgebras. De fato, notemos que* $\{aE_{ij} \mid 1 \leq i,j \leq n, a \in \beta\}$ *é uma base de* $M_n(A)$ *como espaço vetorial, onde* β *é uma base de* A. *Consideremos a transformação linear definida por* $aE_{ij} \mapsto E_{ij} \otimes a$. *É claro que a última aplicação é a inversa de* f, *ou seja,* f *é bijetiva. Resta mostrar que* f *é um homomorfismo de álgebra. Ora, como* f *é linear, basta verificarmos para os elementos da base de* $M_n(K) \otimes A$. *Antes disso, observemos que* $E_{ij}E_{rs} = E_{is}$, *se* $j = r$ *e* 0 *caso contrário. Daí,*

- *Se* $j \neq r$, *temos:*

$$\begin{aligned} f((E_{ij} \otimes a)(E_{rs} \otimes b)) &= f(E_{ij}E_{rs} \otimes ab) = f(0 \otimes ab) = \\ &= 0 = aE_{ij}bE_{rs} = f(E_{ij} \otimes a)f(E_{rs} \otimes b). \end{aligned}$$

- *Se* $j = r$, *temos:*

$$\begin{aligned} f((E_{ij} \otimes a)(E_{rs} \otimes b)) = f(E_{ij}E_{rs} \otimes ab) &= abE_{ij}E_{rs} \\ &= aE_{ij}bE_{rs} = f(E_{ij} \otimes a)f(E_{rs} \otimes b). \end{aligned}$$

Deste modo, f *é um homomorfismo bijetor, ou seja,* $M_n(K) \otimes A \simeq M_n(A)$.

Dado um homomorfismo, definimos dois conjuntos muito importantes no estudo de morfismos e que já são conhecidos no estudo de outras estruturas.

Definição 1.1.26 *Dado um homomorfismo* $\varphi\colon A \to B$, *definimos o núcleo de* φ, *denotado por* $ker\varphi$, *como o conjunto* $ker\varphi = \{a \in A \mid \varphi(a) = 0_B\}$ *e a imagem de* φ, *denotada por* $Im\varphi$, *como o conjunto* $Im\varphi = \{\varphi(a) \mid a \in A\}$.

Da definição acima, não é difícil ver que $ker\varphi$ é um ideal de A e também pode-se mostrar que um homomorfismo é injetor se, e somente se, seu núcleo é o trivial, isto é, o núcleo é constituído apenas pelo zero. E é claro que $Im\varphi$ é uma subálgebra de B, podendo não ser um ideal de B.

Como é de praxe, é natural estudar o chamado "Teorema Fundamental dos Isomorfismos" sempre que vemos uma nova estrutura algébrica. A seguir iremos enunciar o teorema padrão, porém iremos omitir sua demonstração por ser idêntica a demonstração da teoria de anéis.

Teorema 1.1.27 *(Teorema fundamental dos Isomorfismos) Seja* φ *um homomorfismo entre* A *e* B. *Então* $(A/ker\varphi) \simeq Im\varphi$.

Exemplo 1.1.28 *Sendo A um álgebra unitária, consideremos a aplicação*

$$\begin{aligned} \psi : K &\rightarrow A \\ \lambda &\mapsto \psi(\lambda) = \lambda 1 \end{aligned}$$

É fácil ver que ψ é um mergulho de K em A e assim, pelo teorema fundamental dos isomorfismos, temos que K é isomorfo a $Im\psi = \{\lambda 1 \mid \lambda \in K\}$, donde $Im\psi$ é um corpo. Disso segue a identificação natural entre K e $\{\lambda 1 \mid \lambda \in K\}$.

Observação 1.1.29 *Pelos comentários feitos nos Exemplos 1.1.17 e 1.1.28, temos que $Z(M_n(K)) \simeq K$ (por abuso de notação, $Z(M_n(K)) = K$). Tal identificação será útil mais a frente.*

Uma classe de álgebras muito importante é a das álgebras cujos únicos ideais são os triviais, estas recebem um nome especial, como está descrito na definição a seguir.

Definição 1.1.30 *Seja A uma álgebra tal que $A^2 \neq \{0\}$. Dizemos que A é simples, se $\{0\}$ e A são seus únicos ideais. Além disso, dizemos que A é central simples se A é simples e $Z(A) = K$.*

Exemplo 1.1.31 *O anel das matrizes $M_n(K)$ é uma álgebra central simples sobre K. Basta lembrar dos comentários anteriores que $Z(M_n(K)) = K$ e, com alguns cálculos, mostrar que os únicos ideais de $M_n(K)$ são os triviais.*

Munidos da definição acima, enunciaremos o Teorema de Skolem-Noether o qual caracteriza os automorfismos de uma álgebra central simples. Tendo em vista a quantidade de pré-requisitos para sua demonstração, esta será omitida, porém pode ser encontrada em [40, pág. 68].

Teorema 1.1.32 (Skolem-Noether) *Sejam A uma álgebra central simples sobre K e B uma K-álgebra simples. Sejam $\sigma, \tau : B \rightarrow A$ homomorfismos de álgebras. Então, existe um automorfismo interno φ de A tal que $\tau = \varphi\sigma$.*

Como consequência imediata temos o seguinte corolário.

Corolário 1.1.33 *Se A é uma álgebra central simples de dimensão finita, então todo automorfismo φ de A é interno.*

Iremos finalizar a seção enunciando o "Teorema do Centralizador Duplo", para isto, necessitaremos de certas definições. Seja S um subconjunto de uma álgebra A, podemos definir o conjunto

$$C_A(S) = \{a \in A \mid as = sa \text{ para todo } s \in S\}.$$

O conjunto $C_A(S)$ é uma subálgebra de A chamado de centralizador de S em A. Além disso, $S \subset C_A(C_A(S))$ e $C_A(A) = Z(A)$. Consideremos uma caso particular, seja $A = EndV$ a álgebra dos endomofirsmos de V e considere S uma subálgebra de A, observe que

$$End_S(V) = \{f \in A \mid af = fa, \forall a \in S\} = C_A(S).$$

Assim, podemos considerar, neste caso particular, a notação de centralizador dado anteriormente.

Estamos prontos para enunciar o resultado, sua prova pode ser encontrado em [14, Teorema 5.18.1.].

Teorema 1.1.34 (Centralizador Duplo) *Seja A, B duas subálgebras da álgebra $End(V)$, onde V é um espaço de dimensão finita, tal que A é semissimples e $B = End_A(V)$. Então $A = End_B(V)$, isto é, o centralizador do centralizador de A é o próprio A.*

1.2 Módulos sobre álgebras

Além da estrutura de Álgebra, outra estrutura que será utilizada em nosso estudo é a de **Módulo**. Tal estrutura é uma generalização do espaço vetorial, uma vez que a diferença está no fato que no espaço vetorial os escalares estão num corpo, aqui os escalares estão sobre um anel (módulos sobre anéis). Nesta seção, para evitarmos repetições, todas as álgebras consideradas serão associativas com unidade.

Definição 1.2.1 *Seja A uma álgebra. Definimos um A-módulo (ou módulo sobre A) como sendo um espaço vetorial M, munido de um produto por escalar*

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

que satisfaz:

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

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

para quaisquer $a, a_1, a_2 \in A$, $m, m_1, m_2 \in M$ *e* $\lambda \in K$.

Observe que os três primeiros itens na definição acima exigem que o produto "$\cdot$" seja uma aplicação bilinear.

Exemplo 1.2.2 *Dada* A *uma álgebra, então* A *é naturalmente um módulo sobre si mesma, cujo produto é a multiplicação da álgebra* A.

Exemplo 1.2.3 *Sejam* G *um grupo,* V *um* K*-espaço vetorial e* $\varphi : G \to GL(V)$ *um homomorfismo de grupos onde* $\varphi(g) = \varphi_g$. *Consideremos o produto*

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

Como φ *é um homomorfismo e* φ_g *é linear, segue que* V *munido desse produto é um* KG*-módulo (ou, simplesmente,* G*-módulo).*

Definição 1.2.4 *Dada* A *uma álgebra e* M *um* A*-módulo, dizemos que um subespaço vetorial* N *de* M *é um submódulo (ou* A*-submódulo) de* M *se* $a \cdot n \in N$, *para quaisquer* $a \in A$ *e* $n \in N$.

Exemplo 1.2.5 (Módulos quocientes) *Dados* A *uma álgebra,* M *um* A*-módulo e* N *um submódulo de* M, *consideremos em* M *a relação de congruência módulo* N, *definida da seguinte forma*

$$m_1 \equiv m_2 (mod N) \text{ se } m_1 - m_2 \in N.$$

Essa relação é de equivalência. Denotanto por M/N *o conjunto quociente da relação módulo* N ($M/N = \{m + N \mid m \in N\}$), *definimos:*

$$\begin{array}{rcl} + : M/N \times M/N & \to & M/N \\ (\overline{m_1}, \overline{m_2}) & \mapsto & \overline{m_1} + \overline{m_2} = \overline{m_1 + m_2} \end{array}$$

e

$$\begin{array}{rcl} \cdot : A \times M/N & \to & M/N \\ (a, \overline{m}) & \mapsto & a \cdot \overline{m} = \overline{am}. \end{array}$$

Tais operações estão bem definidas e facilmente se vê que M/N *munido delas é um* A*-módulo.*

Exemplo 1.2.6 *Sejam* $K[x]$ *o anel de polinômios,* V *um* K*-espaço vetorial e uma transformação linear* $T : V \to V$. *O espaço* V *é um* $K[x]$*-módulo com a aplicação* $K[x] \times V$ *em* V *dada por*

$$(a_0 + a_1 x + \cdots + a_n x^n) \cdot v = (a_0 I + a_1 T + \cdots + a_n T^n)(v).$$

Definição 1.2.7 *Sejam A uma álgebra e M_1 e M_2 dois A-módulos. Dizemos que uma transformação linear $\phi : M_1 \to M_2$ é um homomorfismo de A-módulos quando $\phi(am) = a\phi(m)$, para quaisquer $a \in A$ e $m \in M_1$. Se ϕ for uma bijeção, diremos que este homomorfismo é um isomorfismo de A-módulos.*

Exemplo 1.2.8 *Sejam M um A-módulo e $\gamma \in K$. Consideremos a aplicação*

$$\begin{aligned} T_\gamma : M &\to M \\ m &\mapsto \gamma m. \end{aligned}$$

Tome $a \in A$ e $m \in M$ arbitrários, então

$$T_\gamma(a \cdot m) = \gamma(a \cdot m) = a \cdot (\gamma m) = a \cdot (T_\gamma(m)).$$

Assim, T_γ é um homomorfismo de A-módulos.

Assim como visto para álgebras, também temos a noção de simplicidade para módulos.

Definição 1.2.9 *Um A-módulo M é simples se $M \neq \{0\}$ e M não tem submódulos próprios não nulos, ou seja, os únicos submódulos de M são $\{0\}$ e M. Além disso, dizemos que M é semissimples se ele é soma direta de módulos simples.*

Nas condições da definição anterior, uma álgebra A é semissimples (simples) se é semissimples (simples) como A-módulo.

Exemplo 1.2.10 *Todo A-módulo de dimensão 1 (sobre K) é simples. Além disso, todo módulo simples é semissimples.*

Munidos da definição de semissimplicidade, enunciaremos o importante Teorema de Maschke o qual estabelece condições para que um anel de grupo seja semissimples.

Teorema 1.2.11 (Maschke) *Seja G um grupo finito e K um corpo cuja característica não divide $|G|$. Então todo KG-módulo (ou simplesmente G-modulo) é semissimples. Em particular, KG é um anel semissimples.*

Demonstração: Ver [22, Seção 5.2, pág. 219]. ∎

Exemplo 1.2.12 *Sendo K um corpo de característica zero, do Teorema de Maschke concluímos que KS_n, com $n \in \mathbb{N}$ é semissimples, uma vez que S_n é finito.*

Conforme comentado no início desta seção, módulos são generalização da noção de espaços vetoriais. Uma pergunta natural é se conseguimos obter uma ideia similar de base para módulos. A resposta é sim e a veremos de forma mais formal na definição abaixo.

Definição 1.2.13 *Dizemos que um A-módulo M (não-nulo) é livre se existe um subconjunto B de M satisfazendo:*

i) B é um conjunto gerador de M;

ii) Para todo $a_1, \ldots, a_n \in A$ e todo $m_1, \ldots, m_n \in B$, tais que $a_1m_1 + \cdots + a_nm_n = 0_M$, tem-se $a_1 = \ldots = a_n = 0$, ou seja, B é linearmente independente (LI) sobre A.

Um subconjunto B de M satisfazendo as condições $i)$ e $ii)$ da definição acima é chamado de base de M. Assim, um módulo é dito livre se possui alguma base. Aqui é importante comentarmos que, diferente dos espaços vetoriais, nem todo módulo tem base. Por exemplo, $\mathbb{Q}$ não é um $\mathbb{Z}$-módulo livre.

Exemplo 1.2.14 *Todo espaço vetorial não nulo é um módulo livre sobre K.*

Exemplo 1.2.15 *Sendo A uma álgebra qualquer e $n \in \mathbb{N}$. Temos que o A-módulo A^n é livre. De fato, para cada $i = 1, \ldots, n$, considere o elemento $e_i \in A^n$ que possui 1 na i-ésima entrada e 0 nas demais. Não é difícil ver que $\{e_1, \ldots, e_n\}$ é uma base de A^n.*

1.3 Álgebra livre e identidades polinomiais

No Exemplo 1.1.11 vimos a álgebra dos polinômios em várias indeterminadas, onde estas eram comutativas. Com cálculos simples podemos ver que se as indeterminadas forem não comutativas ainda continuamos com um exemplo de K-álgebra, sendo esta agora denotada por $K\langle X \rangle$, onde X será um conjunto de indeterminadas que comutam com os escalares em K.

Nesta seção definiremos as álgebras livres e veremos, por exemplo, que $K\langle X \rangle$ é um exemplo de tal estrutura. Tal conceito é extremamente importante no estudo das identidades polinomiais (PI's), uma vez que a álgebra livre é o "ambiente" em que as PI's são definidas.

1.3.1 Álgebra livre, identidades polinomiais e T-ideais

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 $h : X \to A$ 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 do conjunto X, denotado por $|X|$, será chamada* ***posto*** *de F.*

Exemplo 1.3.2 *Consideremos a álgebra unitária $K[x_1, \ldots, x_n]$ dos polinômios associativos e comutativos nas variáveis $x_1, \ldots, x_n$, a qual como já vimos é gerada pelo conjunto $X = \{x_1, \ldots, x_n\}$. Note que ela é uma álgebra livremente gerada pelo conjunto X na classe das álgebras associativas, comutativas e unitárias.*

De fato, dada uma álgebra associativa, comutativa e unitária A, e elementos $a_1, \ldots, a_n$ em A consideremos a aplicação

$$\begin{aligned} \varphi : X &\to A \\ x_i &\mapsto \varphi(x_i) = a_i. \end{aligned}$$

Daí, podemos construir o homomorfismo

$$\begin{aligned} \phi : K[x_1, \ldots, x_n] &\to A \\ f(x_1, \ldots, x_n) &\mapsto f(a_1, \ldots, a_n) \end{aligned}$$

o qual estende φ e é o único que o estende, já que podemos considerar primeiramente nos monômios e depois aplicar a Proposição 1.1.22.

Nosso objetivo agora é construir uma álgebra livre na classe de todas as álgebras associativas unitárias e, para isso, consideremos $X = \{x_1, x_2, \ldots\}$ um conjunto infinito e enumerável de variáveis não comutativas. Uma palavra em X será entendida como uma sequência $x_{i_1} x_{i_2} \cdots x_{i_n}$, onde $n \in \mathbb{N} \cup \{0\}$ e $x_{i_j} \in X$ e denotaremos por 1 a palavra vazia, isto é, quando $n = 0$. Dizemos que duas palavras $x_{i_1} x_{i_2} \cdots x_{i_n}$ e $x_{j_1} x_{j_2} \cdots x_{j_m}$ são iguais se $n = m$ e $i_1 = j_1$, $i_2 = j_2$, $\ldots$, $i_n = j_n$.

Seja $K\langle X \rangle$ o espaço vetorial que tem por base o conjunto de todas as palavras em X. Assim, seus elementos, os quais chamaremos de polinômios, são somas (formais) finitas de termos (ou monômios) que são produtos (formais) de um escalar por uma palavra em X. Em símbolos,

$$K\langle X \rangle = \Big\{ \sum \lambda_n a_n \mid \lambda_n \in K, a_n \text{ é uma palavra em X e } \{\lambda_n \neq 0\} \text{ é finito} \Big\}.$$

Definamos em $K\langle X\rangle$ a seguinte multiplicação

$$(x_{i_1}\cdots x_{i_k})(x_{j_1}\cdots x_{j_l}) = x_{i_1}\cdots x_{i_k}x_{j_1}\cdots x_{j_l}, \text{ onde } x_{i_t}, x_{j_s} \in X.$$

E estendemos o resultado pela Proposição 1.1.9. Facilmente notamos que o espaço $K\langle X\rangle$ munido deste produto é uma álgebra associativa com unidade (a palavra vazia) gerada pelo conjunto X.

Proposição 1.3.3 *A álgebra $K\langle X\rangle$ é livre na classe das álgebras associativas com unidade, livremente gerada pelo conjunto X.*

Demonstração: Sejam A uma álgebra associativa com unidade e $h : X \to A$ uma aplicação qualquer com $h(x_i) = a_i$, para $i \in \mathbb{N}$. Então existe uma aplicação linear $\varphi_h : K\langle X\rangle \to A$, tal que $\varphi_h(1) = 1_A$ e $\varphi_h(x_{i_1}x_{i_2}\cdots x_{i_n}) = a_{i_1}a_{i_2}\cdots a_{i_n}$. Pela Proposição 1.1.22, temos que φ_h é um homomorfismo de álgebras e a unicidade segue do fato de estender elementos da base e satisfazer $\varphi_h\,|_X = h$. ■

Munido das estruturas aqui definidas, definiremos agora o conceito de identidades polinomiais para uma álgebra dada.

Definição 1.3.4 *Seja A uma álgebra. Dizemos que um polinômio $f(x_1, \ldots, x_n)$ em $K\langle X\rangle$ é uma identidade polinomial da álgebra A, se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_1, \ldots, a_n \in A$. Neste caso, denotamos por $f \equiv 0$ em A.*

Observe que $f = f(x_1, \ldots, x_n)$ é uma identidade polinomial de A se, e somente se, f pertence ao núcleo de cada homomorfismo de $K\langle X\rangle$ em A. Com efeito, basta tomarmos $\phi_h : K\langle X\rangle \to A$ o homomorfismo de álgebras obtido da definição de álgebra livre o qual estende uma aplicação $h : X \to A$, daí

$$\phi_h(f(x_1, \ldots, x_n)) = f(\phi_h(x_1), \ldots, \phi_h(x_n)) = f(h(x_1), \ldots, h(x_n)),$$

seguindo o desejado.

Denotando por $T(A)$ o conjunto de todas as identidades polinomiais de A, temos a seguinte definição:

Definição 1.3.5 *Dizemos que A é uma álgebra com identidade polinomial, ou uma PI-álgebra, se $T(A) \neq \{0\}$, isto é, se a álgebra admite uma identidade polinomial não nula.*

Vejamos agora alguns exemplos de PI-álgebras.

Exemplo 1.3.6 *Seja A um álgebra, então $f(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1$ é uma identidade polinomial para A se, e somente se, A é comutativa. Em particular, concluímos que toda álgebra comutativa é uma PI-álgebra.*

Exemplo 1.3.7 *O polinômio $f(x_1, x_2, x_3) = [[x_1, x_2]^2, x_3]$, conhecido como polinômio de Hall, é uma identidade polinomial para $M_2(K)$. Com efeito, se $A = [X, Y]$, com $X, Y \in M_2(K)$ quaisquer, temos da propriedade cíclica do traço, e por ele ser linear, que $tr(A) = 0$. Por outro lado, o polinômio característico é tal que*

$$x^2 - tr(A)x + det(A)I_2 = 0.$$

Substituindo x por A, temos

$$A^2 = -det(A)I_2.$$

Assim, A^2 é uma matriz escalar, logo comuta com qualquer outra matriz. Ou seja,

$$[A^2, Z] = 0 \Rightarrow [[X, Y]^2, Z] = 0,$$

para todo $Z \in M_2(K)$. Em particular, concluímos que $M_2(K)$ é uma PI-álgebra.

Dada uma álgebra A, $T(A)$ é claramente uma ideal de $K\langle X\rangle$. Além disso, note que dados $f = f(x_1, x_2, \ldots, x_n) \in T(A)$, $\psi : K\langle X\rangle \to A$ um homomorfismo qualquer e $\varphi \in End(K\langle X\rangle)$, então $\psi \circ \varphi : K\langle X\rangle \to A$ é um homomorfismo de álgebras. Assim, como $f \equiv 0$ em A, temos $f \in ker(\psi \circ \varphi)$. Deste modo,

$$\psi(\varphi(f)) = (\psi \circ \varphi)(f) = 0 \Rightarrow \varphi(f) \in ker\psi.$$

Portanto, da arbitrariedade de ψ, segue que $\varphi(f) \in T(A)$. Ou seja, $T(A)$ é fechado (ou invariante) por endomorfismos de $K\langle X\rangle$. Isto motiva a definição a seguir.

Definição 1.3.8 *Um ideal I de $K\langle X\rangle$ é dito ser um T-ideal se para todo endomorfismo ϕ de $K\langle X\rangle$, temos que $\phi(I) \subseteq I$, ou, equivalentemente, se $f(g_1, \ldots, g_n) \in I$ para quaisquer $f(x_1, \ldots, x_n) \in I$ e $g_1, \ldots, g_n \in K\langle X\rangle$.*

Pelo que comentamos antes da definição, $T(A)$ é um T-ideal de $K\langle X\rangle$. Por outro lado, é fácil mostrar que todos os T-ideais de $K\langle X\rangle$ são deste tipo, ou seja, é conjunto de identidades para uma certa álgebra. Com efeito, basta tomar $B = \dfrac{K\langle X\rangle}{I}$. Dado $f = f(x_1, \ldots, x_n) \in T(B)$, temos

$$\overline{f(x_1, \ldots, x_n)} = f(\overline{x_1}, \ldots, \overline{x_n}) = \overline{0}.$$

Assim, $f \in I$ e, consequentemente, $T(B) \subseteq I$. Agora, considerando $g(x_1, \ldots, x_n) \in I$ e $\overline{g_1}, \ldots, \overline{g_n} \in B$. Como I é um T-ideal, temos $g(g_1, \ldots, g_n) \in I$ e, assim,

$$g(\overline{g_1}, \ldots, \overline{g_n}) = \overline{g((g_1, \ldots, g_n))} = \overline{0}.$$

Daí, $g \in T(B)$ e $I \subseteq T(B)$. Temos então a igualdade desejada.

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

1.3.2 Variedades de álgebras

Sabemos que cada álgebra A determina um T-ideal em $K\langle X \rangle$, mas por outro lado muitas álgebras têm os mesmos T-ideais (como o ideal de suas identidades). É de fácil verificação que se considerarmos K um corpo qualquer de característica zero e C uma álgebra comutativa, tem-se $T(C) = \langle [x_1, x_2] \rangle_T$. Em particular, $T(\mathbb{R}) = T(\mathbb{C})$, mesmo $\mathbb{R}$ e $\mathbb{C}$ sendo $\mathbb{R}$-álgebras não-isomorfas. Para deixar tal conexão mais clara, precisamos ter a noção de uma variedade de álgebras.

Para motivar a nomenclatura usada, vamos compreender um conceito de geometria algébrica. Dados K um corpo algebricamente fechado, $K[x_1, x_2, \ldots, x_n]$ o anel de polinômios em K com n variáveis e $\{f_i\}_{i=1,2,\ldots,n}$ uma família de polinômios em $K[x_1, x_2, \ldots, x_n]$, um subconjunto de K^n formado por pontos que anulam todos os polinômios de $\{f_i\}_{i=1,2,\ldots,n}$ é dito, no estudo de geometria algébrica, uma variedade algébrica. Em símbolos:

$$V = \{(x_1, x_2, \ldots, x_n) \mid f_i(x_1, x_2, \ldots, x_n) = 0, \forall i = 1, 2, \ldots, n\} \subseteq K^n.$$

Baseado neste conceito, podemos imaginar agora o conceito de variedades de álgebras, vendo agora dentro do estudo de PI-teoria.

Definição 1.3.9 *Dado um conjunto não-vazio $S \subset K\langle X\rangle$, a classe de todas as álgebras A tais que $f \equiv 0$ em A, para todo $f \in S$, é chamada de variedade $\mathcal{V} = \mathcal{V}(S)$ determinada por S.*

Uma variedade $\mathcal{V}$ é chamada não trivial se $S \neq 0$. Além disso, $\mathcal{V}$ é própria se é não-trivial e contém uma álgebra não-nula. Diante da definição, temos $\mathcal{V}(S) = \mathcal{V}(T(S))$ e, daí, V é uma variedade gerada pelo T-ideal. Se $\mathcal{V}$ é uma variedade de álgebra, definimos o T-ideal da variedade $\mathcal{V}$, denotado por $T(\mathcal{V})$, como sendo a interseção de todos os T-ideais $T(A)$ com $A \in \mathcal{V}$. A variedade de álgebras definida por $T(\mathcal{V})$ é chamada de variedade gerada por $\mathcal{V}$, a qual é a própria $\mathcal{V}$, e denotada por $var(\mathcal{V})$. Se $\mathcal{V} = \{A\}$, então denotamos $var(\mathcal{V})$ simplesmente por $var(A)$, esta é a variedade gerada por $T(A)$. Observe que a variedade definida por S é igual à variedade definida por $\langle S\rangle_T$.

Exemplo 1.3.10 *A classe de todas as álgebras comutativas formam uma variedade própria com $S = \{[x, y]\}$.*

Exemplo 1.3.11 *Se $S = \{x^n\}$, então $\mathcal{V}(S)$ é a variedade de todas as álgebras que são nil de índice limitado por n.*

Veremos agora o conceito de álgebra relativamente livre, o qual nasce do nosso desejo em generalizar o conceito de álgebra livre.

Definição 1.3.12 *Seja $\mathcal{V}$ uma variedade, $A \in \mathcal{V}$ uma álgebra e $Y \subseteq A$ um subconjunto de A. Dizemos que A é uma álgebra relativamente livre de $\mathcal{V}$ (com respeito ao conjunto Y), se para qualquer álgebra $B \in \mathcal{V}$ e para cada aplicação $\alpha : Y \to B$, existe um único homomorfismo $\beta : A \to B$ estendendo α. A cardinalidade de Y é chamada de posto de A.*

Quando $\mathcal{V}$ é a variedade obtida pelo polinômio nulo, temos, justamente, a definição de uma álgebra livre, livremente gerada pelo conjunto Y.

Veremos agora um resultado que será muito utilizado na Seção 1.3.4.

Teorema 1.3.13 *Sejam X um conjunto não vazio, $K\langle X\rangle$ uma álgebra livre em X e $\mathcal{V}$ uma variedade com ideal correspondente $T(\mathcal{V}) \subseteq K\langle X\rangle$. Então $K\langle X\rangle/T(\mathcal{V})$ é uma álgebra relativamente livre no conjunto $\overline{X} = \{x + T(\mathcal{V}) \mid x \in X\}$. Ademais, qualquer duas álgebras relativamente livres com respeito à $\mathcal{V}$ de mesmo posto são isomorfas.*

Demonstração: Da definição de álgebra relativamente livre, queremos mostrar que dados $B \in \mathcal{V}$ e $\alpha : \overline{X} \to B$ uma aplicação, existe um único homomorfismo de $K\langle X\rangle/T(\mathcal{V})$ em B estendendo A. Com efeito, para construir tal homomorfismo, iniciemos definindo a aplicação β, onde

$$\begin{aligned} \beta : X &\to B \\ x &\mapsto \beta(x) = \alpha(x + T(\mathcal{V})). \end{aligned}$$

Como $K\langle X\rangle$ é a álgebra livre em X, β pode ser estendido para um único homomorfismo

$$\bar{\beta} : K\langle X\rangle \to B.$$

Agora, note que se $f \in T(\mathcal{V})$, então f é uma identidade de B. Daí, $\bar{\beta}(f) = 0$, ou seja, $T(\mathcal{V}) \subseteq ker\bar{\beta}$ e α estende para um único homomorfismo dado por

$$\begin{aligned} \bar{\beta}_0 : \frac{K\langle X\rangle}{T(\mathcal{V})} &\to B \\ \bar{f} &\mapsto \bar{\beta}_0(\bar{f}) = \bar{\beta}(f). \end{aligned}$$

Portanto, $\dfrac{K\langle X\rangle}{T(\mathcal{V})}$ é um álgebra relativamente livre em $\overline{X}$.

Por fim, consideremos $F_1, F_2 \in \mathcal{V}$ duas álgebras relativamente livres com o mesmo posto em $X = \{x_1 \mid i \in I\}$ e $Y = \{y_i \mid i \in I\}$, respectivamente. Como F_1 e F_2 são álgebras relativamente livres com respeito a $\mathcal{V}$, existem $\alpha_1 : F_1 \to F_2$ e $\alpha_2 : F_2 \to F_1$ homomorfismos, tais que

$$\alpha_1(x_i) = y_i \text{ e } \alpha_2(y_i) = x_i, \forall i \in I.$$

Deste modo, $\alpha_1 \circ \alpha_2$ e $\alpha_2 \circ \alpha_1$ são as aplicações identidades em Y e X, respectivamente. Logo, α_1 e α_2 são isomorfismos, e, portanto, F_1 e F_2 são isomorfas. ■

Teorema 1.3.14 *Existe uma correspondência biunívoca π entre os T-ideais de $K\langle X\rangle$ e as variedades de álgebras. Ademais, para cada dois T-ideais V_1 e V_2, temos $V_1 \subseteq V_2$ se, e somente se, $\pi(V_1) \supseteq \pi(V_2)$.*

Demonstração: Dado um T-ideal V, defina $\mathcal{V} = \pi(V)$ como sendo a variedade determinada por todos os polinômios pertencentes a V. Essa correspondência é sobrejetora, uma vez que podemos considerar V como o T-ideal associado à variedade. Ademais, sejam V_1 e V_2 T-ideais, tais que $V_1 \neq V_2$ e $\pi(V_i) = \mathcal{V}_i$, para $i = 1, 2$. Então, existe um polinômio $f(x_1, \ldots, x_n) \in V_1 \backslash V_2$ (ou em $V_2 \backslash V_1$). Daí, $f(x_1, \ldots, x_n) \equiv 0$ em $\mathcal{V}_1$, mas não é identidade para a álgebra relativamente livre $F(\mathcal{V}_2) = \dfrac{K\langle X\rangle}{V_2} \in \mathcal{V}_2$. Daí $\mathcal{V}_1 \neq \mathcal{V}_2$ e π é uma bijeção.

Claramente, $\mathcal{V}_1 \supset \mathcal{V}_2$ se, e só se, toda identidade polinomial para $\mathcal{V}_1$ é satisfeita também por $\mathcal{V}_2$, isto é, $T(\mathcal{V}_1) \subset T(\mathcal{V}_2)$. ■

Também nos referimos a $K\langle X\rangle / T(\mathcal{V})$ como a álgebra relativamente livre da variedade $\mathcal{V}$ de posto $|X|$.

1.3.3 Polinômios homogêneos e multilineares

Estudaremos agora alguns tipos de polinômios que serão utilizados no decorrer deste trabalho. Como veremos nesta subseção, dado qualquer polinômio $f \in K\langle X\rangle$, podemos escrevê-lo como soma de outros polinômios específicos. Tal fato é importante uma vez que, sobre um corpo infinito, o estudo das identidades de uma dada álgebra pode ser reduzido ao estudo de polinômios homogêneos. Inicialmente, definiremos o grau de um monômio e de um polinômio com respeito a uma indeterminada.

Definição 1.3.15 *Dado $m \in K\langle X\rangle$ um monômio, $f \in K\langle X\rangle$ um polinômio e $x_i \in X$. Definimos o* ***grau de*** *m* ***em*** *x_i, denotado por $deg_{x_i} m$, como sendo o número de vezes em que x_i aparece em m e definimos o* ***grau de*** *f* ***em*** *x_i, e denotamos por $deg_{x_i} f$, como sendo o maior grau em x_i dos monômios que formam f.*

Munidos da definição acima, podemos agora definir os tipos de polinômios que trabalharemos.

Definição 1.3.16 *a) Um polinômio $f(x_1, \ldots, x_n) \in K\langle X\rangle$ é dito* ***homogêneo em uma indeterminada*** *x_i quando todos os seus monômios têm o mesmo grau em x_i.;*

b) Um polinômio f é dito ***multihomogêneo*** *se é homogêneo em todas as suas indeterminadas;*

c) Um polinômio f é dito ***multilinear*** *quando for linear em todas as suas indeterminadas, isto é, quando cada indeterminada tiver grau 1 em cada monômio de f.*

Denotando por S_n o grupo das permutações de $\{1, 2, \ldots, n\}$, se f é multilinear, então podemos escrevê-lo da forma

$$f = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}, \text{ com } \alpha_\sigma \in K.$$

Exemplo 1.3.17 *O polinômio* $f(x_1, x_2, x_3, x_4) = x_1x_2^2 + x_2x_3x_2x_4x_1 + x_3x_1x_3x_2^2$ *é homogêneo em* x_2 *e em* x_1*, mas não é multihomogêneo, nem também multilinear.*

Exemplo 1.3.18 *O polinômio* $f(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1$ *é multilinear.*

Agora, definiremos um tipo especial de polinômio que será utilizado em nosso trabalho.

Definição 1.3.19 *Seja* $f(x_1, \ldots, x_n, y_1, \ldots, y_t)$ *um polinômio linear nas* n *primeiras variáveis. Dizemos que* f *é alternante nas* n *primeiras variáveis se para quaisquer* $1 \leq i < j \leq n$ *o polinômio* f *se anula quando substituímos* x_i *por* x_j*. Dizemos que* f *é alternante se ele é alternante em todas as variáveis.*

Exemplo 1.3.20 *O polinômio*

$$St_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} (-1)^{\sigma} x_{\sigma(1)}x_{\sigma(2)} \cdots x_{\sigma(n)}$$

onde $(-1)^{\sigma}$ *denota o sinal da permutação* $\sigma \in S_n$*, é um polinômio multilinear e alternante, chamado de* **Polinômio Standard de grau** n*. Em [18, pág. 18], encontramos a demonstração do Teorema de Amitsur-Levitzki o qual nos garante que para cada* $n \in \mathbb{N}$*, o polinômio standard* St_{2n} *é a identidade de menor grau para a álgebra* $M_n(K)$*.*

O próximo resultado nos dará um critério para verificar se um dado polinômio multilinear é identidade ou não para um determinada álgebra.

Proposição 1.3.21 *Considere* A *uma álgebra gerada por* β*, como espaço vetorial. Se* $f(u_1, u_2, \ldots, u_n) = 0$*, com* f *multilinear, para quaisquer* $u_1, u_2, \ldots, u_n \in \beta$*, então* $f \in T(A)$*.*

Demonstração: Com efeito, dados $a_1, \ldots, a_n \in A$, podemos escrever

$$a_j = \sum \alpha_{ji}u_i, u_i \in \beta.$$

Assim, como $f = f(x_1, \ldots, x_n)$ é linear em cada variável, segue que

$$f(a_1, \ldots, a_n) = \sum \alpha_{1i_1} \cdots \alpha_{ni_n} f(u_{i_1}, \ldots, u_{i_n}) = 0.$$

■

Concluímos que para verificar que um polinômio multilinear é uma identidade polinomial para uma determinada álgebra, basta que o mesmo se anule para os elementos de um conjunto gerador da mesma, como espaço vetorial. Em particular, podemos considerar a sua base.

Dado $f(x_1, \dots, x_n) \in K\langle X\rangle$, facilmente vemos que podemos sempre escrever

$$f = \sum_{i_1 \geq 0, \dots, i_n \geq 0} f^{(i_1, \dots, i_n)}$$

onde $f^{(i_1,\dots,i_n)}$ é a soma de todos os monômios em f onde $x_1, \dots, x_n$ tem grau $i_1, \dots, i_n$, respectivamente. Os polinômios $f^{(i_1,\dots,i_n)}$ que são não-nulos são chamados de **componentes multihomogêneas** de f. Assim, todo polinômio pode ser escrito como soma de polinômios multihomogêneos.

Exemplo 1.3.22 *Consideremos o polinômio*

$$f(x_1, x_2, x_3) = x_1x_2 + 3x_1x_3 - 2x_2x_3 + 4x_1x_2x_3x_1 + x_2^2x_1x_3 - x_2x_1.$$

Note que temos as seguintes componentes multihomogêneas em f:

- $f^{(1,1,0)} = x_1x_2 - x_2x_1$;
- $f^{(1,0,1)} = x_1x_3$;
- $f^{(0,1,1)} = -2x_2x_3$;
- $f^{(1,2,1)} = 4x_1x_2x_3x_1 + x_2^2x_1x_3$.

E, temos:

$$f = f^{(1,1,0)} + f^{(1,0,1)} + f^{(0,1,1)} + f^{(1,2,1)}.$$

Teorema 1.3.23 *Seja K um corpo infinito. Se $f \equiv 0$ é uma identidade polinomial para a álgebra A, então toda componente multihomogênea de f é também um identidade polinomial para A.*

Demonstração: Veja [18, pág 6, Theorem 1.3.2].

■

Teorema 1.3.24 *Se $charK = 0$, todo polinômio não nulo $f \in K\langle X\rangle$ é equivalente ao conjunto finito de polinômios multilineares.*

Demonstração: Veja [18, pág 7, Theorem 1.3.8].

■

Observação 1.3.25 (Processo de Multilinearização) *Dados uma álgebra A e um polinômio f que é identidade para A, podemos obter um polinômio multilinear que é também identidade para A e tem grau menor ou igual do que o grau de f.*

Com efeito, sendo $f = f(x_1, \ldots, x_n)$, consideremos o polinômio

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

Como f é uma identidade para A, segue que g também é uma identidade para A com o grau total igual, mas o grau em y_1 e y_2 menor igual do que f em x_1. Note que se em g o grau de x_1 é 1, não há mais o que fazer. Caso o grau de x_1 seja maior ou igual que 2 nessa parcela, basta realizar esse processo mais vezes até obter grau 1. Fazendo esse processo em cada variável e parando quando obtermos um polinômio multilinear, obtemos o desejado. Tal algoritmo é eficiente para encontrar um polinômio multilinear que é consequência de f.

Vejamos um exemplo para ilustrar esse processo.

Exemplo 1.3.26 *Consideremos o polinômio $f(x_1, x_2) = x_1^2x_2 + x_2x_1x_2$, o qual seja uma identidade para uma álgebra A. Aplicando o processo de multilinearização, temos:*

$$\begin{aligned}
g(y_1 + y_2, x_2) &= f(y_1 + y_2, x_2) - f(y_1, x_2) - f(y_2, x_2) \\
&= (y_1 + y_2)^2x_2 + x_2(y_1 + y_2)x_2 - y_1^2x_2 - x_2y_1x_2 - y_2^2x_2 - x_2y_2x_2 \\
&= y_1y_2x_2 + y_2y_1x_2.
\end{aligned}$$

Daí, g é uma identidade multilinear para essa álgebra.

1.3.4 Elementos genéricos e matrizes genéricas

Se A é uma álgebra sobre um corpo K, nós obtemos uma nova álgebra sobre K ao estendermos os escalares, a qual tem suas identidades satisfeitas por A. Em geral, essa álgebra "maior" tem um T-ideal de identidades diferente, no entanto, veremos que isso ocorre essencialmente quando K é finito.

Seja C uma álgebra comutativa com unidade sobre K e consideremos a álgebra $A \otimes C$. Algumas das identidades polinomiais de A ainda podem permanecer sendo identidades em $A \otimes C$. Neste caso, tais identidades recebem um nome especial.

Definição 1.3.27 *Seja f uma identidade para a álgebra A. Nós dizemos que f é uma identidade estável para A se, para toda álgebra comutativa C, f é também uma identidade de $A \otimes C$.*

É claro que se K é um corpo finito, nem toda identidade de K é estável, basta vermos que se $|K| = n$, então $x^n - x = 0$ é uma identidade para K, mas não é identidade em qualquer corpo que seja extensão própria de K. Basta tomar C uma extensão do corpo K com ordem maior do que K, logo $c^n \neq c$, para todo $c \in C$. e observar que para $a \in A$ não nulo,

$$f(a \otimes c) = (a \otimes c)^n - (a \otimes c) = a^n \otimes c^n - a \otimes c = a \otimes c^n - a \otimes c = a \otimes (c^n - c).$$

Portanto, f não é estável.

Vamos agora mostrar que para álgebras sobre corpos infinitos, todas as identidades são estáveis.

Lema 1.3.28 *Se K é um corpo infinito e A é uma K-álgebra, então toda identidade polinomial de A é estável.*

Demonstração: Ver [18, Lemma 1.4.2, pág. 10] ■

Seja A um álgebra de dimensão n sobre um corpo infinito K. Considerando $\{u_1, \ldots, u_n\}$ uma base de A sobre K, tomemos ξ^i_α, com $i \geq 1, 1 \leq \alpha \leq n$, indeterminadas comutativas e considere $K[\xi^i_\alpha \mid i \geq 1, 1 \leq \alpha \leq n]$ a álgebra dos polinômios sobre K nessas indeterminadas. Daí, tome $B = A \otimes K[\xi^i_\alpha]$.

Definição 1.3.29 *Os elementos*

$$\xi^i = \sum_{\alpha=1}^{n} u_\alpha \otimes \xi^i_\alpha, i = 1, 2, \ldots$$

são chamados elementos genéricos de A. A subálgebra $\tilde{A}$ de B gerada por $\xi^1, \xi^2, \ldots$ sobre K é chamada de álgebra dos elementos genéricos de A.

Teorema 1.3.30 *Se K é infinito, a álgebra $\tilde{A}$ é uma álgebra relativamente livre de posto enumerável na variedade $var(A)$, isto é, $\tilde{A} \simeq K\langle X\rangle/T(A)$, onde X é enumerável.*

Demonstração: Sejam $X = \{x_1, x_2, \ldots\}$ e $\psi : K\langle X\rangle \to \tilde{A}$ o homomorfismo induzido pela aplicação $x_i \mapsto \xi^i, i = 1, 2, \ldots$. Devemos provar que $ker\psi = T(A)$. Ora, mas pelo Lema 1.3.28, $T(A \otimes K[\xi^i_j]) = T(A)$, donde $T(A) \subseteq ker\psi$. Suponhamos agora que $g = g(x_1, \ldots, x_n) \in ker\psi$, ou seja, $g(\xi^1, \ldots, \xi^n) = 0$ em $\tilde{A}$ e sejam $a_1, \ldots, a_n \in A$ arbitrários. Como $\{u_1, \ldots, u_m\}$ é base de A, podemos escrever cada a_i da forma

$$a_i = \sum_{j=1}^{m} \lambda^i_j u_j,$$

onde $\lambda_1^i, \ldots, \lambda_m^i \in K$. Como $K[\xi_j^i]$ é a álgebra comutativa livre de posto enumerável, a aplicação $\xi_j^i \mapsto \lambda_j^i$ é estendida a um homomorfismo $K[\xi_j^i] \to K$. Daí, devido a propriedade universal para produto tensorial, a aplicação induzida por $\xi_j^i \mapsto \lambda_j^i$, com $1 \leq i \leq, 1 \leq j \leq m$, pode ser estendida a um homomorfismo $\varphi : A \otimes K[\xi_j^i] \to A$ dado por $\varphi(\xi^i) = a_i$, com $1 \leq i \leq n$. Daí,

$$0 = \varphi(g(\xi^i, \ldots, \xi^n)) = g(\varphi(\xi^1), \ldots, \varphi(\xi^n)) = g(a_1, \ldots, a_n).$$

Como $a_1, \ldots, a_n$ são elementos arbitrários de A, $g(x_1, \ldots, x_n)$ é uma identidade para A e, portanto, $ker\psi = Id(A)$. ■

Um caso especial é quando $A = M_n(K)$ é a álgebra das matrizes de ordem n sobre K. Neste caso, tomando as matrizes unitárias $E_{\alpha\beta}$ como uma base de $M_n(K)$, nós temos a álgebra polinomial $\Delta = K[\xi_{\alpha\beta}^i]$ nas variáveis $\xi_{\alpha\beta}^i$, $i \geq 1$, $1 \leq \alpha, \beta \leq n$. Então $M_n(K) \otimes \Delta \simeq M_k(\Delta)$ e $X_i = \sum_{\alpha,\beta=1}^{n} \xi_{\alpha\beta}^i E_{\alpha\beta}$ é a matriz com entradas $\xi_{\alpha\beta}^i$. Os elementos X_i são chamados de matrizes genéricas de ordem n e, sendo $\mathcal{X} = \{X_1, X_2, \ldots\}$, temos a álgebra $K\langle \mathcal{X} \rangle$ chamada da álgebra das matrizes genéricas sobre K. Utilizando isso e aplicando o Teorema 1.3.30 temos o seguinte:

Corolário 1.3.31 *A álgebra $K\langle \mathcal{X} \rangle$ das matrizes genéricas de ordem n sobre um corpo infinito K é a álgebra relativamente livre de posto enumerável na variedade gerada por $M_n(K)$.*

Daí, concluímos que para verificar se uma dada identidade é satisfeita pela álgebra de matrizes, basta verificar para as matrizes genéricas (isto é, utilizar variáveis em suas entradas). Isto justifica o uso das matrizes genéricas no Capítulo 3.

1.4 Identidades de Newton

Nesta seção, mostraremos que o polinômio característico de uma matriz pode ser escrito em função do seu traço. Para isto, iremos provar as conhecidas Identidades de Newton.

Consideremos $K[t] = K[t_1, \ldots, t_n]$ a álgebra dos polinômios nas indeterminadas comutativas $t_1, \ldots, t_n$. Neste caso, cada permutação $\sigma \in S_n$, determina um automorfismo, denotado por σ, dado por $\sigma(t_i) = t_{\sigma(i)}$, para cada $1 \leq i \leq n$.

Definição 1.4.1 *Os polinômios*

$$e_k = e_k(t_1, \ldots, t_n) = \sum_{1 \leq t_1 \leq \ldots \leq t_k \leq n} t_{i_1} \cdots t_{t_k},$$

com $1 \leq k \leq n$ *são chamados* ***polinômios simétricos elementares****. Além disso,*

$$p_k = p_k(t_1, \ldots, t_n) = t_1^k + \cdots + t_n^k$$

serão chamados ***polinômios potência simétricos****.*

A pergunta natural que podemos fazer diante destes dois tipos polinômios acima definidos é se existe relação entre eles. A resposta é positiva e é isto que nos diz as Identidades de Newton.

Proposição 1.4.2 (Identidades de Newton) *Para cada* $k = 1, \ldots, n$ *temos*

$$ke_k = \sum_{r=1}^{k} (-1)^{r-1} p_r e_{k-r},$$

com $e_0 = 1$*.*

Demonstração: Seja x uma variável qualquer e assim calcularemos a série de potência formal

$$\begin{aligned}
\sum_{r \geq 1} (-1)^{r-1} p_r x^{r-1} &= \sum_{i=1}^{n} \sum_{r \geq 1} (-1)^{r-1} t_i^r x^{r-1} \\
&= \sum_{i=1}^{n} \frac{t_i}{1 + t_i x} \\
&= \sum_{i=1}^{n} \frac{d}{dx} log(1 + t_i x) \\
&= \frac{d}{dx} log(\prod_{i=1}^{n} (1 + t_i x)) \\
&= \frac{d}{dx} log \left(\sum_{k=0}^{n} e_k x^k \right) \\
&= \frac{(\sum_{k=1}^{n} k e_k x^{k-1})}{(\sum_{k=0}^{n} e_k x^k)}.
\end{aligned}$$

Assim,

$$\Big(\sum_{r \geq 1} (-1)^{r-1} p_r x^{r-1} \Big) \cdot \Big(\sum_{k=0}^{n} e_k x^k \Big) = \Big(\sum_{k=1}^{n} k e_k x^{k-1} \Big).$$

Comparando os coeficientes de x^{k-1} em ambos os membros, para $k = 1, \ldots, n$, temos o resultado. ■

Considere C uma álgebra comutativa e $M_n(C) \simeq M_n(K) \otimes C$ a álgebra das matrizes de ordem n com entradas em C. Podemos considerar em $M_n(C)$ a função traço usual $tr : M_n(C) \to C$, ou seja, somando os elementos da diagonal principal. Obtemos, da proposição anterior, o seguinte corolário:

Corolário 1.4.3 *Seja C uma álgebra comutativa sobre K, onde K é uma corpo de característica zero, e $A \in M_n(C)$. Se*

$$f_A(x) = det(xI_n - A) = \sum_{i=0}^{n} \alpha_i x^{n-i}$$

é o polinômio característico da matriz A, então para quaisquer $N = 1, \ldots, n$, temos

$$\alpha_N = \sum_{\lambda \vdash N} q_\lambda tr(A^{\lambda_1}) \cdots tr(A^{\lambda_r}),$$

onde $q_\lambda \in K$ são escalares que não dependem da escolha da matriz A.

Demonstração: Suponhamos inicialmente que C é um domínio de integridade. Então, sendo $A \in M_n(F)$, onde F é o corpo de frações de C, tome $\epsilon_1, \ldots, \epsilon_n$ os seus autovalores em alguma extensão de F, temos que

$$f_A(x) = (x - \epsilon_1) \cdots (x - \epsilon_n) = \sum_{i=0}^{n} (-1)^i e_i(\epsilon_1, \ldots, \epsilon_n) x^{n-i},$$

onde $e_i(\epsilon_1, \ldots, \epsilon_n)$ é a função simétrica elementar avaliada em $\epsilon_1, \ldots, \epsilon_n$. Também, para todo $j = 1, \ldots, n$, onde $\epsilon_1^j, \ldots, \epsilon_n^j$ são os autovalores de A^j, $p_j(\epsilon_1, \ldots, \epsilon_n) = tr(A^j)$, é a soma p_j avaliada em $\epsilon_1, \ldots, \epsilon_n$. A conclusão do corolário para este caso segue das identidades de Newton, aplicando-as uma quantidade finita de vezes.

Consideremos agora $B = K[Y]$ a álgebra relativamente livre na variedade das álgebras comutativas sobre K em um conjunto enumerável Y, a qual é um domínio. Assim, considerando a aplicação

$$\begin{aligned} \alpha : Y &\to C \\ y_i &\mapsto \alpha(y_i) = b_i \end{aligned}$$

segue da definição da álgebra relativamente livre que existe um único homomorfismo φ de B em C, o qual é um epimorfismo que estende α. Disto, φ induz um epimorfismo $\overline{\varphi} : M_n(B) \to M_n(C)$ dado por $\overline{\varphi}(a_{ij}) = (\varphi(a_{ij}))$ para $(a_{ij}) \in M_n(B)$. Daí, para cada $A' \in M_n(B)$, $tr(\overline{\varphi}(A')) = \varphi(tr(A'))$, a conclusão também segue neste caso. ■

1.5 Álgebra com traço

Neste trabalho a álgebra que será objeto principal de estudo é a $M_n(K)$. Como veremos a seguir, ela faz parte de uma classe de álgebras que são conhecidas como álgebras com traço. Nesta seção, iremos definir tais álgebras, assim como as identidades com traço, e construir a álgebra livre nas classes das álgebras associativas com traços.

Definição 1.5.1 *Dadas uma álgebra associativa A, dizemos que uma aplicação linear $tr : A \to A$ é uma aplicação traço na álgebra A se, para todos $a, b \in A$, valem:*

(i) $tr(a)b = btr(a)$;

(ii) $tr(tr(a)b) = tr(a)tr(b)$;

(iii) $tr(ab) = tr(ba)$.

O par (A, tr) é chamada ***álgebra com traço****.*

Exemplo 1.5.2 *A álgebra $M_n(K)$ das matrizes de ordem n munida da função traço usual de matrizes tr, ou seja, $tr(A)$ é a soma de todos os elementos da diagonal da matriz A, é uma álgebra com traço. Mais geralmente, seja C uma álgebra comutativa C, a aplicação traço definido antes do Corolário 1.4.3 é um exemplo de traço sobre $M_n(C)$.*

Exemplo 1.5.3 *Defina sobre a álgebra $M_n(E)$, álgebra das matrizes de ordem n sobre a álgebra de Grassmann E, uma aplicação dada por $qtr\colon M_n(E) \to E$ obtida somando apenas as componentes de E_1 nas entradas de sua diagonal. Não é difícil observar que essa aplicação satisfaz as propriedades (ii) e (iii) da definição de traço. Porém, não satisfaz a condição $qtr(M_n(E)) \subseteq Z(M_n(E))$, uma vez que pelo item (i) a imagem do traço deve estar no centro. Concluindo que $(M_n(E), qtr)$ não é um álgebra com traço. Por este motivo, a aplicação "qtr" é chamada de quase traço, e uma conversa detalhada sobre tal assunto pode ser encontrada em [8].*

Exemplo 1.5.4 *Seja "tr" a aplicação traço dada antes do Corolário 1.4.3. Considere a subálgebra $M_{a,b}(E)$ da álgebra $M_{a+b}(E)$ dada no Exemplo 1.1.18. Podemos definir sobre $M_{a,b}(E)$ a aplicação $ptr\colon M_{a,b}(E) \to E_0$ dada por*

$$ptr\begin{pmatrix} A & B \\ C & D \end{pmatrix} = tr(A) + tr(D).$$

Não é difícil observar que essa aplicação satisfaz quase todas as propriedades da definição de traço, exceto a propriedade cíclica, isto é, $tr(AB) = tr(BA)$. Porém, verifica-se que a aplicação $mtr\colon M_{a,b}(E) \to E_0$ dada por

$$mtr\begin{pmatrix} A & B \\ C & D \end{pmatrix} = tr(A) - tr(D)$$

satisfaz todas as propriedades da definição anterior. Assim $(M_{a,b}(E), ptr)$ não é uma álgebra com traço, mas $(M_{a,b}(E), mtr)$ é. Para maiores detalhes sobre a álgebra com traço $(M_{a,b}(E), mtr)$ mencionamos a referência [5].

Considerando (A, tr) uma álgebra com traço chamaremos de **álgebra de traços puro** a imagem de A por tr, denotado por $tr(A)$. Segue da definição da aplicação traço que $tr(A)$ é uma subálgebra de $Z(A)$. Um ideal (resp. subálgebra) em uma álgebra com traço é um **ideal com traço** (resp. **subálgebra com traço**) se é um ideal (resp. subálgebra) tr-invariante.

Definição 1.5.5 *Sejam (A, τ) e (B, θ) álgebras com traço, onde A e B são álgebras com unidade. Uma aplicação $\varphi\colon A \to B$ será chamada um **homomorfismo entre álgebras com traço**, se φ é um homomorfismo de álgebras e $\varphi(\tau(a)) = \theta(\varphi(a))$, para todo $a \in A$.*

Pode-se construir a álgebra associativa livre com traço sobre o conjunto X da seguinte forma: Denotando por $\mathcal{M}$ o conjunto de todos os monômios em $K\langle X\rangle$, podemos definir um símbolo formal $Tr(v)$ para todo v elemento em $\mathcal{M}$. Assim, $K\langle X \cup Tr(\mathcal{M})\rangle$ denotará a álgebra associativa livre livremente gerada pelo conjunto X junto com os símbolos $Tr(v)$, para todo $v \in \mathcal{M}$. Note que a existência da álgebra relativamente livre em $K\langle X \cup Tr((M))$ com traço, denotada por $KTR\langle X\rangle$, é construída pelo Teorema 1.3.13 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) $Tr([a, b])$; e,

v) $[Tr(a), b]$,

para todo a, b, $c \in \mathcal{M}$. O símbolo formal Tr será chamado de **traço formal sobre** $K\langle X\rangle$.

Seja (A, tr) uma álgebra unitária na classe das álgebras com traço. Pela definição da álgebra livre $K\langle X\rangle$, uma aplicação $\mu\colon X \to A$ dada por $\mu(x_i) = a_i$ pode ser estendida para um homomorfismo $\varphi\colon K\langle X\rangle \to A$. Segue que, na álgebra relativamente livre $KTR\langle X\rangle$, obtemos um homomorfismo $\varphi : KTR\langle X\rangle \to A$, tal que

$$\tilde{\varphi}(Tr(x_{i_1}\cdots x_{i_n})) = tr(a_{i_1}\cdots a_{i_n}),$$

para toda palavra $x_{i_1}\cdots x_{i_n}$ em $\mathcal{M}$. Considerando a linearidade da aplicação Tr, temos que $KTR\langle X\rangle$ é a **álgebra livre com traço na classe das álgebras unitárias com traço** 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 omissão dessa variável (ou expressão) no lugar indicado em f. A subálgebra $G\langle X\rangle$ em $KTR\langle X\rangle$ gerada pelo conjunto

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

é chamada **álgebra de polinômios generalizados** e seus elementos serão chamados de **polinômios com traço**. Claramente, $G\langle X\rangle$ é gerado como espaço vetorial pelos monômios generalizados da forma

$$\widehat{a}_0 Tr(a_1)\cdots Tr(a_s), \tag{1.1}$$

onde os a_i's são palavras em $\mathcal{M}$ e $a_1, \ldots, a_s$ são não vazias. Note que a representação de elementos da forma (1.1) não é única, mas é fácil contornar esse problema, basta tomar como representante de uma classe de elementos congruentes da forma (1.1) o elemento tal que a palavra $a_0a_1\cdots a_t$ é máxima no sentido de uma ordem dada $(a_1 > \ldots > a_n)$. Além disso, cada elemento de $G\langle X\rangle$ é chamado de **polinômio com traço** e se um elemento de $G\langle X\rangle$ for um combinação linear de elementos dada na expressão (1.1) o qual o termo a_0, em cada parcela, não ocorrer, dizemos que tal elemento é um **polinômio com traço puro**. O conjunto de todos os polinômios com traço puro será denotado por $TG\langle X\rangle$. É claro que $TG\langle X\rangle$ é uma subálgebra de $G\langle X\rangle$. É bem verdade que $G\langle X\rangle$ tem estrutura de $TG\langle X\rangle$-módulo.

Definição 1.5.6 *Seja (A, tr) uma álgebra com traço. Dizemos que um polinômio com traço $f(x_1,\ldots,x_n)\in G\langle X\rangle$ é uma* ***identidade com traço*** *para (A, tr), se substituindo Tr por tr, obteremos $f(a_1,\ldots,a_n)=0$ para qualquer $a_1, \ldots, a_n \in A$.*

Tendo essa estrutura em $G\langle X\rangle$, nós podemos definir a noção de um T-ideal com traço.

Definição 1.5.7 *a) Um T-ideal com traço I de $G\langle X\rangle$ é um ideal que é fechado sobre Tr e sobre todas as substituições.*

b) Um T-ideal com traço J de $TG\langle X\rangle$ é um ideal fechado sobre as substituições.

Facilmente se verifica que dado qualquer $A \subseteq G\langle X\rangle$, existe um T-ideal com traço minimal de $G\langle X\rangle$ contendo A e ele é o ideal gerado pelos elementos obtidos de A ao fazer todas as possíveis substituições e assumindo os valores Tr. Similarmente para $B \subseteq TG\langle X\rangle$. Referiremos a esse ideal como o T-ideal com traço gerado por A em $G\langle X\rangle$ (respectivamente, por B em $TG\langle X\rangle$).

Observe que para qualquer álgebra com traço (A, tr), o ideal de todas as suas identidades com traço é um T-ideal com traço, denotado por $T_{Tr}(A, tr)$ ou simplesmente por $T_{Tr}(A)$, quando não houver duvida sobre qual aplicação traço estamos trabalhando. 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 $g_i \equiv 0, i \in \Lambda$.

Consideremos a álgebra das matrizes de ordem n com o traço usual $(M_n(K), tr)$. Dada $A \in M_n(K)$ podemos considerar o seu polinômio característico dado por

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

onde seus coeficiente dependem de $tr(A^j)$, para $j = 1, \ldots, n$ (ver Corolário 1.4.3). Pelo famoso Teorema de Cayley-Hamilton, temos $\chi_A(A) = 0$, além disso, temos que $deg\chi_A(\lambda) = n$. Assim, considerando x uma indeterminada qualquer em X, podemos chamar $f_n(x) = \chi_x(x) \in G\langle X\rangle$ de polinômio de Cayley-Hamilton de grau n.

Exemplo 1.5.8 *Seja $A = M_n(K)$ a álgebra das matrizes de ordem n sobre K munida da aplicação traço usual "tr". A identidade de Cayley-Hamilton de grau n é uma identidade com traço pra a álgebra (A, tr).*

No próximo capítulo estudaremos de forma mais detalhada as identidades com traço, onde nosso objetivo será mostrar que, sobre um corpo de característica zero, toda identidade com traço para $(M_n(K), tr)$ segue da identidade de Cayley-Hamilton de grau n.

Observação 1.5.9 *As definições e resultados que se encontram na Seção 1.3, com mínimas adaptações, continuam sendo válidas para álgebras com traço.*

1.6 Representação de grupos

Uma vez que a Teoria de Invariantes tem a ação de grupo como assunto base, decidimos revisar a definição de ação e exemplificar com as ações que serão usadas no decorrer do trabalho. Ademais, definiremos estabilizador e órbita.

Definição 1.6.1 *Seja G um grupo e X um conjunto não vazio. Dizemos que uma aplicação*

$$\begin{aligned} \pi : G \times X &\rightarrow X \\ (g,x) &\mapsto \pi(g,x) = g \cdot x \end{aligned}$$

é uma ação de G em X se satisfaz as seguintes condições:

1) $1 \cdot x = x$, para todo $x \in X$ (1 denota o elemento neutro do grupo G);

2) $h \cdot (k \cdot x) = (hk) \cdot x$, para todo $h, k \in G$.

Exemplo 1.6.2 *Tomando $X = G$ e π como a operação do grupo temos uma ação como definido acima.*

Exemplo 1.6.3 *Se G é um grupo, a aplicação*

$$\begin{aligned} \rho_1 : G \times G &\rightarrow G \\ (g,x) &\mapsto g \cdot x = gxg^{-1} \end{aligned}$$

*é uma ação de G em si mesmo chamada de **ação por conjugação**.*

Exemplo 1.6.4 *Dado $G = GL(V)$, a aplicação*

$$\begin{aligned} \rho_2 : G \times V^{\otimes i} &\rightarrow V^{\otimes i} \\ (A, v_1 \otimes v_2 \otimes \cdots \otimes v_i) &\mapsto A \cdot (v_1 \otimes v_2 \otimes \cdots \otimes v_i) = Av_1 \otimes Av_2 \otimes \cdots \otimes Av_i \end{aligned}$$

*é uma ação de G em $V^{\otimes i}$ chamada de **ação diagonal**. Neste caso $G \subseteq End(V^{\otimes i})$.*

Exemplo 1.6.5 *A aplicação*

$$\begin{aligned} \rho_2 : S_n \times End(V^{\otimes i}) &\rightarrow End(V^{\otimes i}) \\ (\sigma, v_1 \otimes v_2 \otimes \cdots \otimes v_i) &\mapsto \sigma \cdot (v_1 \otimes v_2 \otimes \cdots \otimes v_i) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(i)} \end{aligned}$$

*é uma ação de S_n em $End(V^{\otimes i})$ chamada de **ação simétrica**.*

Exemplo 1.6.6 *Seja P_n o subespaço dos polinômios multilineares de $K\langle X\rangle$ nas variáveis $x_1, x_2, \ldots, x_n$. Temos que $\beta = \{x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(n)} \mid \sigma \in S_n\}$ é uma base de P_n. Considere a aplicação bilinear $\cdot\colon KS_n \times P_n \to P_n$ que satisfaz*

$$\sigma \cdot (x_{i_1}x_{i_2}\cdots x_{i_n}) = x_{\sigma(i_1)}x_{\sigma(i_2)}\cdots x_{\sigma(i_n)}$$

onde $\sigma \in S_n$ e $x_{i_1}x_{i_2}\cdots x_{i_n} \in \beta$, com $\{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$. Munido desse produto, "$\cdot$" é uma ação de S_n em P_n.

Definição 1.6.7 *Sejam $\pi : G \times X \to X$ uma ação de G em X e $x \in X$. Definimos a órbita de x por π (ou π-órbita de x) e o estabilizador de x em relação a π , denotados respectivamente por $\mathcal{O}_\pi(x)$ e $St_\pi(x)$, como sendo*

$$\mathcal{O}_\pi(x) = \{g \cdot x \mid g \in G\} \text{ e } St_\pi(x) = \{g \in G \mid g \cdot x = x\}.$$

Exemplo 1.6.8 *Considerando S_n o grupo das permutações de n elementos e ação por conjugação (vamos denotá-la por ρ), temos $St_\rho(\pi) = C_{S_n}(\pi)$ e a órbita de x é $\mathcal{O}_\rho(\pi) = \{\sigma\pi\sigma^{-1} \mid \sigma \in S_n\}$. (Este último conjunto é chamado de classe de conjugação de π em S_n)*

Exemplo 1.6.9 *Um fato conhecido da Teoria de grupos é que*

$$\alpha(i_1 i_2 \ldots i_k)\alpha^{-1} = (\alpha(i_1)\alpha(i_2)\ldots\alpha(i_k))$$

para todo $k \in \mathbb{N}$ e todo $\alpha \in S_n$. Assim, duas permutações σ e θ de S_n de mesmo tipo se, e somente se, estão na mesma órbita.

Daremos continuidade ao assunto título desta subseção.

Definição 1.6.10 *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.

Definição 1.6.11 *Sejam G um grupo, V e W espaços vetoriais e φ e ψ representações de G em V e W, respectivamente. Dizemos que φ e ψ são equivalentes se existe uma transformação linear $T : V \to W$ bijetora tal que $\psi_g T = T\varphi_g$, para todo $g \in G$.*

Exemplo 1.6.12 *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. Recordamos que $End(V)$ denotará a álgebra dos K-endomorfismos de V. Considerando a álgebra de grupo KG e ρ uma representação de G em V, segue que ρ induz um homomorfismo de K-álgebras $\rho' \colon KG \to End(V)$ tal que $\rho'(1_G) = 1$.

Observação 1.6.13 *Uma representação do grupo G determina KG-módulo (ou G-módulo) de modo único, da seguinte forma: Se $\rho \colon G \to GL(V)$ é uma representação de G, V torna-se um G-módulo (à esquerda) definindo $gv = \rho(g)(v)$, para quaisquer $g \in G$, $v \in V$. Reciprocamente, se M é um G-módulo, então $\rho \colon G \to GL(M)$ tal que $\rho(g)(m) = gm$, para $g \in G$, $m \in M$, é possível definir uma representação de G em M, por extensão. Aqui M está sendo visto com seus escalares sobre K, ou seja, M é um espaço vetorial.*

Da Definição 1.6.10 e pela observação anterior, podemos considerar que V é um G-módulo e consequentemente dizemos que φ é uma **representação simples** (semissimples) se V é um G-módulo simples (semissimples). Neste contexto, o Teorema de Maschke (ver Teorema 1.2.11) pode ser reescrito para a versão de representação. Além disso, é possível demonstrar que a quantidade de representações simples de um grupo finito 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 [22, Seção 5.3, pág. 261]).

A demonstração do resultado principal do Capítulo 3, faz uso dos G-módulos semissimples sobre um corpo de característica zero. Caso G seja finito o resultado segue do Teorema de Maschke, porém para o caso em que G é infinito não é tão óbvio. Nosso objetivo no decorrer desta seção, é conhecer o conceito de representação racional do grupo $GL_n(K)$ e sua aplicação em módulos.

Seja V um espaço vetorial m-dimensional. Denotamos como $GL_m(K) = GL_m$ o grupo das matrizes invertíveis de ordem m com entradas em K isomorfo à $GL(V)$.

Definição 1.6.14 *Uma representação do grupo GL_m de grau s, digamos a aplicação $\varphi \colon GL_m \to GL_s$, é dita* **racional** *(ou polinomial) se as entradas $(\varphi(g))_{pq}$ da matriz $\varphi(g)$ de ordem s são polinômios nas entradas a_{kl}, para $g \in GL_m$; k, $l = 1, \ldots, m$ e p,*

$q = 1, \ldots, s$. Uma representação racional φ é **homogênea** *de grau d se os polinômios $(\varphi(g))_{pq}$ são homogêneos de grau d. Um GL_m-módulo W é* **racional** *(ou polinomial), se a representação correspondente é polinomial. De forma análoga, definimos módulos polinomiais homogêneos.*

Fixemos o espaço vetorial V_m com base $\{x_1, \ldots, x_m\}$ e com a ação canônica de GL_m. Assumimos que

$$K\langle V_m\rangle = K\langle x_1, \ldots, x_m\rangle$$

é a álgebra livre gerada por $\{x_1, \ldots, x_m\}$. O espaço vetorial $K\langle V_m\rangle$ é um GL_m-módulo à esquerda quando munido da ação:

$$gf(x_1, \ldots, x_m) = f(g(x_1), \ldots, g(x_n)), g \in GL_m, f(x_1, \ldots, x_m) \in K\langle V_m\rangle.$$

Observação 1.6.15 *Uma importante questão a observar é que tais estruturas dependem mais da estrutura do espaço vetorial, do que da multiplicação da álgebra.*

Teorema 1.6.16 *[13, Seção 12.4] Toda representação racional de GL_m é soma direta de subrepresentações polinomiais homogêneas irredutíveis.*

Este resultado é suficiente para ser aplicado no resultado principal do Capítulo 3.

1.7 O grupo simétrico e teoria de Young

Nesta seção K denotará um corpo de característica zero.

Definição 1.7.1 *Dado $n \in \mathbb{N}$, definimos uma partição λ de n como sendo uma k-upla $\lambda = (\lambda_1, \ldots, \lambda_k)$, com $\lambda_i \in \mathbb{N}$, tal que $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k$ e $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$.*

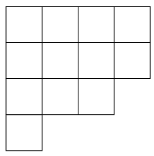
Usaremos a notação $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \vdash n$ para dizer que λ é uma partição de n.

Observação 1.7.2 (Ordem Lexicográfica) *Sendo λ_1 e λ_2 partições do mesmo número natural n, escreva $\lambda_1 = (n_1, n_2, \ldots, n_r, 0, 0, \ldots)$ e $\lambda_2 = (m_1, m_2, \ldots, m_s, 0, 0, \ldots)$. Dizemos que $\lambda_1 > \lambda_2$ se $n_k > m_k$ para $k = min\{i \in \mathbb{N} \mid n_i \neq m_i\}$ (ordem lexicográfica). É fácil verificar que essa é uma relação de ordem total sobre as partições do número n.*

Definição 1.7.3 *Sendo $\lambda = (n_1, n_2, \ldots, n_k) \vdash n$, definimos o diagrama de Young D_λ da partição λ como sendo o conjunto $D_\lambda = \{(i, j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i \leq k, 1 \leq j \leq n_\lambda\}$.*

Representamos D_λ por n quadrados (células) dispostas em k filas horizontais, chamadas de linhas, onde a i-ésima linha é composta por n_i células. Da esquerda para a direita os primeiros quadrados de cada linha aparecem em uma mesma fila vertical, a qual é chamada de coluna. Deste modo, a célula correspondente ao elemento $(i, j) \in D_\lambda$ está na i-ésima linha e j-ésima coluna. No decorrer do texto, vamos identificar o elemento (i, j) com a correspondente célula.

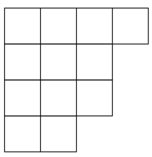
Exemplo 1.7.4 *Considerando* $\lambda = (4, 4, 3, 1)$ *uma partição do número* 12*, o diagrama de Young* D_λ *é:*

$D_\lambda =$ 

Da teoria de grupos, já sabemos que o número de classes de conjugação de S_n coincide com o número de partições de n, deste modo podemos associar uma partição $\lambda = (\lambda_1, \ldots, \lambda_k)$ às classes de conjugação de uma permutação constituindo dos ciclos disjuntos de tamanhos $\lambda_1, \ldots, \lambda_k$.

Definição 1.7.5 *Seja* λ *uma partição de* n *e* D_λ *o seu diagrama. Definimos o diagrama conjugado de* D_λ *(ou, o diagrama dual de* λ*), como sendo o diagrama* $D_{\lambda'}$ *obtido trocando-se as linhas de* D_λ *por suas colunas, e as suas colunas por suas linhas. A partição conjugada de* λ *será a partição* λ' *do diagrama* $D_{\lambda'}$

Exemplo 1.7.6 *Sendo* $\lambda = (4, 4, 3, 1)$ *uma partição de* 12*, temos* $\lambda' = (4, 3, 3, 2)$ *e*

$D_{\lambda'} =$ 

Definição 1.7.7 *Sejam* $n \in \mathbb{N}$*,* $I_n = \{1, 2, \ldots, n\}$ *e* $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \vdash n$*. Definimos uma tabela de Young como sendo uma bijeção* $T_\lambda : D_\lambda \to I_n$*. Dizemos que* T_λ *é* ***Standard*** *se*

(i) $T(i, j) < T(i, j+1)$ *para* $1 \leq i \leq k$ *e* $1 \leq j < \lambda_i$*;*

(ii) $T(i, j) < T(i+1, j)$ *para* $1 \leq i < k$ *e* $1 \leq j \leq \lambda_{i+1}$*.*

Em outras palavras, dada λ uma partição de n, uma tabela de Young T_λ será o diagrama D_λ preenchido com o valor $T(i, j) \in I_n$ na posição (i, j), para cada $(i, j) \in D_\lambda$ e uma **tabela Standard T** será uma tabela onde os valores crescem da esquerda para a direita, em cada linha, e de cima para baixo, em cada coluna.

Exemplo 1.7.8 *Sendo* $\lambda = (3,1,1,1) \vdash 6$, *consideremos a seguinte Tabela de Young associada a essa partição*

$$T_\lambda = \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 \\ \cline{1-1} 5 \\ \cline{1-1} 6 \\ \cline{1-1}\end{array}.$$

Pelo que foi definido acima, T_λ *é uma tabela Standard. Por outro lado, considerando esta mesma partição, vemos que a seguinte tabela de Young*

$$T_\lambda^* = \begin{array}{|c|c|c|}\hline 1 & 5 & 3 \\ \hline 4 \\ \cline{1-1} 6 \\ \cline{1-1} 2 \\ \cline{1-1}\end{array}$$

não é Standard.

Observação 1.7.9 *Dado* $\alpha \in S_n$, *definimos* αT *como sendo a composição* $\alpha \circ T$. *Assim, dadas duas tabelas* T_1, T_2 *associadas ao mesmo diagrama, existe* $\alpha \in S_n$ *tal que* $T_2 = \alpha T_1$.

Exemplo 1.7.10 *Dada a tabela de Young*

$$T_1 = \begin{array}{|c|c|c|c|}\hline 1 & 4 & 7 & 3 \\ \hline 2 & 6 \\ \cline{1-2} 5 & 8 \\ \cline{1-2} 9 \\ \cline{1-1}\end{array}$$

e a permutação $\sigma = (1342)(65)(78) \in S_9$, *temos*

$$\sigma T_1 = \begin{array}{|c|c|c|c|}\hline 3 & 2 & 8 & 4 \\ \hline 1 & 5 \\ \cline{1-2} 6 & 7 \\ \cline{1-2} 9 \\ \cline{1-1}\end{array}.$$

Definição 1.7.11 *Dada uma tabela de Young* $T : D_\lambda \to I_n$, *para* $\lambda \vdash n$, *definimos os seguintes subgrupos de* S_n:

$$P_T = \{\sigma \in S_n \mid \sigma(L) = L, \text{ para toda linha } L \text{ de } T\}$$

e

$$Q_T = \{\sigma \in S_n \mid \sigma(C) = C, \text{ para toda coluna } C \text{ de } T\},$$

onde P_T *é o estabilizador linha e* Q_T *é o estabilizador coluna.*

Exemplo 1.7.12 *Considerando a tabela* T_1 *do exemplo anterior, temos*

$$P_{T_1} = S_{\{1,4,7,3\}} \times S_{\{2,6\}} \times S_{\{5,8\}} \times \{9\} = S_{\{1,4,7,3\}} \times S_{\{2,6\}} \times S_{\{5,8\}}$$

e

$$Q_{T_1} = S_{\{1,2,5,9\}} \times S_{\{4,6,8\}} \times \{7\} \times \{3\} = S_{\{1,2,5,9\}} \times S_{\{4,6,8\}}.$$

Observe que diferentes tabelas de Young para a mesma partição λ definem diferentes subgrupos P_T e Q_T. Usando esses subgrupos, para cada tabela de Young T de uma partição λ de n, definimos os seguintes elementos da Álgebra de Grupo KS_n

$$a_T := \sum_{\sigma \in P_T} \sigma, b_T := \sum_{\sigma \in Q_T} sgn(\sigma)\sigma \text{ e } c_T := a_T.b_T,$$

onde o último elemento, c_T, é chamado **Simetrizador de Young.**

Observe que $P_T \cap Q_T = \{Id\}$ e então cada elemento de S_n pode ser escrito em mais de uma maneira como produto de $p \in P_T$ e $q \in Q_T$. Em particular, o simetrizador de Young pode ser escrito como $c_T = \sum \pm\sigma$ com $\sigma = p.q$ para únicos p e q, e o coeficiente $\pm 1 = sgn(q)$.

Veremos algumas propriedades e resultados dos objetos até aqui definidos nesta seção. Iremos omitir tais demonstrações por se tratar de serem clássicos na teoria, mas todas elas podem se encontradas em [17, Subseção 4.2, pág. 52].

Lema 1.7.13 *Sejam $n \in \mathbb{N}$ e T uma tabela de Young do diagrama de uma partição λ de n. Valem:*

(i) Se $\sigma_1, \sigma_2 \in P_T, \mu_1, \mu_2 \in Q_T$ e $\sigma_1\mu_1 = \sigma_2\mu_2$, então $\sigma_1 = \sigma_2$ e $\mu_1 = \mu_2$.

(ii) $P_{\sigma T} = \sigma P_T \sigma^{-1}$ e $Q_{\sigma T} = \sigma Q_T \sigma^{-1}$, para todo $\sigma \in S_n$.

(iii) $a_{\sigma T} = \sigma a_T \sigma^{-1}, b_{\sigma T} = \sigma b_T \sigma^{-1}$ e $c_{\sigma T} = \sigma c_T \sigma^{-1}$, para todo $\sigma \in S_n$.

(iv) $a_T\sigma = \sigma a_T = a_T$ e $\sigma c_T = c_T$, para todo $\sigma \in P_T$.

(v) $b_T\sigma = \sigma b_T = sgn(\sigma)b_T$ e $c_T\sigma = sgn(\sigma)c_T$, para todo $\sigma \in Q_T$.

(vi) $p.c_T.sgn(q)q = c_T$, onde c_T é o único elemento em KS_n, a menos de escalar, satisfazendo essa propriedade, $p \in P_T$ e $q \in Q_T$.

Demonstração: Os itens (i) - (iii) são obtidos diretamente. Já a demonstração dos outros itens pode ser encontrados em [17, Lemma 4.21]. ■

Lema 1.7.14 *Sejam λ_1, λ_2 partições de uma número natural d e T_1 e T_2 tabelas de Young dos diagramas D_{λ_1} e D_{λ_2}, respectivamente. Se existem dois elementos pertencentes simultaneamente a uma mesma linha de T_2 e a uma mesma coluna de T_1, então $b_{T_1}a_{T_2}$ é zero e, consequentemente, $c_{T_1}c_{T_2} = 0$.*

Demonstração: Sejam $i, j \in I_d$ elementos pertencentes a uma mesma linha de T_2 e a uma mesma coluna de T_1. Então, $\beta = (ij) \in P_{\lambda_2} \cap Q_{\lambda_1}$ e, assim, pelo Lema 1.7.13, $b_{T_1} = -b_{T_1}\beta$ e $\beta a_{T_2} = a_{T_2}$. Desta forma,

$$b_{T_1}a_{T_2} = -b_{T_1}\beta\beta a_{T_2} = -b_{T_1}a_{T_2} \Rightarrow b_{T_1}a_{T_2} = 0.$$

A segunda afirmação segue do fato que $c_{T_1}c_{T_2} = a_{T_1}b_{T_1}a_{T_2}b_{T_2} = 0$. ■

Proposição 1.7.15 *Sejam $\alpha \in S_n$, λ, λ_1 e λ_2 partições de n e T, T_1 e T_2 tabelas de Young dos diagramas D_λ, D_{λ_1} e D_{λ_2}, respectivamente. Então, valem:*

a) Existe $\gamma \in K$ tal que $c_T\alpha c_T = \gamma c_T$.

b) Se $\lambda_1 > \lambda_2$, então $c_{T_1}\alpha c_{T_2} = 0$.

Demonstração: Ver [17, Lemma 4.23] ■

Para cada $\alpha \in KS_n$, consideremos o operador linear $\mathcal{F} : KS_n \to KS_n$ definido por $\mathcal{F}_\alpha(x) = x\alpha$. Sendo $\alpha = \sum_{\rho \in S_n} \gamma_\rho \rho$, teremos que $\mathcal{F}_\alpha = \sum_{\rho \in S_n} \gamma_\rho \mathcal{F}_\rho$ e, nestas condições, $tr\mathcal{F}_\alpha = \sum_{\rho \in S_n} \gamma_\rho tr\mathcal{F}_\rho$. Não é difícil observar que $tr\mathcal{F}_\rho = 0$, para todo $\rho \in S_n \setminus \{Id\}$, e também que $tr\mathcal{F}_{Id} = dim_K KS_n = n!$.

Sendo T uma tabela de Young, temos

$$tr\mathcal{F}_{c_T} = \sum_{p \in P_T, q \in Q_T} (-1)^q tr\mathcal{F}_{pq} = n!$$

uma vez que $pq = Id$ se, e somente se, $p = q = Id$. (Ver Lema 1.7.13). Além disso, do lema anterior temos que $c_T^2 = ac_T$, para algum $a \in K$. Caso $a = 0$, teríamos $c_T^2 = 0$ e

$$\mathcal{F}_{c_T^2}(x) = xc_T^2 = (xc_T)c_T = \mathcal{F}_{c_T}^2(x),$$

consequentemente, $\mathcal{F}_{c_T}^2 = 0$, implicando que $\mathcal{F}_{c_T}$ é nilpotente e daí $tr\mathcal{F}_{c_T} = 0$, o que seria uma contradição. Devemos então ter $a \neq 0$. Assim, tomando $e_T = a^{-1}c_T$, temos

$$e_T^2 = a^{-2}c_T^2 = a^{-2}(ac_T) = a^{-1}c_T = e_T.$$

Considerando agora

$$V_T = KS_nc_T = \{\alpha c_T \mid \alpha \in KS_n\} = KS_ne_T.$$

Observe que V_T é um ideal à esquerda de KS_n e, é portanto, um submódulo de KS_n. Sabemos que $\gamma Id_{V_T} \in End_{KS_n}V_T$, para todo $\gamma \in K$. Tomando agora $\varphi \in End_{KS_n}V_T$, observe que $\varphi(e_T) = \alpha e_T$, para algum $\alpha \in KS_n$, temos agora, então

$$\varphi(e_T) = \varphi(e_T e_T) = e_T\varphi(e_T) = e_T\alpha e_T = \gamma e_T,$$

para alguma $\gamma \in K$. Assim, para todo $x \in V_T$, temos que $x = \beta e_T$, para algum $\beta \in KS_n$, V_T visto com S_n módulo, e daí

$$\varphi(x) = \varphi(\beta e_T) = \beta\varphi(e_T) = \beta\gamma e_T = \gamma x.$$

Concluímos que $\varphi = \gamma Id_{V_T}$ e consequentemente $End_{KS_n}V_T = \{\alpha Id_{V_T} \mid \alpha \in K\}$. Portanto, $End_{KS_n}V_T$ é isomorfo ao corpo K.

Teorema 1.7.16 *Seja $d \in \mathbb{N}, \lambda, \lambda_1$ e λ_2 partições de d e T, T_1 e T_2 tabelas de Young associadas aos diagramas D_λ, D_{λ_1} e D_{λ_2}, respectivamente. Então:*

a) V_T é uma S_n-módulo simples;

b) V_{T_1} e V_{T_2} são S_n-módulos simples isomorfos se, e somente se, $\lambda_1 = \lambda_2$.

Demonstração: *a*) Seja W_T um submódulo de V_T. Como toda S_n-representação é completamente redutível (pelo Teorema de Maschke), então deve existir W_1 submódulo de V_T tal que $V_T = W_T \oplus W_1$. Tomando a aplicação

$$\begin{aligned} \varphi : V_T \ &\to V_T \\ \alpha + \beta \quad &\mapsto \quad \varphi(\alpha + \beta) = \alpha, \end{aligned}$$

para $\alpha \in W_T$ e $\beta \in W_1$, temos que $\varphi \in End_{KS_n}V_T$ e $\varphi^2 = \varphi$. Como $End_{KS_n}V_T$ é isomorfo ao corpo, temos $\varphi = 0$ ou $\varphi = Id$, e assim, $W_T = \{0\}$ ou $W_T = V_T$. Logo, V_T é simples.

b) Sendo $\lambda_1 \neq \lambda_2$, suponhamos sem perda de generalidade que $\lambda_1 > \lambda_2$. Segue do último lema que $e_{T_1}\alpha e_{T_2} = 0$, para todo $\alpha \in KS_n$. Seja $\varphi\colon V_{T_1} \to V_{T_2}$ um homomorfismo de S_n-módulos. Neste caso, existe $\alpha \in KS_n$ tal que $\varphi(e_{T_1}) = \alpha e_{T_2}$. Nestas condições,

$$\varphi(e_{T_1}) = \varphi(e_{T_1}e_{T_1}) = e_{T_1}\varphi(e_{T_1}) = e_{T_1}\alpha e_{T_2} = 0$$

e consequentemente $\varphi = 0$. Assim, V_{T_1} e V_{T_2} não são isomorfos.

Reciprocamente, suponha que $\lambda_1 = \lambda_2$. Temos então que $T_1 = \rho T_2$, para algum $\rho \in S_n$. Do Lema 1.7.13 temos que $e_{T_1} = a\rho e_{T_2}\rho^{-1}$, para algum $a \in K$. Logo,

$$V_{T_1} = V_{T_2}\rho^{-1} \simeq V_{T_2},$$

como queríamos demonstrar. ■

1.8 Funções polinomiais e funções invariantes

Consideremos o anel de polinômios $K[t_1, \ldots, t_n]$ com coeficientes em K, podemos ver cada t_i como funções coordenadas em K^n, isto é, $t_i(x) = x_i$, quando $x = (x_1, \ldots, x_n)$. Isso sugere o seguinte: dado um espaço vetorial V de dimensão finita, denotamos por $K[V]$ a K-álgebra comutativa gerada pelo espaço dual V^*. Fixando uma base para V e denotando por t_i o i-ésimo elemento da base dual à base canônica de $V = K^n$, $K[V]$ consiste dos polinômios em t_i. Tal anel é chamado de **anel das funções polinomiais** e seus elementos são **funções polinomiais**.

Um tipo importante de funções polinomiais são as funções invariantes, as quais são definidas como segue.

Definição 1.8.1 *Seja G o grupo das transformações invertíveis de um espaço V. Uma função $f \in K[V]$ é chamada G-invariante, ou invariante, se $f(gv) = f(v)$ para todo $g \in G$ e $v \in V$. Os invariantes formam uma subálgebra de $K[V]$ chamada de anel invariante e é denotada por $K[V]^G$.*

Como a órbita de $v \in V$ é definida pelo subconjunto $G_V := \{gV \mid g \in G\} \subset V$, é claro que uma função é G-invariante se, e somente se, é constante em todas as órbitas de G em V.

Um outro caminho para descrever o anel invariante é considerar a ação linear de G no anel $K[V]$,

$$(g, f) \mapsto gf, gf(v) := f(g^{-1}v) \text{ para } g \in G, f \in K[V], v \in V.$$

Como afirmado em [27], esta descrição é comumente chamada de representação regular de G no anel das funções polinomiais. (A inversa g^{-1}, nesta definição, é necessária a fim de obtermos uma ação à esquerda no espaço das funções). Claramente uma função f é invariante, se e somente se, é um ponto fixo sobre esta ação, isto é, $gf = f$ para todo $g \in G$. Isso explica a notação $K[V]^G$ para o anel dos invariantes.

Exemplo 1.8.2 *Considerando $SL_n(K)$ o grupo das matrizes com determinante igual a 1, temos a ação de $SL_n(K)$ em $GL_n(K)$ dada por $(A, B) \mapsto A \cdot B = AB$. Pelo Teorema de Binet, o qual nos afirma que o determinante é um morfismo com relação a multiplicação, obtermos que a função f dada por $A \mapsto detA$ é invariante com respeito a essa ação.*

Definição 1.8.3 *Considerando a ação simétrica de S_n em $V = K^n$, obtemos que as funções $f \in K[x_1, \ldots, x_n]$, tais que $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$ que são invariantes com respeito a essa ação, são chamadas de* ***funções simétricas****.*

Exemplo 1.8.4 *Considerando a ação por conjugação em $G = GL_n(K)$, temos que a função traço é invariante, uma vez que o traço possui a propriedade cíclica, ou seja, $tr(AB) = tr(BA)$.*

1.9 Polarização e restituição

A importância do uso dos operadores de polarização e restituição para a teoria de invariantes é indiscutível. Com o objetivo de estudar as invariantes e concomitantes em álgebras de matrizes podemos reduzir (em característica zero) ao estudos do casos multilineares. Esse texto foi baseado em [27]. Nesta seção, ainda iremos considerar K um corpo cuja a característica é zero.

Definição 1.9.1 *Dada $f \in K[V]$ nas variáveis $(x_1, \ldots, x_n)$, dizemos que f é uma função simétrica se f é invariante sobre permutações dessas variáveis.*

Seja $f \in K[V]$ uma função homogênea de grau d. Sendo $v = \sum_{i=1}^{d} t_i v_i, t_i \in K$ e $v_i \in V$, obtemos

$$f(v) = f(\sum_{i=1}^{d} t_i v_i) = \sum_{s_1+\cdots+s_d=d} t_1^{s_1} \cdots t_d^{s_d} f_{s_1 \cdots s_d}(v_1, \ldots, v_d) \tag{1.2}$$

onde os polinômios $f_{s_1 \cdots s_d} \in K[V]$ estão bem definidos e são multihomogêneos de grau $(s_1, \ldots, s_d)$.

Os polinômios multilineares $f_{11 \cdots 1} \in K[V]$ são chamados de polarização (completa) de f e consideremos a aplicação $\mathcal{P}$ que associa a cada função homogênea de grau d a sua polarização. Daí, faz sentido denotarmos a polarização completa de f por $\mathcal{P}f$. Note que $\mathcal{P}f$ é multilinear. Ademais, $\mathcal{P}f$ é simétrica, uma vez que se $\sigma \in S_d$ é uma permutação, então $f(x_1 + \cdots + x_d) = f(x_{\sigma(1)} + \cdots + x_{\sigma(d)})$.

Proposição 1.9.2 *Nas condições acima estabelecidas, vale a seguinte igualdade:*

$$\mathcal{P}f(v,\ldots,v) = d!f(v)$$

Demonstração: Note que se substituirmos em (1.2) os v_i's por v, temos no lado esquerdo da igualdade:

$$\begin{aligned} f(t_1 v + \cdots + t_d v) &= f\left(\left(\sum t_i\right) v\right) \\ &= \left(\sum t_i\right)^d f(v) \\ &= (t_1^d + \ldots + d! t_1 t_2 \cdots t_d) f(v), \end{aligned}$$

onde a última igualdade segue do binômio de newton. Comparando com o lado direito de (1.2), temos na parcela obtida quando $s_1 = s_2 = \ldots = s_d = 1$ a seguinte igualdade:

$$t_1 \cdots t_d f_{1\cdots 1}(v,\ldots,v) = d! t_1 t_2 \cdots t_d f(v).$$

Assim, temos o desejado. ■

Para um polinômio $g(v_1,\ldots,v_d)$ em d variáveis vetoriais, o operador linear

$$\mathcal{R} : g(v_1,\ldots,v_d) \mapsto \frac{1}{d!} g(v,\ldots,v)$$

é chamado de restituição.

O próximo resultado irá relacionar os operadores polarização e restituição.

Teorema 1.9.3 *As aplicações $\mathcal{P}$ e $\mathcal{R}$ são isomorfismos inversos entre o espaço das formas homogêneas de grau d e o espaço das funções multilineares simétricas em d variáveis.*

Demonstração: Da forma como foi definido o operador $\mathcal{R}$, segue que $\mathcal{R}\mathcal{P}f = f$. Assim, basta mostrarmos que $\mathcal{P}\mathcal{R}g = g$. Para isso, seja $g(v_1,\ldots,v_d)$ uma função multilinear simétrica. Então,

$$\mathcal{P}\mathcal{R}g = \mathcal{P}\frac{1}{d!} g(v,\ldots,v).$$

Diante disso, basta analisarmos a parte multilinear de $\frac{1}{d!} g(v,\ldots,v)$. Ora, defina o vetor $v = \sum v_i$. Da multilinearidade de g tem-se

$$g(v,\ldots,v) = \sum g(v_{i_1}, v_{i_2}, \ldots, v_{i_d}),$$

onde o somatório é sobre todas as possíveis sequências de índices $i_1, i_2, \ldots, i_d \in \{1, \ldots, d\}$ (com possíveis repetições). Ora, mas a parte multilinear é exatamente a soma sobre todas as sequências sem repetições, isto é, as permutações. Assim,

$$\mathcal{PR}g = \frac{1}{d!} \sum_{\sigma \in S_d} g(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(d)}),$$

e como g é simétrico, $\mathcal{PR}g = g$. Assim, temos o desejado. ■

Nós podemos generalizar o processo de polarização, para uma função multihomogênea. Para isso, basta realizar o processo de polarização em cada uma das variáveis v_i, de modo isolado. A polarização completa será multilinear e simétrica em cada v_i correspondente a variável que foi substituída. E a função inicial é obtida da forma polarizada por uma sequência de restituições.

Neste contexto, considere $V = V_1 \oplus \cdots \oplus V_r$ um espaço de dimensão finita. Uma função $f \in K[V]$ é chamada **multihomogênea de grau** $h = (h_1, \ldots, h_r)$ se f é homogêneo de grau h_i em V_i, ou seja, para todo $v_1, \ldots, v_r \in V$, $t_1, \ldots, t_r \in K$ temos

$$f(t_1v_1, t_2v_2, \ldots, t_rv_r) = t_1^{h_1} t_2^{h_2} \cdots t_r^{h_r} f(v_1, v_2, \ldots, v_r). \tag{1.3}$$

Em particular se $h = (1, \ldots, 1)$ dizemos que f é uma multilinear.

É claro que toda função polinomial f é escrita de modo único como soma de funções multihomogêneos: $f = \sum f_h$, onde f_h são chamados **componentes multihomogêneos de** f.

Observação 1.9.4 *Para a notação não ficar tão "pesada", em alguns resultados poderemos nos concentrar nos polinômios de uma só variável para exemplificar a Eq.* (1.3), *e assumir que os resultados aqui apresentados valem para polinômios com um número maior de variáveis.*

Definição 1.9.5 *Seja S um subespaço de $K[V]$. Dizemos que S é um espaço* **estável** *se para cada $f \in S$ temos que suas componente multihomôgenea ainda está contida em S.*

Seja S um subespaço de $K[V]$. Denotemos por $S^{(m)}$ um subespaço de S como sendo o espaço gerado por todas as funções polinomiais multilineares em S. Munidos dessa notação, provaremos o teorema conhecido como **Método de Aronhold** (ver [31, Seção 2.4, pág. 44]).

Teorema 1.9.6 *Seja S, R subespaço estáveis de $K[V]$ tais que $S^{(m)} \subset R^{(m)}$, então $S \subset R$.*

Demonstração: Seja $f \in S$. Podemos supor que f é uma função multihomogênea. Devemos provar que $f \in R$. Nós sabemos que f pode ser obtido por restituição da forma polarizada completa $f = \mathcal{RP}f$. As hipóteses implicam que $\mathcal{P}f \in S^{(m)}$ e daí $\mathcal{P}f \in R^{(m)}$. Como R é um espaço fechado sobre polarização e restituição, temos $f = \mathcal{RP}f \in R$. ■

Como consequência direta temos o seguinte resultado.

Corolário 1.9.7 *Se dois espaços S, R de $K[V]$ são estáveis e $S^{(m)} = R^{(m)}$, então $S = R$.*

Este corolário será utilizado em nossos cálculos com invariantes, da seguinte maneira: Iremos calcular o espaço W dos invariantes em A sobre o grupo G das transformações lineares em um espaço n-dimensional. Nós iremos encontrar uma lista de invariantes formando um subespaço V fechado sobre polarização. Daí, nosso objetivo será de encontrar todos os invariantes e provar que $V = W$. Ora, mas para isso, sobre um corpo de característica zero, bastará mostrar para os multilineares, uma vez que se f é uma invariante, então todas as suas componentes multihomogenenas são também invariantes.

Observação 1.9.8 *De modo informal, podemos dizer que o processo de multilinearização está para identidades polinomiais, assim como o processo de polarização está para invariantes.*

Capítulo 2

Invariantes algébricos e identidades com Traço

Neste capítulo temos como objetivo inicial estudar a solução da conjectura proposta por Artin, em [4], dada por Procesi em seu trabalho intitulado “The Invariant theory of $n \times n$ matrices”, ver ([29]). Tal conjectura, diz que a natureza das invariantes de m matrizes de ordem n, digamos $X_1, \ldots, X_m$, são polinômios em elementos da forma $Tr(X_{i_1} X_{i_2} \cdots X_{i_R})$, isto é, que dependem do traço.

Além do que já foi mencionado, estabeleceremos uma relação entre os invariantes e as concomitantes de matrizes de ordem n sobre um corpo de característica zero. Tal relação entre invariantes e concomitantes é impressionante, pois afirma que toda relação entre estes é consequência do polinômio de Cayley-Hamilton. Munido deste resultado poderemos concluir que se uma álgebra sobre um corpo de característica zero satisfaz a identidade x^n, então ela satisfaz todas as identidades de matrizes de ordem n.

Para evitar repetições neste capítulo, K denotará um corpo de característica zero, $V \simeq K^n$ um espaço vetorial de dimensão n, $M_n(K) \simeq End(V)$ o anel das matrizes $n \times n$, V^* o espaço dual de V e $G = GL(V) \simeq GL_n(K)$ o grupo das matrizes inversíveis. Além disso, dados U e V espaços vetoriais, denotaremos por $\mathcal{L}(U, V)$ o conjunto de todas as transformações lineares de U em V.

Por fim, mencionamos que além do texto sob autoria de C. Procesi, o livro [23] foi de grande ajuda para o entendimento de todo este capítulo.

2.1 Invariantes das matrizes de ordem n

Nesta seção, temos como objetivo mostrar o teorema conhecido no estudo da teoria de invariantes por "Primeiro Teorema Fundamental" para a álgebra das matrizes. Tal teorema afirma que toda função polinomial invariante em matrizes, sobre a ação de G, é um polinômio que depende de uma certa aplicação traço (aqui pode ser muitas vezes confundida com o traço usual de matrizes).

No que segue, dada uma forma linear $\phi \in V^*$ e um vetor $v \in V$, denotaremos por $\langle \phi, v \rangle := \phi(v)$ o escalar $\phi(v)$.

Utilizando a propriedade universal, podemos realizar o produto tensorial entre operadores. Para isso, consideremos U_1, U_2, V_1 e V_2 espaços vetoriais e $f : U_1 \to V_1$ e $g : U_2 \to V_2$ duas aplicações lineares. A aplicação definida por

$$\begin{aligned} \psi : U_1 \times U_2 &\to V_1 \otimes V_2 \\ (u, v) &\mapsto f(u) \otimes g(v) \end{aligned}$$

é bilinear. Da propriedade universal de produto tensorial obtemos uma única aplicação linear denotada por $f \otimes g : U_1 \otimes U_2 \to V_1 \otimes V_2$ a qual é caracterizada pela propriedade

$$(f \otimes g)(u \otimes v) = f(u) \otimes g(v). \tag{2.1}$$

Observação 2.1.1 *Em vista do que será estudado, é útil escrever o emparelhamento dual no nível de vetores decomponíveis $\langle \varphi \otimes \psi, u \otimes v \rangle = \langle \varphi, u \rangle \langle \psi, v \rangle$. Tal possibilidade surge de* (2.1) *e considerando V_1 e V_2 espaços isomorfos ao corpo.*

Agora, identifiquemos a álgebra $M_n(K)^{\otimes i}$ com $End(V^{\otimes i})$, e disto obteremos propriedades para a álgebra de matrizes a partir das que conhecemos da álgebra dos endomorfismos.

Lema 2.1.2 *Os espaços $M_n(K)^{\otimes i}$ e $End(V^{\otimes i})$ são isomorfos como álgebras.*

Demonstração: Inicialmente, consideremos a aplicação

$$\begin{aligned} \varphi : \quad M_n(K)^i &\to End(V^{\otimes i}) \\ (A_1, \ldots, A_i) &\mapsto \varphi(A_1, \ldots, A_i) \end{aligned}$$

onde $\varphi(A_1, \ldots, A_i)(v_1 \otimes \cdots \otimes v_i) = A_1 v_1 \otimes \cdots \otimes A_i v_i$.

Note que φ está bem definida e, das propriedades do produto tensorial, é linear em cada entrada. Logo, pela propriedade universal do produto tensorial, existe uma única transformação linear $T_\varphi : M_n(K)^{\otimes i} \to End(V^{\otimes i})$ dada por

$$(A_1 \otimes \cdots \otimes A_i) \mapsto T_\varphi(A_1 \otimes \cdots \otimes A_i) = \varphi(A_1, \ldots, A_i).$$

Para finalizar basta que verifiquemos que T_φ é um isomorfismo de álgebras. Com efeito, dados $A = A_1 \otimes \cdots \otimes A_i$, $B = B_1 \otimes \cdots \otimes B_i \in M_n(K)^{\otimes i}$ e $v = v_1 \otimes \cdots \otimes v_i \in V^{\otimes i}$ arbitrários, temos:

$$\begin{aligned}
T_\varphi(A \cdot B)(v) &= T_\varphi((A_1 \otimes \cdots \otimes A_i) \cdot (B_1 \otimes \cdots \otimes B_i))(v_1 \otimes \cdots \otimes v_i) \\
&= T_\varphi(A_1B_1 \otimes \cdots \otimes A_iB_i)(v_1 \otimes \cdots \otimes v_i) \\
&= \varphi(A_1B_1, \ldots, A_iB_i)(v_1 \otimes \cdots \otimes v_i) \\
&= A_1B_1v_1 \otimes \cdots \otimes A_iB_iv_i \\
&= \varphi(A_1, \ldots, A_i)(B_1v_1 \otimes \cdots \otimes B_iv_i) \\
&= (\varphi(A_1, \ldots, A_i) \circ \varphi(B_1, \ldots, B_i))(v_1 \otimes \cdots \otimes v_i)
\end{aligned}$$

ou seja,

$$T_\varphi(A \cdot B)(v) = T_\varphi(A) \circ T_\varphi(B)(v).$$

Da arbitrariedade dos elementos tomados, T_φ é um homomorfismo de álgebras.

Por fim, observamos que T_φ é uma bijeção. Da definição de T_φ, junto com a aplicação dada em (2.1), podemos ver T_φ como sendo a transformação linear dada por

$$T_\varphi(A_1 \otimes \cdots \otimes A_i) = A_1 \otimes \cdots \otimes A_i. \tag{2.2}$$

Observe que $M_n(K)^{\otimes i}$ tem base formada por tensores cuja as entradas são elementos da base canônica de $M_n(K)$, ou seja, $M_n(K)^{\otimes i}$ tem base formada por elementos da forma

$$E = E_{r_1s_1} \otimes E_{r_2s_2} \otimes \cdots \otimes E_{r_is_i}, \tag{2.3}$$

onde cada $E_{r_js_j}$ são matrizes elementares. A interpretação da Aplicação (2.2) pode ser feita de modo natural, a imagem da matriz E é um homomorfismo de modo que cada entrada do tensor $T_\varphi(E)$ é dado por $E_{rs}(v_l) = \delta_{sl}v_r$, onde δ_{sl} é o chamado delta de Kronecker. Agora, tome um elemento de $M_n(K)^{\otimes i} \cap ker T_\varphi$, digamos A. Pelo comentário anterior, podemos escrever o elemento A como combinação linear de elementos da forma (2.3), digamos

$$A = \sum_{j=1}^{l} \alpha_j E_{r_1^j s_1^j} \otimes E_{r_2^j s_2^j} \otimes \cdots \otimes E_{r_i^j s_i^j},$$

de modo que o conjunto $\{E_{r_1^j s_1^j} \otimes E_{r_2^j s_2^j} \otimes \cdots \otimes E_{r_i^j s_i^j} \mid j = 1, \ldots, l\}$ seja linearmente independente. Por T_φ ser linear temos que

$$T_\varphi(A) = \sum_{j=1}^{l} \alpha_j E_{r_1^j s_1^j} \otimes E_{r_2^j s_2^j} \otimes \cdots \otimes E_{r_i^j s_i^j}$$

é o endomorfismo, sobre $V^{\otimes i}$, nulo. Fixemos um elemento da base $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V e tome o tensor básico $v = v_{l_1} \otimes \cdots \otimes v_{l_i}$ de $V^{\otimes i}$. Considerando a Igualdade (2.3), temos

$$E_j(v) = E_{r_1 s_1}(v_{l_1}) \otimes E_{r_2^j s_2^j}(v_{l_2}) \otimes \cdots \otimes E_{r_i^j s_i^j}(v_{l_i}) = \delta_{s_1^j l_1} \cdots \delta_{s_i^j l_i}(v_{r_1^j} \otimes \cdots \otimes v_{r_i^j})$$

Assim, $E_j(v) \neq 0$ se, e somente se, $s_u^j = l_u$, para cada $u = 1, \ldots, i$. Além disso, se $E_j(v)$ e $E_u(v)$ são não nulos para algum v fixado em $V^{\otimes i}$, então $E_j(v) = E_u(v)$ se, e somente se, $E_j = E_u$. Em resumo, é possível determinar alguns v's em $V^{\otimes i}$ de modo que

$$\sum_{j=1}^{l} \alpha_j (E_{r_1^j s_1^j} \otimes E_{r_2^j s_2^j} \otimes \cdots \otimes E_{r_i^j s_i^j})(v) = 0 \Rightarrow \alpha_j = 0,$$

para cada $j = 1, \ldots, l$. Concluindo que $A = 0$, ou seja, T_φ é injetiva. Ademais, como $M_n(K)^{\otimes i}$ e $End(V^{\otimes i})$ tem a mesma dimensão, segue do Teorema do Núcleo e da Imagem que T_φ é um isomorfismo de álgebras. ■

Considerando agora a ação diagonal de G em $V^{\otimes i}$, a qual, como visto no Exemplo 1.6.4, é dada por

$$A \cdot (v_1 \otimes v_2 \otimes \cdots \otimes v_i) = A \cdot v_1 \otimes A \cdot v_2 \otimes \cdots \otimes A \cdot v_i,$$

vamos construir um G-isomorfismo entre os espaços $V^{*\otimes i} \otimes V^{\otimes i}$ e $End(V^{\otimes i})$.

Proposição 2.1.3 *Os espaços $V^{*\otimes i} \otimes V^{\otimes i}$ e $End(V^{\otimes i})$ são G-isomorfos.*

Demonstração: Por simplicidade de notação, consideremos inicialmente U e V dois espaços de dimensão finita e a aplicação definida por

$$\begin{aligned} T_0 : U \times V &\rightarrow \mathcal{L}(U^*, V) \\ (u, v) &\mapsto T_0(u, v). \end{aligned}$$

onde $T_0(u,v)(u_0^*) = \langle u_0^*, u\rangle v$ (aqui deixamos claro que $\mathcal{L}(U^*,V)$ denota o conjunto de todas as transformações lineares de U^* em V). Desse modo, para todo $u_1, u_2 \in U$, $v \in V$ e $\lambda \in K$, temos:

$$\begin{aligned} T_0(\lambda u_1 + u_2, v)(u_0^*) &= \langle u_0^*, \lambda u_1 + u_2\rangle v \\ &= u_0^*(\lambda u_1 + u_2)v \\ &= \lambda u_0^*(u_1)v + u_0^*(u_2)v \\ &= \lambda T_0(\lambda u_1, v)(u_0^*) + T_0(u_2, v)(u_0^*). \end{aligned}$$

Assim, a aplicação T_0 é linear na primeira entrada. Utilizando as propriedades de produto escalar num espaço vetorial, facilmente vemos que T_0 é linear na segunda entrada. Daí, a aplicação T_0 é bilinear, e, portanto, existe uma única aplicação linear T, tal que

$$\begin{aligned} T : U \otimes V &\rightarrow \mathcal{L}(U^*, V) \\ u \otimes v &\mapsto T(u \otimes v) = T_0(u, v). \end{aligned}$$

Deste modo, para mostrarmos que $U \otimes V$ e $\mathcal{L}(U^*,V)$ são isomorfos como espaços vetoriais, basta verificarmos que T é uma bijeção. Com efeito, considere $\{u_1, \ldots, u_n\}$ e $\{v_1, \ldots, v_m\}$ bases dos espaços U e V, respectivamente. Seja $k \in kerT$, assim podemos escrever ele da forma

$$k = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij}(u_i \otimes v_j) = \sum_{i,j} \alpha_{ij}(u_i \otimes v_j).$$

Considere, agora, $\{f_1, \ldots, f_n\}$ a base dual do espaço U^*, neste caso,

$$0 = T(k)(f_r) = \sum_{i,j} \alpha_{ij} T(u_i \otimes v_j)(f_r) = \sum_{j=1}^{m} \alpha_{rj}\langle f_r, u_r\rangle v_j = \sum_{j=1}^{m} \alpha_{rj} v_j,$$

para cada $r = 1, \ldots, n$. Deste comentário temos que $k = 0$, ou seja, T é injetiva. Por fim, a bijeção de T segue do fato que

$$dim(U \otimes V) = dimU.dimV = dimU^*.dimV = dim(\mathcal{L}(U^*, V)).$$

Podemos então considerar o caso em que U e V são $V^{*\otimes i}$ e $V^{\otimes i}$, respectivamente. Nestas condições $\mathcal{L}(U^*,V) = End(V^{\otimes i})$. Assim resta mostrar que T é um G-isomorfismo. Ora, dados $g \in G$, a ação diagonal de G em V, dada por

$$\langle g, \varphi \otimes x\rangle = \langle \varphi, g \cdot x\rangle, \tag{2.4}$$

onde $\varphi = \varphi_1 \otimes \varphi_2 \otimes \cdots \otimes \varphi_i, x = x_1 \otimes x_2 \otimes \cdots \otimes x_i$ e considerando a ação de G sobre $V^{\otimes i}$ dada por $g \cdot x = g \cdot x_1 \otimes g \cdot x_2 \otimes \cdots \otimes g \cdot x_i$, com $\varphi_j \in V^*$ e $x_j \in V$, $j = 1, \ldots, i$, teremos

$$\begin{aligned} T(\langle g, \varphi \otimes x \rangle)(y) &= T(\varphi \otimes g \cdot x)(y) \\ &= \langle y, \varphi \rangle g \cdot x \\ &= g \cdot (\langle y, \varphi \rangle x) \\ &= g \cdot T(\varphi \otimes x)(y), \text{ para todo } y \in V^{*\otimes i}. \end{aligned}$$

Assim, temos o desejado. ■

Assim, usando o fato de que um espaço vetorial de dimensão finita é isomorfo ao seu dual, concluímos que o espaço vetorial G-invariante $(V^{*\otimes i} \otimes V^{\otimes i})^*$, que é o espaço das aplicações lineares

$$V^{*\otimes i} \otimes V^{\otimes i} \to K \tag{2.5}$$

invariantes sobre G, é identificado pela aplicação T como sendo o espaço dos endomorfismos G-lineares de $V^{\otimes i}$.

Antes de darmos continuidade a resolução de nosso problema, faremos uma pausa para fazer uma observação importante. Tal observação, a princípio, pode parecer que não tem relação com nosso contexto, mas veremos que isto não é verdade.

Observação 2.1.4 *A topologia de Zariski é uma topologia adequada para o estudo de variedades algébricas, os principais objetos de estudo em geometria algébrica. Como em qualquer espaço topológico, é importante saber como é a descrição de seus conjuntos fechados, pois sabemos que o complementar desses conjuntos serão os nossos abertos. Para isto, temos: Um conjunto $X \subset K^n$ é dito ser fechado na topologia de Zariski se ele é da forma*

$$V(S) = \{(x_1, \ldots, x_n) \in K^n \mid f(x_1, \ldots, x_n) = 0, \forall f \in S\}$$

para algum $S \subseteq K[t_1, \ldots, t_n]$.

É fato conhecido que $G = \{A \in M_n(K) \mid detA \neq 0\}$. Por outro lado, a aplicação determinante $det\colon M_n(K) \to K$ é polinomial com entradas em $t_1, \ldots, t_{n^2}$. Neste caso $V(\{det\})$ é um fechado em $M_n(K) \simeq K^{n^2}$ na topologia de Zariski, implicando que $G = V(\{det\})^c$ é um aberto nessa topologia.

Observe que além da ação diagonal de G sobre o espaço $V^{\otimes i}$ temos uma ação do grupo simétrico S_i sobre o mesmo espaço V dado por

$$\sigma \cdot (v_1 \otimes \cdots \otimes v_i) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(i)}.$$

Essas duas ações comutam entre si e nos dá imersões de G e S_i em $End(V^{\otimes i})$. Denotando por $\langle G\rangle$ o subespaço de $End(V^{\otimes i})$ gerado pela imagem de G e por $\langle S_i\rangle$ o subespaço gerado pela imagem de S_i, temos o seguinte resultado:

Teorema 2.1.5 *(i)* $\langle G\rangle = End_{S_i}(V^{\otimes i})$;

(ii) $\langle S_i\rangle = End_G(V^{\otimes i})$.

Demonstração: Se identificarmos $End(V^{\otimes i})$ com $End(V)^{\otimes i}$, um elemento $g \in G$ é aplicado para o tensor simétrico $g \otimes \cdots \otimes g$. Por outro lado, a imagem de $End_{S_i}(V^{\otimes i})$ são todos os elementos de $End(V)^{\otimes i}$ que são invariantes pela ação de conjugação (em cada entrada do tensor) do grupo simétrico. Aqui a ação no tensor é sempre a ação diagonal como dado no Exemplo 1.6.4. Em outras palavras, a imagem de $End_{S_i}(V^{\otimes i})$ em $End(V)^{\otimes i}$ é o subespaço de todos os tensores simétricos em $End(V)^{\otimes i}$. Desta forma, seja $\mathcal{B}_0 = \{e_1, \ldots, e_{n^2}\}$ uma base de $End(V)$, então o conjunto

$$\mathcal{B} = \{e_{m_1} \otimes \cdots \otimes e_{m_i} \mid e_{m_j} \in \mathcal{B}_0, 1 \leq j \leq i\}$$

forma uma base para $End(V)^{\otimes i}$ que é estável sobre a S_i-ação, isto é, $\sigma \cdot \mathcal{B} \subset \mathcal{B}$, para todo $\sigma \in S_i$. Assim, qualquer S_i-órbita contém um único representante da forma

$$e_1^{\otimes h_1} \otimes \cdots \otimes e_{n^2}^{\otimes h_{n^2}}$$

com $h_1 + \cdots + h_{n^2} = i$. Se denotarmos por $r(h_1, \ldots, h_{n^2})$ a soma de todos os elementos na correspondente S_i-órbita, então esses vetores forma uma base dos tensores simétricos em $End(V)^{\otimes i}$.

A afirmação segue, então, se pudermos mostrar que toda aplicação linear λ sobre os tensores simétricos, que é nulo sobre todo $g \otimes \cdots \otimes g$ com $g \in G$, é a aplicação nula. Ora, se escrevermos $e = \sum x_j e_j$ (um vetor genérico), então

$$\lambda(e \otimes \cdots \otimes e) = \sum x_1^{h_1} \cdots x_{n^2}^{h_{n^2}} \lambda(r(h_1, \ldots, h_{n^2})) \tag{2.6}$$

é uma função polinomial sobre $End(V)$ nula. Pela Observação 2.1.4, G é um subconjunto aberto de Zariski de $End(V)$. Assim o único polinômio que se anula sobre ele é o nulo. Portanto, $\lambda(r(h_1, \ldots, h_{n^2})) = 0$, para todo $(h_1, \ldots, h_{n^2})$, terminando a demonstração do item (i).

Já para o segundo item, observe, inicialmente, que a álgebra de grupo KS_i é semissimples, ver Teorema de Maschke. Assim, qualquer imagem por uma aplicação sobrejetiva de álgebra semissimples é semissimples. Portanto, $\langle S_i \rangle$ é também uma subálgebra semissimples de $End(V^{\otimes i})$. Além disso, usando a definição de centralizador, é fácil observar que

$$End_G(V^{\otimes i}) = \{X \in End(V^{\otimes i}) \mid X \circ g = g \circ X, \forall g \in G\} = C_{End(V^{\otimes i})}(\langle G \rangle).$$

Já pela primeira parte desta demonstração,

$$\langle G \rangle = End_{S_i}(V^{\otimes i}) = \{a \in End(V^{\otimes i}) \mid a\sigma = \sigma a \text{ para todo } \sigma \in S_i\} = C_{End(V^{\otimes i})}(\langle S_i \rangle).$$

Destes comentários, podemos aplicar o Teorema 1.1.34 e teremos

$$C_{End(V^{\otimes i})}(End_{S_i}(V^{\otimes i})) = C_{End(V^{\otimes i})}(C_{End(V^{\otimes i})}(\langle S_i \rangle)) = \langle S_i \rangle.$$

Em resumo, temos $End_G(V^{\otimes i}) = \langle S_i \rangle$. Como queríamos demonstrar. ■

Pelo item (ii) do teorema anterior, concluímos que a álgebra das transformações G-lineares de $V^{\otimes i}$ é gerada, como espaço vetorial, pelos endomorfismos λ_σ, onde $\sigma \in S_i$, definido por

$$\lambda_\sigma(v_1 \otimes v_2 \otimes \cdots \otimes v_i) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(i)}. \tag{2.7}$$

Inferimos que para encontrar uma expressão explícita para os invariantes da forma (2.5), basta encontrarmos para λ_σ. Ora, pela Observação 2.1.1, temos

$$\begin{aligned} \langle \lambda_\sigma, \varphi_1 \otimes \cdots \otimes \varphi_i \otimes X_1 \otimes \cdots \otimes X_i \rangle &= \langle \varphi_1 \otimes \cdots \otimes \varphi_i, X_{\sigma^{-1}(1)} \otimes \cdots \otimes X_{\sigma^{-1}(i)} \rangle \\ &= \prod_j \langle \varphi_j, X_{\sigma^{-1}(j)} \rangle \\ &= \prod_j \langle \varphi_{\sigma(j)}, X_j \rangle. \end{aligned}$$

Aqui estamos considerando a ação dada em (2.4). Em resumo, temos uma parte do Primeiro Teorema Fundamental:

Teorema 2.1.6 *Qualquer invariante multilinear $\gamma : V^{*\otimes i} \otimes V^{\otimes i} \to K$ é uma combinação linear dos invariantes*

$$\mu_\sigma(\varphi_1 \otimes \cdots \otimes \varphi_i \otimes X_1 \otimes \cdots \otimes X_i) := \prod_j \langle \varphi_{\sigma(j)}, X_j \rangle.$$

Vamos interpretar os λ_σ's de forma diferente. Recordaremos o isomorfismo canônico entre $End(V)$ e $V^* \otimes V$, argumentado anteriormente, dado pela fórmula:

$$(\varphi \otimes v)(u) = \langle \varphi, u \rangle v.$$

Isto é um G-isomorfismo e usaremos isto para identificar sistematicamente os dois espaços.

As seguintes expressões serão chamadas de multiplicação dos endomorfismos e a aplicação traço, respectivamente:

$$\varphi \otimes v \cdot \psi \otimes u = \varphi \otimes \langle \psi, v \rangle u \tag{2.8}$$

$$tr(\varphi \otimes v) = \langle \varphi, v \rangle. \tag{2.9}$$

Observe que o produto dado em (2.8) é obtido da seguinte maneira: Dado $\varphi \in V^*$ e $v \in V$, podemos considerar a aplicação

$$f_{\varphi,v} : V^* \times V \to V^* \otimes V,$$

dada por $f_{\varphi,v}(\psi, u) = \varphi \otimes \langle \psi, v \rangle u$. Observe que $f_{\varphi,v}$ é bilinear. Pela propriedade universal do produto tensorial, deve existir uma transformação linear

$$T_{\varphi,v} : V^* \otimes V \to V^* \otimes V,$$

tal que $T_{\varphi,v}(\psi \otimes u) = f_{\varphi,v}(\psi, u)$. Observando agora que a aplicação

$$\begin{aligned} T : V^* \times V &\to End(V) \\ (\varphi, v) &\to T_{\varphi,v} \end{aligned}$$

é bilinear, concluímos que existe uma única transformação linear F de $V^* \otimes V$ em $End(V)$ tal que $F(\varphi \otimes v) = T_{\varphi,v}$. Logo o produto

$$\begin{aligned} \cdot : (V^* \otimes V) \times (V^* \otimes V) &\to (V^* \otimes V) \\ (\varphi \otimes v, \psi \otimes u) &\to \varphi \otimes v \cdot \psi \otimes u = F(\varphi \otimes v)(\psi \otimes u) \end{aligned}$$

é bilinear e satisfaz

$$\varphi \otimes v \cdot \psi \otimes u = F(\varphi \otimes v)(\psi \otimes u) = T_{\varphi,v}(\psi \otimes u) = \varphi \otimes \langle \psi, v \rangle u,$$

para quaisquer $u, v \in V$ e $\varphi, \psi \in V^*$.

Além disso, por contas diretas, usando a multiplicação definida acima e lembrando que $\langle \varphi, v\rangle = \varphi(v) \in K$, para todo $\varphi \in V^*$ e $v \in V$, temos que a expressão obtida em (2.9) satisfaz as condições da definição de traço.

Observação 2.1.7 *Seja $\beta^* = \{\varphi_1, \ldots, \varphi_n\}$ a base dual do espaço V^* relativa a base $\beta = \{v_1, \ldots, v_n\}$. Podemos definir a aplicação $\Psi\colon V^* \otimes V \to M_n(K)$ induzida por $\Psi(\varphi_i \otimes v_j) = E_{ij}$. Note que,*

$$\Psi(\varphi_i \otimes v_j \cdot \varphi_r \otimes v_s) = \Psi(\varphi_i \otimes \langle \varphi_r, v_j\rangle \otimes v_s) = \delta_{rj} E_{is}$$

e $\Psi(\varphi_i \otimes v_j) \cdot \Psi(\varphi_r \otimes v_s) = E_{ij} \cdot E_{rs} = \delta_{rj} E_{is}$. Pela Proposição 1.1.22, Ψ é um homomorfismo de álgebras, e não é difícil observar que tal homomorfismo é na verdade um isomorfismo de álgebras. Concluímos que o produto dado em (2.8) torna $V^* \otimes V$ e $M_n(K)$ álgebras isomorfas.

Nós podemos usar os isomorfismos anteriores para obter um outro isomorfismo entre G-espaços, da seguinte forma:

$$(V^* \otimes V)^{\otimes i} \simeq (End V)^{\otimes i} \simeq M_n(K)^{\otimes i} \simeq End(V^{\otimes i}) \simeq V^{*\otimes i} \otimes V^{\otimes i}. \tag{2.10}$$

Daí, a descrição de um invariante linear de $V^{*\otimes i} \otimes V^{\otimes i}$ obtido no teorema anterior é, portanto, uma descrição para os invariantes multilineares de $M_n(K)^{\otimes i}$. Então, escolhendo um $\sigma \in S_n$ e considerando um invariante linear $\mu_\sigma : M_n(K)^{\otimes i} \to K$, obteremos um nova fórmula explícita para μ_σ em termo de matrizes genéricas.

Teorema 2.1.8 *Seja $\sigma \in S_i$ e suponhamos que*

$$\sigma = (i_1 i_2 \cdots i_k)(j_1 j_2 \cdots j_n) \cdots (t_1 t_2 \cdots t_l)$$

é a decomposição de σ em ciclos disjuntos. Então, dadas $A_1, A_2, \ldots, A_i \in M_n(K)$, temos:

$$\mu_\sigma(A_1 \otimes A_2 \otimes \cdots \otimes A_i) = tr(A_{i_1} A_{i_2} \cdots A_{i_k}) tr(A_{j_1} A_{j_2} \cdots A_{j_n}) \cdots tr(A_{t_1} A_{t_2} \cdots A_{t_l}).$$

Demonstração: Como os dois lados da igualdade são aplicações multilineares, é suficiente provar quando $A_1, \ldots, A_i$ são decomponíveis, isto é, $A_j = \varphi_j \otimes x_j$ (uma vez que esses vetores geram o espaço), onde $\varphi_j \in V^*$ e $x_j \in V$. Daí, pelo isomorfismo obtido em (2.10) podemos supor, sem perda de generalidade, que

$$\mu_\sigma(A_1 \otimes \cdots \otimes A_i) = \mu_\sigma(\varphi_1 \otimes \varphi_2 \cdots \otimes \varphi_i \otimes x_1 \otimes \cdots \otimes x_i).$$

Nesta caso,

$$\begin{aligned}
\mu_\sigma(A_1 \otimes \cdots \otimes A_i) &= \mu_\sigma(\varphi_1 \otimes \varphi_2 \cdots \otimes \varphi_i \otimes x_1 \otimes \cdots \otimes x_i) \\
&= \prod_{j=1}^{i} \langle \varphi_{\sigma(i)}, x_i \rangle \\
&= \langle \varphi_{i_2}, x_{i_1} \rangle \langle \varphi_{i_3}, x_{i_2} \rangle \cdots \langle \varphi_{i_k}, x_{i_{k-1}} \rangle \langle \varphi_{i_1}, x_{i_k} \rangle \\
&\quad \langle \varphi_{j_2}, x_{j_1} \rangle \cdots \langle \varphi_{j_1}, x_{j_n} \rangle \cdots \langle \varphi_{t_1}, x_{t_l} \rangle.
\end{aligned}$$

Consideremos, por exemplo, o produto

$$M = \langle \varphi_{i_2}, x_{i_1} \rangle \langle \varphi_{i_3}, x_{i_2} \rangle \cdots \langle \varphi_{i_k}, x_{i_{k-1}} \rangle \langle \varphi_{i_1}, x_{i_k} \rangle.$$

Usando a multiplicação de endomorfismo dado em (2.8), segue que:

$$\begin{aligned}
\varphi_{i_1} \otimes x_{i_1} \cdot \varphi_{i_2} \otimes x_{i_2} \cdot \ldots \cdot \varphi_{i_k} \otimes x_{i_k} &= \varphi_{i_1} \otimes \langle \varphi_{i_2}, x_{i_1} \rangle x_{i_2} \cdot \ldots \cdot \varphi_{i_k} \otimes x_{i_k} \\
&= \langle \varphi_{i_2}, x_{i_1} \rangle \varphi_{i_1} \otimes x_{i_2} \cdot \ldots \cdot \varphi_{i_k} \otimes x_{i_k} \\
&= \langle \varphi_{i_2}, x_{i_1} \rangle \langle \varphi_{i_3}, x_{i_2} \rangle \cdots \langle \varphi_{i_k}, x_{i_{k-1}} \rangle \varphi_{i_1} \otimes x_{i_k}.
\end{aligned}$$

Logo, aplicando o traço obtido em (2.9), obtemos:

$$\begin{aligned}
tr(A_{i_1} A_{i_2} \cdots A_{i_k}) &= tr(\varphi_{i_1} \otimes x_{i_1} \cdot \varphi_{i_2} \otimes x_{i_2} \cdot \ldots \cdot \varphi_{i_k} \otimes x_{i_k}) \\
&= tr(\langle \varphi_{i_2}, x_{i_1} \rangle \langle \varphi_{i_3}, x_{i_2} \rangle \cdots \langle \varphi_{i_k}, x_{i_{k-1}} \rangle \varphi_{i_1} \otimes x_{i_k}) \\
&= \langle \varphi_{i_2}, x_{i_1} \rangle \langle \varphi_{i_3}, x_{i_2} \rangle \cdots \langle \varphi_{i_k}, x_{i_{k-1}} \rangle tr(\varphi_{i_1} \otimes x_{i_k}) \\
&= \langle \varphi_{i_2}, x_{i_1} \rangle \langle \varphi_{i_3}, x_{i_2} \rangle \cdots \langle \varphi_{i_k}, x_{i_{k-1}} \rangle \langle \varphi_{i_1}, x_{i_k} \rangle,
\end{aligned}$$

ou seja,

$$M = tr(A_{i_1} A_{i_2} \cdots A_{i_k}).$$

Assim, fazendo o mesmo processo para os demais produtos, obtemos o desejado. ■

Como já encontramos uma descrição para as invariantes multilineares, o Corolário 1.9.7 estabelece o seguinte teorema:

Teorema 2.1.9 ***(Primeiro Teorema Fundamental)*** *Cada polinômio invariante em matrizes $A_1, \ldots, A_i \in M_n(K)$ é um polinômio em invariantes $tr(A_{i_1} A_{i_2} \cdots A_{i_j})$, onde $x_{i_1} \cdots x_{i_j}$ percorre todos os monômios em variáveis não comutativos.*

2.2 Matrizes concomitantes

Nesta seção queremos trabalhar com um tipo especial de aplicações polinomiais chamadas de **matrizes concomitantes**. Tal nome se dá pois elas estão associadas ao anel de matrizes. Para isso, devemos considerar a seguinte definição:

Definição 2.2.1 *Dados conjuntos X e Y munidos de uma ação de G, dizemos que uma aplicação f é G-**concomitante**, ou um morfismo, se é uma aplicação $f : X \to Y$, tal que $f(g \cdot x) = g \cdot f(x)$.*

Nesta seção, nosso objetivo é descrever as aplicações concomitantes $f\colon V \to W$ no seguinte caso: $V = M_n(K)^i$, $W = M_n(K)$ e $G = GL_n(K)$ com as ações usais sendo em V a ação diagonal e em cada coordenada a ação por conjugação. Denotaremos tal conjunto por $S_{i,n}$.

Inicialmente notemos que $S_{i,n}$ é um anel não comutativo sobre a soma e o produto pontuais. Além disso, $S_{i,n}$ é o subanel do anel das aplicações polinomiais de $M_n(K)^i$ para $M_n(K)$, denotado por $P_{i,n}$, formado pelos elementos fixados à esquerda pelo grupo G, onde G age em $P_{i,n}$ da seguinte maneira:

$$\begin{array}{rcl} \cdot : G \times P_{i,n} & \to & P_{i,n} \\ (g, \varphi) & \mapsto & g \cdot \varphi \end{array}$$

onde $(g \cdot \varphi)(u) = g(\varphi(g^{-1} \cdot u))$ e a segunda ação é a ação diagonal. Com efeito, primeiramente, considere que φ seja fixado à esquerda pelo grupo G, temos

$$\varphi(g \cdot v) = g\varphi(g \cdot v) = g(\varphi(g^{-1} \cdot g \cdot v)) = g(\varphi((g^{-1}g) \cdot v)) = g\varphi(v).$$

Logo, φ é uma concomitante. Reciprocamente, supondo φ uma concomitante,

$$\begin{array}{rcl} \varphi(g^{-1} \cdot v) = g^{-1}\varphi(v) & \Rightarrow & g(\varphi(g^{-1} \cdot v)) = g(g^{-1}\varphi(v)) \\ & \Rightarrow & (g \cdot \varphi)(v) = (gg^{-1})\varphi(v) \\ & \Rightarrow & (g \cdot \varphi)(v) = \varphi(v), \end{array}$$

ou seja, φ é fixado à esquerda pelo grupo G.

Notemos ainda que $P_{i,n}$ é isomorfo, como anel, ao anel das matrizes de ordem n sobre o anel das funções polinomiais em $M_n(K)^i$, isto é, um anel de polinômios em

$i \cdot n^2$ variáveis. Se identificarmos os escalares K como o centro de $M_n(K)$, vemos que o anel dos invariantes de $M_n(K)^i \to K$, denotado por $T_{i,n}$, é um subanel do centro de $S_{i,n}$. E, portanto, $S_{i,n}$ é uma $T_{i,n}$-álgebra.

Além disso, note que, entre as matrizes concomitantes, podemos considerar as chamadas j-projeções concomitantes, indicadas por X_j e dadas por:

$$X_j \colon (A_1, A_2, \ldots, A_i) \to A_j.$$

Formulemos agora o Primeiro Teorema Fundamental das Matrizes Concomitantes.

Teorema 2.2.2 *O anel $S_{i,n}$ é gerado, como uma álgebra sobre $T_{i,n}$, pelos elementos X_j. Em particular, $S_{i,n}$ é finitamente gerado.*

Demonstração: Dada uma concomitante $f : M_n(K)^i \to M_n(K)$ construamos um invariante sobre a ação diagonal

$$\begin{array}{rcl} \bar{f}: & M_n(K)^{i+1} & \to K \\ & (A_1, \ldots, A_{i+1}) & \mapsto tr(f(A_1, \ldots, A_i) \cdot A_{i+1}). \end{array}$$

Note ainda que $\bar{f}$ é linear em X_{i+1}.

Afirmação 1: A aplicação traço é não degenerada, isto é, dada $A \in M_n(K)$, se $tr(AB) = 0$, para toda $B \in M_n(K)$, então $A = 0$.

De fato, seja $A = \sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} E_{\alpha\beta}$. Da propriedade cíclica da aplicação traço temos que

$$0 = tr(AE_{rj}) = tr(AE_{ri}E_{ij}) = tr(E_{ij}AE_{ri}) = a_{jr},$$

para quaisquer i, j, r em $\{1, 2, \ldots, n\}$. E assim temos o desejado.

Afirmação 2: Dadas $f, g : M_n(K)^i \to M_n(K)$ duas concomitantes, se $\bar{f} = \bar{g}$, então $f = g$.

De fato, dadas quaisquer $A_1, \ldots, A_{i+1} \in M_n(K)$. Tal afirmação segue aplicando a Afirmação 1 junto da arbitrariedade do elemento A_{i+1}.

De mão dessas duas afirmações, o Teorema 2.1.9 para os invariantes, implica que se f é uma concomitante, então $\bar{f}$ é um polinômio nos elementos $tr(A_{i_1}A_{i_2}\cdots A_{i_j})$, sendo linear em A_{i+1}. Daí,

$$\bar{f} = \sum \lambda_{i_1 i_2 \cdots i_j} tr(A_{i_1}A_{i_2}\cdots A_{i_j}A_{i+1})$$

com $\lambda_{i_1 i_2 \cdots i_j} \in T_{i,n}$ e $i_1, i_2, \ldots, i_j \neq i+1$. (Se A_{i+1} aparecem no meio do monômio, podemos mudar ele para o fim por uma permutação cíclica). Temos, então

$$\bar{f}(A_1, \ldots, A_i, A_{i+1}) = tr\left(\left(\sum \lambda_{i_1 i_2 \cdots i_j} A_{i_1} A_{i_2} \cdots A_{i_j}\right) \cdot A_{i+1}\right).$$

Portanto, pela Afirmação 2, $f = \sum \lambda_{i_1 i_2 \cdots i_j} X_{i_1} X_{i_2} \cdots X_{i_j}$. ∎

2.3 Teorema da finitude para álgebras graduadas

Iniciemos essa seção definindo álgebras graduadas. Para um maior aprofundamento, indicamos a referência [18], mais especificamente o seu Capítulo 3, Seções 1-3.

Definição 2.3.1 *Sejam A um álgebra e G um grupo. Definimos uma G-graduação em A como sendo uma família $\{A_g \mid g \in G\}$ de subespaços vetoriais de A, tais que*

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

para quaisquer $g, h \in G$. Dizemos que uma álgebra é G-graduada caso ela tenha uma G-graduação.

Neste caso, o subespaço A_g é chamado de componente homogênea de grau g e os seus elementos não nulos de *elementos homogêneos de grau g*. Um subespaço V de A é graduado se

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

Uma subálgebra (respectivamente, um ideal) é chamado de graduado se ele como subespaço é graduado.

Exemplo 2.3.2 *Toda álgebra A admite uma G-graduação, basta considerar $A_\epsilon = A$ e $A_g = \{0\}$, para todo $g \in G \setminus \{\epsilon\}$. Aqui ϵ denota o elemento neutro de G. Tal graduação é chamada de trivial.*

Exemplo 2.3.3 *Considere a álgebra de polinômios $A = K[x_1, \ldots, x_n]$ sobre um corpo K em variáveis comutativas. Considerando a soma direta*

$$A = \bigoplus_{d \in \mathbb{Z}} K[x_1, \ldots, x_n]_d,$$

onde $K[x_1, \ldots, x_n]_d = 0$ se $d < 0$ e $K[x_1, \ldots, x_n]_d$ é o K-espaço vetorial gerado pelos monômios $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ de grau $d = e_1 + \cdots + e_n$ para $d \geq 0$. Temos que A admite uma graduação natural pelo grupo dos números inteiros.

Observação 2.3.4 *Quando as variáveis do polinômio forem não comutativas, pode-se obter uma graduação natural pelos inteiros de forma análoga, onde as componentes homogêneas de grau d serão o K-espaços vetoriais gerados pelos monômios de grau d. Tal graduação será chamada usual.*

Também é possível definir uma gradução em módulos.

Definição 2.3.5 *Sejam G um grupo e A uma álgebra G-graduada. Dizemos que um A-módulo M é graduado, se existe uma família de grupos $\{M_g\}_{g\in G}$ tais que*

$$M = \bigoplus_{g\in G} M_g \text{ e } A_g M_h \subseteq M_{gh},$$

para todo g, $h \in G$.

Como no caso de álgebras, um elemento não nulo $x \in M$ é dito homogêneo se $x \in M_g$, para algum $g \in G$. Além disso, cada M_g é um A-módulo e todo elemento de M será uma soma finita de elementos homogêneos.

Aqui uma pergunta natural é: "se dado um A-módulo M G-graduado e N um submódulo, então M/N é G-graduado?". De fato isto ocorre de maneira natural para o caso em que N é também G-graduado, uma vez que

$$\frac{M}{N} = \bigoplus_{g\in G} \frac{M_g}{N \cap M_g}.$$

Dizemos que essa graduação do módulo quociente é herdada da graduação de M.

Nesta seção analisaremos a finitude necessária para os geradores de $S_{i,n}$ e $T_{i,n}$, ou seja, estudaremos o comprimento dos monômios que os geram. Dado $f \in S_{i,n}$ uma matriz com entradas polinomiais, podemos considerar seu polinômio característico

$$\chi_f(\lambda) = \lambda^n + \sum_{i=1}^{m} \sigma_i(f)\lambda^{i-1}.$$

onde $\sigma_1(f) = -tr(f)$ e os outros são obtidos pelas funções de Newton já discutidas na Seção 1.4. Claramente, temos pelo Teorema de Cayley-Hamilton que $\chi_f(f) = 0$. Além disso, note que podemos considerar em $S_{i,n}$ e $T_{i,n}$ uma graduação herdada pelos polinômios que os definem. Assim, $S_{i,n}$, como também $T_{i,n}$, admitem uma graduação usual pelo grupo abeliano $\mathbb{Z}$, onde o grau será o usual de uma aplicação polinomial e $(S_{i,n})_0 = (T_{i,n})_0 = K$. Daí, se $f \in S_{i,n}$ é homogêneo de grau h, então $\sigma_i(f)$ é homogêneo de grau ih.

Baseado nas observações anteriores e tendo em mente os Teoremas 2.1.9 e 2.2.2, nós desenvolveremos aqui uma abordagem geral do teorema da finitude que vamos aplicar para as algebras $T_{i,n}$ e $S_{i,n}$. Para isto, considere $A = \bigoplus_{i=0}^{\infty} A_i$ uma álgebra $\mathbb{Z}$-graduada comutativa sobre um corpo $A_0 = K$, $A^+ = \sum_{i=1}^{\infty} A_i$ e $A_d = \{0\}$, sempre que $d < 0$.

Lema 2.3.6 (Nakayama - versão graduada) *Sejam $M = \bigoplus_{i=0}^{\infty} M_i$ um A-módulo $\mathbb{Z}$-Graduado e N um submódulo de M que seja graduado. Se $M = N + A^+M$, então $M = N$.*

Demonstração: Suponhamos que $N = 0$ e que exista $m \in M$ homogêneo não nulo de menor grau possível. Como $m \in A^+M$, temos

$$m = \sum_i a_i v_i,$$

com $a_i \in A$ homogêneo de grau positivo e $v_i \in M$ homogêneo. Daí,

$$deg(a_i) + deg(v_i) = deg(m) \text{ e } deg(a_i) > 0,$$

para algum $i \in \mathbb{Z}_+$ não nulo, temos:

$$deg(v_i) < deg(m),$$

o que contradiz a minimalidade de $deg(m)$. Caso $N \neq 0$, basta considerarmos o módulo M/N. Daí, vemos que $M/N = A^+(M/N)$. Assim, pelo que já foi feito acima, $M/N = 0$, e consequentemente $M = N$. ∎

Antes de prosseguirmos, enunciaremos um conhecido resultado de PI-álgebra o qual a demonstração pode ser encontrada em [12, pág. 79].

Teorema 2.3.7 ***(Teorema de Nagata-Higman)*** *Seja R é uma álgebra associativa satisfazendo a identidade $x^n \equiv 0$, para algum $n \in \mathbb{N}$. Se $charK = 0$ ou maior que n, então $R^N = 0$ para $N \leq 2^n - 1$, ou seja,*

$$x_1 x_2 \cdots x_{2^n - 1} \equiv 0$$

é uma identidade para R.

Observação 2.3.8 *Razmyslov, em [32], melhorou o índice de nilpotência dado no teorema anterior. Mais precisamente, nas notações do teorema anterior, Razmyslov argumentou que $N \leq n^2$.*

Consideremos agora uma álgebra associativa $\mathbb{Z}$-graduada R e um subconjunto X de R^+ tal que:

(i) $R_0 = A_0 = K$;

(ii) $A \subseteq Z(R)$, onde $Z(R)$ é o centro da álgebra R; e,

(iii) R é gerado como uma A-álgebra por 1 e X.

Teorema 2.3.9 *Se cada elemento $r \in R^+$ satisfaz um polinômio mônico de grau n (onde o polinômio depende de r, mas o n é fixo) $x^n + \sum_{i=1}^{n} \alpha_i x^{n-i} \equiv 0$, com $\alpha_i \in A^+$, e $charK = 0$ ou $charK > n$, então R é gerada sobre A pelos monômios nos elementos de X de grau menor ou igual a $2^n - 2$.*

Demonstração: Consideremos a álgebra $U = R^+/A^+R^+$. Pelo Lema 2.3.6, basta mostrar que os monômios com elementos em $\overline{X}$ de grau menor ou igual a $2^n - 1$ (com $n \geq 1$) geram U, como espaço vetorial sobre K. Com efeito, dado $x \in R^+$, temos $x = \sum_i a_i m_i$, com $a_i \in A$ e cada m_i é um monômio de elementos de X. Assim,

$$x = \sum_i a_i^{(0)} m_i + \sum_j a_j m_j,$$

onde $a_i^{(0)} \in A_0 = K$ e $a_j \in A^+$. Deste modo, em U, temos:

$$\overline{x} = \overline{\sum_i a_i^{(0)} m_i} + \overline{\sum_j a_j m_j} = \sum_i a_i^{(0)} \overline{m_i}.$$

Segue então, da arbitrariedade de x, que U é gerado por $\overline{X}$, como álgebra.

Resta mostrar que U é uma álgebra nilpotente de índice menor ou igual do que $2^n - 1$. Mas isto é imediato do fato que dado $r \in R^+$, temos $r^n + \sum \alpha_i r^{n-i} = 0$, com $\alpha_i \in A_i$. Disto, segue que qualquer $\bar{r} \in U$ satisfaz a identidade $x^n \equiv 0$. O resultado segue aplicando o Teorema de Nagata-Higman. ∎

Assumiremos agora R como uma álgebra munida com uma aplicação A-linear $t : R \to A$ preservando graus. Ademais, assumiremos que, se T denota a álgebra gerada por um conjunto X, os elementos $t(T^+)$ geram A^+, como ideal.

Proposição 2.3.10 *Sobre as hipóteses do Teorema 2.3.9 e R satisfazendo também as hipóteses do comentário do parágrafo anterior, A é gerada como álgebra por elementos $t(r)$, onde r percorre todos os monômio de elementos em X de grau $\leq 2^n - 1$.*

Demonstração: Pelo teorema anterior, R é gerado como uma A-álgebra pelos monômios nos elementos de X de grau menor ou igual a $2^n - 2$, tal conjunto de monômios será denotado por S. Além disso, considere B a subálgebra de A gerada pelos elementos $t(r)$, onde r corre no conjunto S' dos monômios nos elementos de X de grau menor ou igual do que $2^n - 1$. Assim, basta mostrar que $B = A$. Ora, mas como B é uma álgebra graduada e A é um B-módulo graduado, então pelo Lema 2.3.6 é suficiente mostrar que $A = B + B^+A$. Daí, como A^+ é gerado por $t(T^+)$ como ideal sobre a álgebra A e vale $R = AS$ e $T^+ \subseteq T.X$, segue que $T^+ \subseteq ASX$, já que $T = \langle X \rangle \subseteq \langle 1, X \rangle = R$. Daí, pela definição do conjunto S' e como a aplicação traço preserva graus (e, por isso, inclusões também), segue que:

$$t(T^+) \subseteq t(ASX) \Rightarrow t(T^+) \subseteq A.t(SX) = AB^+$$

onde SX é o conjunto dos monômios com grau positivo menor ou igual $2^n - 1$ nos elementos de X. Consequentemente,

$$A^+ = A \cdot t(T^+) \subseteq AB^+ \Rightarrow A = A_0 + A^+ \subseteq B + B^+A.$$

Daí, como B e AB^+ são subconjuntos da álgebra A, temos $A = B + B^+A$. E assim, segue o desejado. ∎

Nós podemos aplicar essa proposição no caso em que já sabemos que A é gerada, como uma álgebra, pelos elementos $t(r)$, com $r \in T$. Em particular, nós podemos aplicar a última proposição para obter o Teorema da Finitude para os anéis de invariantes.

Teorema 2.3.11 *a) O anel $T_{i,n}$ é gerado, sobre K, pelos elementos $tr(X_{i_1} \cdots X_{i_j})$, com $j \leq 2^n - 1$.*

b) $S_{i,n}$ é gerado, como $T_{i,n}$-álgebra, pelos elementos $X_{i_1}X_{i_2} \cdots X_{i_j}$, com $j \leq 2^n - 2$.

Demonstração: Basta tomar $t = tr, X = \{X_1, \ldots, X_i\}, A = T_{i,n}$ e $R = S_{i,n}$. Daí, aplicando a Proposição 2.3.10 temos o item a). Ademais, como todo elemento de $S_{i,n}$ satisfaz seu polinômio característico, o item b) segue aplicando o Teorema 2.3.9. ∎

2.4 Identidades com traço

Consideremos agora o problema de encontrar, em uma forma sistemática, todas as relações acerca dos elementos $tr(M)$ e M, onde M é um monômio nas variáveis concomitantes X_j, onde $j = 1, 2, \ldots, \infty$. Indicaremos por $T_{\infty,n}$ e $S_{\infty,n}$ o anel dos invariantes e concomitantes de uma quantidade infinita de matrizes, respectivamente.

Teorema 2.4.1 *$S_{\infty,n}$ é a álgebra relativamente livre com traço na variedades das álgebras que satisfazem $T_{Tr}(M_n(K), tr)$*

Demonstração: Considerando o traço de matrizes, existe uma aplicação natural $trp\colon S_{\infty,n} \to T_{\infty,n}$ tal que para todo $f \in S_{\infty,n}$ temos que

$$(trp \circ f(X_1, \ldots, X_m))(A_1, \ldots, A_m) = tr(f(A_1, \ldots, A_m)), \tag{2.11}$$

para todo $A_1, \ldots, A_m \in M_n(K)$. Claramente, $(S_{\infty,n}, trp)$ é uma álgebra com traço. Utilizando uma variação do Teorema 1.3.13 é suficiente mostrar que

$$S_{\infty,n} \simeq (G\langle X\rangle / T_{Tr}(M_n(K), tr)),$$

onde $G\langle X\rangle$ é a álgebra de polinômios generalizados dada na Seção 1.5. Para este fim, considere a aplicação canônica $\psi\colon G\langle X\rangle \to S_{\infty,n}$ dada por $\psi(x_i) = X_i$, para todo $i = 1, 2, \ldots$. Nestas condições, $T_{Tr}(M_n(K), tr) \subseteq ker\psi$. Por outro lado, seja f um elemento de $ker\varphi$, então para quaisquer projeções concomitantes $X_1, \ldots, X_n$ em $S_{\infty,n}$, temos que $f(X_1, \ldots, X_n) = 0$, e assim para toda n-upla $(A_1, \ldots, A_n)$ de elementos em $M_n(K)$, temos que $0 = (f(X_1, \ldots, X_n))(A_1, \ldots, A_n) = f(A_1, \ldots, A_n)$. Concluímos que $f \in T_{Tr}(M_n(K), tr)$ e, consequentemente, $ker\varphi = T_{Tr}(M_n(K), tr)$. ■

Utilizando $G\langle X\rangle$ e $TG\langle X\rangle$, notações utilizadas na Seção 1.5, temos duas aplicações sobrejetoras

$$\pi : TG\langle X\rangle \to T_{\infty,n} \quad \text{e} \quad \tau : G\langle X\rangle \to S_{\infty,n}.$$

Nosso objetivo consiste em encontrar relações entre invariantes e concomitantes e, para isto, descreveremos os núcleos das aplicações π e τ. O teorema anterior fica migrando entre as estruturas de matrizes genéricas e concomitantes, de forma mais conveniente, dependo da situação, e assim podemos tentar determinar tais relações. Inicialmente, observemos que temos a compatibilidade de τ e π com as aplicações traço, isto é, o diagrama

$$\begin{tikzcd} G\langle X\rangle \arrow[r, "\tau"] \arrow[d, "Tr"'] & S_{\infty,n} \arrow[d, "trp"] \\ TG\langle X\rangle \arrow[r, "\pi"'] & T_{\infty,n} \end{tikzcd}$$

é comutativo, onde Tr é o traço formal em $G\langle X\rangle$ herdado pelo de $KTR\langle X\rangle$, e trp é o traço construído a partir do traço usual de matrizes, ver aplicação (2.11). Finalmente, τ é compatível com a substituição, isto é, $\tau(f(g_1,\ldots,g_i,\ldots)) = (\tau f)(\tau(g_1),\ldots,\tau(g_i),\ldots)$, para todo $f, g_1,\ldots,g_i,\ldots \in G\langle X\rangle$.

Dos comentários acima, a próxima proposição segue imediatamente:

Proposição 2.4.2 *Os ideais $ker\pi$ e $ker\tau$ são T-ideais com traço.*

Iremos nos referir aos elementos de $ker\pi$ como identidades com traço puro de matrizes de ordem n e aos elementos do $ker\tau$ como identidades com traço de matrizes de ordem n.

Dada uma permutação $\sigma \in S_m$, onde σ tem a seguinte decomposição em ciclos disjuntos

$$\sigma = (i_1 \ldots i_k)(j_1 \ldots j_h)\cdots(t_i \ldots t_l),$$

definiremos um elemento $\phi_\sigma \in TG\langle X\rangle$ da seguinte forma

$$\phi_\sigma = \phi_\sigma(x_1,\ldots,x_m) = Tr(x_{i_1}\cdots x_{i_k})Tr(x_{j_1}\cdots x_{j_h})\cdots Tr(x_{t_1}\cdots x_{t_l}).$$

Veja que ϕ_σ define uma função polinomial de grau m e usando a notação dos Teoremas 2.1.6 e 2.1.8 nós temos que, se $A_1,\ldots,A_m \in M_n(K)$, então

$$\pi(\phi_\sigma)(X_1,\ldots,X_m)(A_1,\ldots,A_m) = \mu_\sigma(A_1 \otimes A_2 \otimes \cdots \otimes A_m). \tag{2.12}$$

O seguinte resultado segue como consequência da teoria do Diagrama de Young.

Teorema 2.4.3 *a) Um elemento $\sum_{\sigma\in S_m} \alpha_\sigma\phi_\sigma$ é uma identidade com traço para matrizes de ordem n se, e somente se, o elemento $\sum_{\sigma\in S_m} \alpha_\sigma\sigma$ pertence ao ideal da álgebra de grupo de S_m gerada pelos simetrizadores de Young relativos aos diagramas com pelos menos $n+1$ linhas.*

b) Em particular nós temos a identidade fundamental com traço

$$\mathcal{F}(x_1,\ldots,x_{n+1}) = \sum_{\sigma\in S_{n+1}} sgn(\sigma)\phi_\sigma,$$

correspondendo ao diagrama de Young com uma coluna e $n+1$ linhas.

Demonstração: $a)$ Da Igualdade 2.12, $\sum \alpha_\sigma\phi_\sigma$ é uma identidade com traço se, e somente se, a aplicação $\sum \alpha_\sigma\mu_\sigma$ é identicamente nula. Ora, mas isso é equivalente aos endomorfismos $\sum \alpha_\sigma \lambda_\sigma$ em $V^{\otimes m}$ induzido por $\sum \alpha_\sigma \sigma$ serem zero. Daí, usando a Teoria de Young e representação do S_m desenvolvida na Seção 1.7, temos o desejado, pois com elas conseguimos entender a ação do simetrizados $c_\lambda \in KS_m$ sobre $V^{\otimes m}$. Vejamos em detalhes.

Seja $\lambda = (\lambda_1, \ldots, \lambda_k)$ uma partição de m e munamos o correspondente diagrama de Young com a tabela Standard. O subgrupo P_T de S_m que preserva cada linha torna-se, em seguida, $P_T = S_{\lambda_1} \times \cdots \times S_{\lambda_k} \hookrightarrow S_m$. Com $a_T = \sum_{p \in P_T} p$, vemos que a imagem da ação de a_T sobre $V^{\otimes m}$ é o subespaço

$$Im(a_T) = Sym^{\lambda_1} V \otimes \cdots \otimes Sym^{\lambda_k} V \hookrightarrow V^{\otimes m},$$

aqui, $Sym^i V$ denota o subespaço de tensores simétricos em $V^{\otimes i}$.

Equivalentemente, dados os diagramas de Young correspondente à partição dual de λ, ou seja, $\lambda^* = (\mu_1, \cdots, \mu_l)$, o subgrupo Q_λ de S_m que preserva cada linha de λ é

$$Q_\lambda = S_{\mu_1} \times \cdots \times S_{\mu_K} \hookrightarrow S_d.$$

Com $b_\lambda = \sum_{q \in Q_\lambda} sgn(q) q$, vemos que a imagem da ação de b_T sobre $V^{\otimes m}$ é o subespaço

$$Im(b_T) = \bigwedge^{\mu_1} V \otimes \ldots \otimes \bigwedge^{\mu_k} V \hookrightarrow V^{\otimes m},$$

aqui, $\bigwedge^i$ denota o subespaço de todos os tensores antissimétricos em $V^{\otimes i}$. Note que $\bigwedge V = 0$, sempre que i é maior que $dimV = n$, pois os tensores são antissimétricos, ou seja, a imagem da ação de b_T sobre $V^{\otimes m}$ é zero sempre que a partição dual λ^* contém uma linha de comprimento maior que $n+1$, ou equivalentemente, λ tendo mais que $n+1$ linhas. Daí, como $c_T = a_T b_T$, temos o desejado.

$b)$ Considerando a partição $\lambda = (1, 1, \ldots, 1)$ de $n+1$, obtemos que

$$P_T = \{Id\} \text{ e } Q_T = S_{n+1}.$$

Daí, $a_T = 1, b_T = \sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma$. Logo, o simetrizador de Young é dado por

$$c_T = \sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma$$

e como o ideal descrito por ele é justamente os múltiplos escalares de $\sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma$, segue do item $a)$ o desejado.

■

Como $\mathcal{F}(x_1,\ldots,x_{n+1})$ é multilinear em todas as variáveis, podemos aplicar um procedimento semelhante ao usado na prova do Teorema 2.2.2 para escrevê-lo formalmente como

$$\mathcal{F}(x_1,\ldots,x_{n+1}) = Tr(\mathcal{G}(x_1,\ldots,x_n)x_{n+1}), \tag{2.13}$$

onde $\mathcal{G}(x_1,\ldots,x_n) \in G\langle X\rangle$ e

$$\mathcal{G}(x_1,\ldots,x_n) = \sum_{k=0}^{n}(-1)^{k+1}\sum_{i_1\neq i_2\neq\cdots\neq i_k} x_{i_1}x_{i_2}\cdots x_{i_k}\sum_{\sigma\in S_{n-k}} sgn(\sigma)\phi_\sigma,$$

com S_{n-k} agindo sobre $\{1,\ldots,m\}-\{i_1,\ldots,i_k\}$.

Uma consequência do Teorema 2.4.3 é o seguinte:

Corolário 2.4.4 *a) Uma identidade com traço puro multilinear de grau $n+1$ em $n+1$ variáveis é múltipla escalar de $\mathcal{F}(x_1,\ldots,x_{n+1})$.*

b) Uma identidade multilinear com traço de grau n em n variáveis é múltipla escalar de $\mathcal{G}(x_1,\ldots,x_n)$.

c) $\mathcal{G}(x_1,\ldots,x_n)$ é obtido por linearização completa do polinômio de Cayley-Hamilton de grau n, vezes $(-1)^{n+1}$.

Demonstração: *a*) Tomado $m=n+1$ no Teorema 2.4.3 , item *a*), o ideal aí descrito será um múltiplo escalar de $\sum_{\sigma\in S_{n+1}} sgn(\sigma)\sigma$. Assim, teremos o desejado.

b) Pela relação estabelecida no Teorema 2.2.2, temos que $f(x_1,\ldots,x_n)\in ker\tau$ se, e somente se, $Tr(f(x_1,\ldots,x_n)x_{n+1})\in ker\pi$. Assim, segue do item (*a*) e pela Igualdade (2.13) o desejado.

c) Das fórmulas de Newton (veja Seção 1.4), vimos que o polinômio característico $\chi_A(\lambda)$ de uma matriz A é um polinômio com coeficientes podendo ser escrito via elementos $tr(A^i)$. Isso nos permite construir um polinômio formal Cayley-Hamilton $\chi_X(X)$, sendo X uma matriz genérica, substituindo no seu polinômio característico o termo $tr(A^k)$ com $trp(X^k)$ e A^l com X^l.

Se X é uma projeção concomitante, então $\chi_X(X)$ é um elemento de $S_{\infty,n}$ homogêneo de grau n. Além disso, pelo Teorema de Cayley-Hamilton, temos $\chi_x(x)\in ker\tau$, ou seja, é uma identidade com traço. Assim, polarizando completamente $\chi_X(X)$ obtemos uma identidade multilinear com traço de grau n. Segue então, pelo item *b*), que ele é um múltiplo escalar de $\mathcal{G}(x_1,\ldots,x_n)$. Mas como seu termo líder (o termo de maior grau com coeficiente em $TG\langle X\rangle)$ é $\sum_{\sigma\in S_n} x_{\sigma(1)}\cdots x_{\sigma(n)}$, ao compararmos com a forma explícita de $\mathcal{G}(x_1,\ldots,x_n)$, segue o desejado. ■

Nós estamos agora prontos para provar o segundo teorema fundamental.

Teorema 2.4.5 (Segundo Teorema Fundamental) *a) O ideal $ker\pi$ é gerado pelos elementos $\mathcal{F}(M_1,\ldots,M_{n+1})$, onde os M_i's variam sobre todos os possíveis monômios em $K\langle X\rangle$.*

b) O ideal $ker\tau$ é gerado por todos os elementos $\mathcal{F}(M_1,\ldots,M_{n+1})$ e $\mathcal{G}(N_1,\ldots,N_n)$, onde os M_i's e N_j's variam sobre todos os possíveis monômios em $K\langle X\rangle$.

Demonstração: $a)$ Primeiramente, nós queremos reduzir a análise para identidades multilineares, uma vez que esse ideal é fechado para polarização e podemos aplicar o Corolário 1.9.7. Seja $f\in ker\pi$ multilinear e de grau m. A priori f pode depender de mais de m variáveis, mas podemos separar f como um soma de polinômios f_i cada um dependendo de m variáveis, tais que f_i e f_j não dependem das mesmas variáveis, se $i\neq j$. Definindo algumas variáveis iguais a zero, vemos que cada f_i é uma identidade com traço. Portanto, nós podemos assumir que f é multilinear de grau m e depende das concomitantes $X_1, X_2,\ldots,X_m$, então

$$f=\sum_{\sigma\in S_m}\alpha_\sigma\phi_\sigma.$$

e, pelo Teorema 2.4.3, o elemento $\sum\alpha_\sigma\sigma$ da álgebra de grupo pertence ao ideal gerado pelos simetrizadores de Young relativo ao diagrama com pelo menos $n+1$ linhas.

Afirmação 1: Este ideal é gerado pelo simetrizador de Young relativo à partição $(1,1,\ldots,1)$ de $n+1$ sobre a imersão natural de S_{n+1} em S_m, onde $m\geq n+1$.

Seja T_λ um diagrama de Young tendo $k\geq n+1$ células na primeira coluna e c_λ um simetrizador dessa tabela. Consideremos que as células na primeira coluna são preenchidas por $I=\{i_1,\ldots,i_k\}$. Denotando por S_I o grupo das permutações de elementos de I e como $Q_\lambda=S_I\times Q'$, para algum Q' subgrupo de S_m que estabilize as outras colunas do diagrama, vemos que

$$b_\lambda=\left(\sum_{\sigma\in S_I} sgn(\sigma)\sigma\right).b',\ b'\in KQ'.$$

Daí, c_λ pertence ao ideal bilateral gerado por $C_I=\sum_{\sigma\in S_I} sgn(\sigma)\sigma$. Considere a permutação ω em S_m dada por $\omega(i_r)=r$, para todo $r\in\{1,\ldots,k\}$, e os demais sendo fixados. Neste caso, podemos interpretar que o c_λ pertence ao ideal gerado por $C_k = \omega C_I \omega^{-1} = \sum_{\sigma \in S_k} sgn(\sigma)\sigma$. É suficiente provar que o C_k está no ideal gerado por C_{n+1}, para todo $n+1 \leq k \leq m$. Mas isso segue do fato de definirmos $\overline{\omega}(i_r) = r$, para todo $r \in \{1, \ldots, n+1\}$ (iremos considerar a mesma notação já usada acima, por abuso de notação) e fixa os demais. Concluindo a Afirmação 1.

Da Afirmação 1,

$$\sum_{\sigma \in S_m} \alpha_\sigma \sigma = \sum_{\tau_i, \tau_j \in S_m} \alpha_{ij} \tau_i \left(\sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma \right) \tau_j.$$

Pelo item $b)$ do Teorema 2.4.3 temos que cada parcela do elemento descrito acima está associado a um polinômio que é identidade com traço para matrizes. Assim, basta analisarmos a forma das identidades com traço associadas aos elementos:

$$\tau \left(\sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma \right) \xi, \tag{2.14}$$

onde $\tau, \xi \in S_m$.

Ora, mas analisar as identidades da forma acima, é suficiente estudar as da forma $\sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma \cdot \xi\tau$. Com efeito, observe que se $\sum_{\lambda \in S_m} \alpha_\lambda \lambda$ corresponde ao polinômio com traço $H(X_1, \ldots, X_m)$ e $\theta \in S_m$, então $\theta(\sum_{\lambda \in S_m} \alpha_\lambda \lambda)\theta^{-1}$ corresponde ao polinômio com traço $H(X_{\theta(1)}, \ldots, X_{\theta(m)})$. Assim, como

$$\tau(\sum sgn(\sigma)\sigma)\xi = \tau(\sum sgn(\sigma)\sigma)\xi\tau \cdot \tau^{-1}.$$

Portanto, as identidades associadas ao elemento (2.14) são iguais as identidades associadas a $(\sum sgn(\sigma)\sigma)\xi\tau$, a menos de posição de variáveis.

No que segue em nossa demonstração, chamaremos $\xi\tau = \eta$.

Afirmação 2: Existe $\gamma \in S_m$ contendo, em cada ciclo, no máximo um elemento $1, 2, \ldots, n+1$, tal que

$$\sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma \cdot \eta = \pm \sum_{\sigma \in S_{n+1}} sgn(\sigma)\sigma \cdot \gamma.$$

Para provar esta afirmação, basta mostrarmos que podemos escrever $\eta = \lambda\gamma$, para algum $\lambda \in S_{n+1}$ e γ do tipo desejado, pois tomando $\beta = \sigma\lambda$, temos

$$\begin{aligned}\sum_{\sigma} sgn(\sigma)\sigma\lambda &= \sum_{\beta} sgn(\beta\lambda^{-1})\beta\lambda^{-1}\lambda \\ &= sgn(\lambda)\sum_{\beta} sgn(\beta)\beta \\ &= sgn(\lambda)\sum_{\sigma} sgn(\sigma)\sigma.\end{aligned}$$

Esta última igualdade segue simplesmente renomeando as permutações. Assim, fazendo γ agir (a direita) em ambos os lados da igualdade anterior, obteremos o resultado. Assuma que η contém no primeiro ciclo mais que um elemento de $\{1, \ldots, n+1\}$, digamos 1 e 2, pois os ciclos são disjuntos. Diante deste comentário, podemos escrever η da seguinte maneira:

$$\eta = (1i_1i_2 \ldots i_r 2j_1j_2 \ldots j_s)(k_1 \ldots k_\alpha) \cdots (z_1 \ldots z_\zeta).$$

Daí, obtemos

$$(12)\eta = (1i_1i_2 \ldots i_r)(2j_1j_2 \ldots j_s)(k_1 \ldots k_\alpha) \cdots (z_1 \ldots z_\zeta).$$

Neste caso, tomando

$$\gamma = (1i_1i_2 \ldots i_r)(2j_1j_2 \ldots j_s)(k_1 \ldots k_\alpha) \cdots (z_1 \ldots z_\zeta) \text{ e } \lambda = (12)^{-1} = (12)$$

temos o desejado para este caso particular. No caso em que η tiver um ciclo contendo mais que um elemento, realizamos o procedimento no máximo n vezes. Assim, provamos a nossa afirmação.

Por fim, se $\sigma \in S_{n+1}$ e γ são do tipo acima, o ciclo de $\sigma\gamma$ é obtido formalmente através da seguinte substituição: em cada ciclo de σ, no lugar de um elemento 1 a sequência $1i_1i_2 \ldots i_k$, no lugar do 2, a sequência $2j_1 \ldots j_l$ e, seguindo desse modo, substituindo $n+1$, pela sequência $(n+1)t_1 \cdots t_2$ e terminando com ciclos de η em que os elementos $1, 2, \ldots, n+1$ não aparecem. Para ficar mais claro esse procedimento, vejamos um exemplo: Sendo $\sigma = (12)(34)$ e $\gamma = (1i_1)(2j_1j_2)(3k_1)(4l_1l_2)(m_1m_2m_3)$, com γ formado por ciclos disjuntos, temos

$$\sigma\gamma = (1i_12j_1j_2)(3k_14l_1l_2)(m_1m_2m_3).$$

Daí, se

$$\gamma = (1i_1 \ldots i_k)(2j_1 \ldots j_s) \cdots ((n+1)t_1 \ldots t_l)(\lambda_1 \ldots \lambda_r) \cdots (\mu_1 \ldots \mu_z),$$

podemos escrever o polinômio com traço correspondente a $(\sum_{\sigma\in S_{n+1}} sgn(\sigma)\sigma)\cdot\gamma$ como

$$(\mathcal{F}(x_1x_{i_1}\cdots x_{i_k}, x_2x_{j_1}\cdots x_{j_s},\ldots,x_{n+1}x_{t_1}\cdots x_{t_k}))\,Tr(x_{\lambda_1}\cdots x_{\lambda_r})\cdots Tr(x_{\mu_1}\cdots x_{\mu_z}).$$

Portanto, repetindo esse processo para todas parcelas de f, o teorema segue.

b) Seja $H(x_1,\ldots,x_m)\in ker\tau$ uma identidade com traço das matrizes de ordem n. Então o polinômio com traço $Tr(H(x_1,\ldots,x_m)\cdot x_{m+1})$ está em $ker\pi$, o qual, pelo item $a)$, tem a forma

$$\sum \lambda_{i_1\ldots i_{n+1}}\mathcal{F}(M_{i_1},\ldots,M_{i_{n+1}}),$$

com $\lambda_{i_1\ldots i_{n+1}}\in TG\langle X\rangle$ e é linear em x_{m+1}. Portanto, podemos assumir que x_{m+1} aparece linearmente em cada termo da soma. Consideremos, então, o termo

$$\lambda\mathcal{F}(M_1,\ldots,M_{n+1}),$$

onde x_{m+1} aparece em λ ou em um dos monômios M_i's. Se x_{m+1} aparece em λ, podemos escrever $\lambda = Tr(\lambda' x_{m+1})$, onde $\lambda'\in G\langle X\rangle$. Caso contrário, permutando os monômios se necessário, podemos assumir que $M_{n+1} = A\cdot x_{m+1}\cdot B$, onde A, B são monômios em $K\langle X\rangle$. Então, por linearidade e da propriedade cíclica do traço formal,

$$\begin{aligned}\lambda\mathcal{F}(M_1,\ldots,M_{n+1}) &= \lambda Tr(\mathcal{G}(M_1,\ldots,M_n)\cdot A\cdot x_{m+1}\cdot B)\\ &= Tr(\lambda\cdot B\cdot\mathcal{G}(M_1,\ldots,M_n)\cdot A\cdot x_{m+1}).\end{aligned}$$

Assim,

$$\begin{aligned}Tr(H(x_1,\ldots,x_m)x_{m+1}) &= Tr\big([\sum\lambda'_{i_1\ldots i_{n+1}}\mathcal{F}(M_{i_1},\ldots,M_{i_{n+1}})\\ &+ \sum\lambda_{j_1\ldots j_{n+1}}\cdot B_{j_{n+1}}\mathcal{G}(N_{j_1},\ldots,N_{j_n})A_{j_{n+1}}]\cdot x_{m+1}\big).\end{aligned}$$

Como a aplicação traço é não degenerada, segue o resultado. ■

Podemos expressar o teorema anterior de uma forma mais conveniente usando os análogos não homogêneos de $\mathcal{F}$ e $\mathcal{G}$. Já sabemos que $\mathcal{G}$ é obtido a menos de sinal, pelo polinômio característico por meio da polarização completa. Quanto a $\mathcal{F}$ temos um resultado similar, já que $\mathcal{F}(x_1,\ldots,x_{m+1}) = Tr(\mathcal{G}(x_1,\ldots,x_m)x_{m+1})$. O análogo do polinômio característico, em $TG\langle X\rangle$, é a expressão de $tr(A^{n+1})$ em termos dos elementos $tr(A^i)$, com $i\leq n$, obtido pela equação $trp(\chi_A(X)\cdot X)$ que na substituição de X por A é zero. Denotaremos a expressão formal associada à $\chi_x(x)$ e a $tr(\chi_x(x)\cdot x)$, de $\mathcal{G}(x)$ e $\mathcal{F}(x)$, respectivamente. Assim, $\mathcal{G}(x)$ é o "polinômio de Cayley Hamilton de grau n" e $\mathcal{F}(x)$ é a expressão de $Tr(x^{n+1})$ em termos de $Tr(x^i)$, e $i\leq n$. Então, temos:

Teorema 2.4.6 *a) $ker\pi$ é o T-ideal com traço puro de $TG\langle X\rangle$ gerado por $\mathcal{F}(x)$.*

b) $ker\tau$ é o T-ideal com traço de $G\langle X\rangle$ gerado pelo polinômio característico $\mathcal{G}(x)$. Aqui X é uma j-concomitante

Demonstração: Observe que (a) e (b) seguem do Teorema 2.4.5 junto com a definição dos T-ideais com traço de $TG\langle X\rangle$ e $G\langle X\rangle$, uma vez que provamos que a completa polarização das formas $\mathcal{F}(X)$ e $\mathcal{G}(X)$, aqui X é um projeção concomitante, encontram-se no T-ideal que eles geram, uma vez que podemos substituir o processo de polarização pelo processo de multilinearização.

Pela Observação 1.9.8, o resultado final da multilinearização é a mesma que a da polarização completa e então a afirmação segue, uma vez que claramente, multilinearizando cada gerador de um T-ideal, continuamos com o mesmo T-ideal.

■

Agora podemos deduzir um intrigante corolário que "amarra" completamente o Teorema 2.3.11 ao Teorema de Nagata-Higman, para isto iremos resgatar a notação dada antes do Lema 2.3.6. Mais explicitamente iremos considerar $K^0\langle x_1,\ldots,x_i\rangle$ sendo a álgebra livre sem unidade em i indeterminadas não comutativas (a qual pode também ser denotado por $K^+\langle x_1,\ldots,x_i\rangle$ a fim de ser compatível com a notação) e $T^+_{i,n}S_{i,n}$ é o ideal com traço da álgebra das matrizes genéricas cujos coeficientes estão em T^+_i, isto é, a álgebra dos elementos que são traços não constantes.

Corolário 2.4.7 *O anel $S^+_{i,n}/T^+_{i,n}S_{i,n}$ é isomorfo à álgebra livre sem unidade $K^0\langle x_1,\ldots,x_i\rangle$ em i variáveis, módulo o T-ideal definido pela identidade polinomial $f(x)=x^n$.*

Demonstração: É claro que $S^+_{i,n}/T^+_{i,n}S_{i,n}$ satisfaz a identidade $f(x)$ e ele é gerado, módulo $T^+_{i,n}S_{i,n}$, pelas aplicações n coordenadas $X_j, j=1,\ldots,i$ sobre K, como K-álgebra (ver Teorema 2.3.11).

Portanto, a aplicação canônica

$$\Psi : K^0\langle x_1,\ldots,x_i\rangle \to S^+_{i,n}/T^+_{i,n}S_{i,n}$$

onde $\Psi(x_i)=X_i$ e os polinômios do domínio são vistos como polinômios ordinários sem traço, é sobrejetiva. Além disso, $ker\Psi$ contém o T-ideal J gerado pela identidade polinomial $f(x)$. Temos que mostrar que a aplicação induzida

$$\bar{\Psi} : K^0\langle x_1,\ldots,x_i\rangle/J \to S^+_{i,n}/T^+_{i,n}S_{i,n}$$

é um isomorfismo, ou seja, $ker\Psi \subseteq J$.

Mostremos que as únicas relações entre os elementos X_j em $S^+_{i,n}/T^+_{i,n}S_{i,n}$ são dedutíveis da identidade polinomial $f(x)$.

Temos uma apresentação de $S^+_{i,n}$ e $T^+_{i,n}$ dada pelo Teorema 2.3.11. A fim de dar uma apresentação para $S^+_{i,n}/T^+_{i,n}S_{i,n}$, temos que adicionar à relação dada nesse teorema, a relação $Tr(M) = 0$ para todo monômio M de grau positivo. Se começarmos dessas relações, isto é, se construirmos $S^+_{i,n}/T^+_{i,n}S_{i,n}$, pegamos justamente a álgebra livre sem unidade sobre K, já que $T_{i,n}/T^+_{i,n} \simeq K$. Logo não há mais nenhum polinômio que se anula em $S^+_{i,n}/T^+_{i,n}S_{i,n}$ além do polinômio característico. Ou seja, $h \in ker\Psi$ significa que a concomitante associada a ela é nula, módulo $T^+_{i,n}S_{i,n}$. Porém, h é um polinômio sem coeficientes que sejam traço, com isto podemos interpretar h como sendo uma identidade com traço.

Agora, se lermos nesta álgebra a relação dada, por exemplo, pelo Teorema 2.4.6, vemos que o polinômio característico $\mathcal{G}(x)$ torna-se x^n, a aplicação traço agora é 0 (bem como $\mathcal{F}(x)$), e então o T-ideal gerado por $\mathcal{G}(x)$ torna-se, módulo $T^+_{i,n}$, exatamente o T-ideal gerado pela identidade $f(x)$. Concluindo que $ker\Psi \subseteq J$.

■

Há uma outra maneira de formular o corolário anterior, que enunciamos por completude.

Corolário 2.4.8 *Se R é uma álgebra associativa sobre um corpo de característica 0 e R satisfaz a identidade polinomial $f(x) = x^n$, então R satisfaz todas as identidades polinomiais da álgebra das matrizes de ordem n.*

Demonstração: É fácil observar que $T(M_n(K)) = ker\tau \cap K\langle x_1, x_2, \ldots\rangle$. Além disso, considere a aplicação

$$\begin{aligned} \psi : K^0\langle x_1, x_2, \ldots\rangle &\rightarrow S^+_{\infty,n}/T^+_{\infty,n}S_{\infty,n} \\ f(x_1, \ldots, x_n) &\mapsto f(X_1, \ldots, X_n) + T^+_{\infty,n}S_{\infty,n} \end{aligned}$$

Dado um $f \in T(M_n(K))$, temos que seu termo constante é nulo, logo $f \in K^0\langle x_1, x_2, \ldots\rangle$, observe ainda que $f(X_1, \ldots, X_n) = f(\bar{X}_1, \ldots, \bar{X}_n)$, para todo $f \in S_{\infty,n}$ com coeficientes que não dependem da aplicação traço. Consequentemente,

$$T(M_n(K)) \subseteq T(S^+_{\infty,n}/T^+_{\infty,n}S_{\infty,n}) = \langle x^n\rangle$$

a última igualdade segue do corolário anterior. Temos então, que dada uma álgebra associativa R que satisfaz a identidade $\langle x^n \rangle$, isto é,

$$\langle x^n \rangle \subseteq T(R) \Rightarrow T(M_n(K)) \subseteq T(R).$$

Portanto, R satisfaz todas as identidades da álgebra das matrizes de ordem n. ■

Terminamos esse capítulo observando que se R é uma álgebra nilpotente com índice de nilpotência n sobre um corpo de característica zero, então ela satisfaz todas as identidades da álgebra das matrizes de ordem n, em particular satisfaz todas as identidades com traço dessa álgebra, considerando a aplicação traço de $t : R \to R$ sendo nula.

No próximo capítulo, iremos mostrar que R, nas condições do parágrafo anterior, é uma subálgebra das álgebras das matrizes sobre um anel comutativo, motivando a pesquisa de determinar subálgebras do anel de matrizes. Nesta linha de raciocínio, será que é suficiente verificar que um anel que satisfaz o polinômio de Cayley-Hamilton é subálgebra da álgebra de matrizes sobre um anel comutativo?

Capítulo 3

Mergulhos em anéis de matrizes

Uma questão interessante na teoria de anéis é identificar subanéis dos anéis de matrizes. Neste caminho, surge uma pergunta natural: "Qual seria uma condição necessária para existir um mergulho de um anel numa álgebra de matrizes (possivelmente com coeficientes em algum anel comutativo)?". Como é relatado no artigo "An example in PI-ring" ([34]), várias conjecturas já foram feitas sobre condições para permitir tais mergulhos. Por exemplo, na teoria das PI-álgebras, uma condição necessária para a existência de tal mergulho é que o anel satisfaça todas as identidades polinomiais do anel de matrizes. Porém, como é visto em [1] e em [34], tal condição não é suficiente. Assim, em geral, tal questão é um problema em aberto até o presente momento.

Procesi, em [30], respondeu parcialmente a pergunta acima, considerando essa questão sobre um corpo de característica zero, no sentido de que, para a existência de tal mergulho, uma condição necessária e suficiente é que o anel satisfaça todas as identidades com traço da álgebra de matrizes e, pelo Teorema 2.4.6, é suficiente que satisfaça a identidade de Cayley-Hamilton de grau n. Neste resultado, Procesi fez uso de uma certa *aplicação universal* que pode ser encontrada no artigo [2].

Neste capítulo estudaremos com detalhes os resultados mencionados acima. Aqui iremos estabelecer um resultado mais geral do que o Corolário 2.4.8, no seguinte sentido: Iremos provar que toda álgebra nil de índice limitado n, sobre um corpo de característica zero, é subálgebra da álgebra de matrizes de ordem n, sobre algum anel comutativo.

3.1 Notações e resultados iniciais

Consideremos R um anel e $M_n(R)$ o anel das matrizes de ordem n sobre R. Dado $A \in M_n(R)$, denotaremos, como de costume, por a_{ij} $(\in R)$ a entrada da matriz A que está na i-ésima linha e j-ésima coluna. Além disso, quando k for um subanel de $Z(R)$, veremos R como uma k-álgebra e, diante disso, pode ser conveniente identificar $M_n(R)$ com $M_n(k) \otimes_k R$.

Seja $\eta : R \to S$ um homomorfismo de anéis. Das propriedades de matrizes, podemos obter um homomorfismo entre $M_n(R)$ e $M_n(S)$ induzido por η dado por:

$$\begin{array}{rcl} M_n(\eta)\colon M_n(R) & \to & M_n(S) \\ (r_{ij})_{n\times n} & \mapsto & M_n(\eta)((r_{ij})_{n\times n}) = (\eta(r_{ij}))_{n\times n}. \end{array}$$

Notação 3.1.1 *No decorrer do texto, o homomorfismo acima será sempre denotado por $M_n(\eta)$, onde η será o homomorfismo que o induz.*

Observação 3.1.2 *A fim de deixar os resultados os mais independentes de outras fontes, utilizaremos alguns resultados da teoria de anéis, os quais são comumente vistos em cursos de graduação. Devido a serem resultados básicos, omitiremos as suas demonstrações, mas os enunciaremos para auxiliar na compreensão do trabalho e serão citados no decorrer do texto como parte integrante desta observação juntamente com o algarismo correspondente informado abaixo.*

i) Se R é um anel com unidade e J é um ideal de $M_n(R)$, então existe algum ideal I de R tal que $J = M_n(I)$.

ii) Se R é um anel e I é um ideal de R, então $M_n(R)/M_n(I) \simeq M_n(R/I)$.

iii) Se I é um ideal de um anel R e $S \subseteq I$, então $\langle S\rangle \subseteq I$ (onde $\langle S\rangle$ é o ideal de R gerado por S).

Com o intuito de evitar repetições no decorrer do capítulo, fixemos mais algumas notações: Aqui k será um anel comutativo com unidade e assumiremos que todos os anéis daqui por diante serão k-álgebras, onde $1 \in k$ age como a unidade, e todos os homomorfismos serão k-homomorfismos, a menos que seja dito o contrário.

Sendo $X = \{x_i \mid i > 0\}$ um conjunto de indeterminadas não comutativas sobre k, denotaremos por $k\langle X\rangle = k\langle \ldots, x_i, \ldots\rangle$ o anel livremente gerado sobre k, com k comutando com os x_i's, e por $k^\circ\langle X\rangle$ o subanel de $k\langle X\rangle$ contendo todos os polinômios com termo independente zero.

Usando a notação de matrizes genéricas dada na Seção 1.3.4, podemos considerar $X_i = (\xi^i_{\alpha\beta})$, com $\alpha, \beta = 1, 2, \ldots, n$, as matrizes genéricas de ordem n sobre o anel de polinômios comutativo $\Delta = k[\xi^i_{\alpha\beta} \mid i \leq 1, 1 \leq \alpha, \beta \leq n]$ nas indeterminadas ξ's sobre k. Assim, considerando $\mathcal{X} = \{X_1, X_2, \ldots\}$, podemos ver

$$k^\circ\langle\mathcal{X}\rangle \subseteq k\langle\mathcal{X}\rangle \subseteq M_n(\Delta)$$

onde $k\langle\mathcal{X}\rangle$ é a k-álgebra gerada por 1 e todos os X_i's e $k^\circ\langle\mathcal{X}\rangle$ é a k-álgebra gerada pelos X_i's (sem a unidade). Por fim, pela propriedade universal da k-álgebra livre $k\langle X\rangle$, temos o seguinte resultado:

Proposição 3.1.3 *Existe um homomorfismo canônico entre $k\langle X\rangle$ e $k\langle\mathcal{X}\rangle$.*

Demonstração: O resultado é imediato, basta considerar o homomorfismo canônico que associa cada indeterminada x_i a sua correspondente matriz genérica X_i. ■

Por economia de notação, decidimos exibir o homomorfismo mais adiante. Além disso, a construção do anel $k\langle X\rangle$ segue passos análogos a construção feita na Proposição 1.3.3, e por tal motivo decidimos não construir este tipo de k-álgebra livre. Aqui precisamos ter cuidado apenas em escolher um homomorfismo de k-módulos no lugar de uma transformação linear, e observar que $k\langle X\rangle$ é um módulo livre sobre k, livremente gerado por pelos monômios em X.

3.2 Aplicação $M_n(k)$-universal

Os resultados que se encontram nesta seção independem da característica do corpo, embora iremos aplicá-los em álgebras sobre um corpo de característica zero.

O objetivo desta seção é obter uma ferramenta que nos auxilie na construção de mergulhos em álgebras de matrizes sobre anéis comutativos. Com isso em mente, iremos mostrar que existe uma k-álgebra comutativa S e um homomorfismo $\rho : R \to M_n(S)$, tais que todo homomorfismo σ de R em $M_n(B)$, onde B é um anel comutativo, satisfaz a relação $M_n(\eta)\rho = \sigma$, onde $M_n(\eta)$ será um homomorfismo contruído a seguir. Além disso, tal álgebra comutativa S é unicamente determinada. Em resumo, desejamos provar o seguinte resultado:

Teorema 3.2.1 *Seja R uma k-álgebra. Então existe uma k-álgebra comutativa S e um homomorfismo $\rho : R \to M_n(S)$ tal que:*

1) As entradas $\{[\rho(r)]_{\alpha\beta} \mid r \in R\}$ geram, junto com 1, o anel S;

2) Para cada homomorfismo $\sigma : R \to M_n(B)$, onde B é uma k-álgebra comutativa com unidade, existe um homomorfismo $\eta : S \to B$ de modo que a aplicação induzida $M_n(\eta) : M_n(S) \to M_n(B)$ satisfaça a relação $M_n(\eta)\rho = \sigma$.

Além disso, S é único a menos de isomorfismo, ρ é único a menos de um múltiplo isomorfo e se S, ρ e σ são dados, então η é unicamente determinado.

Notação 3.2.2 *O par (S, ρ) será chamado de aplicação $M_n(k)$-universal para R.*

Observação 3.2.3 *Quando o anel R for unitário e ρ for um homomorfismo unitário, é possível concluir que existe uma k-álgebra comutativa S_u com unidade e um homomorfismo unitário $\rho_u : R \to M_n(S_u)$ que satisfaz o Teorema 3.2.1 quando restrito apenas ao homomorfismo unitário $\sigma_u : R \to M_n(B)$. Tal conclusão é obtida fazendo os devidos ajustes na demonstração do Teorema 3.2.1 que será feita adiante.*

Iremos nos dedicar nesta seção à prova do Teorema 3.2.1 e a algumas consequências interessantes, mas antes disto iremos exibir o par (S, ρ) para a k-álgebra livre $k\langle X\rangle$. Aqui iremos resgatar algumas notações consideradas antes da Seção 3.2.

Seja $X_i = \sum_{\alpha,\beta=1}^{n} \xi^i_{\alpha\beta} E_{\alpha\beta} = (\xi^i_{\alpha\beta})$, com $i \in \mathbb{N}$, uma matriz genérica de $M_n(k)$ sobre k, ou seja, os elementos de $\{\xi^i_{\alpha\beta} \mid 1 \leq \alpha, \beta \leq n \text{ e } i > 0\}$ são indeterminadas comutativas sobre k. Eles são os coeficientes do elemento X_i sobre a k-álgebra de polinômios nas variáveis $\xi^i_{\alpha,\beta}$, denotado por $\Delta = k[\xi]$. Considerando $k\langle\mathcal{X}\rangle$ a álgebra gerada pelos X_j's, é fácil observar que $k\langle\mathcal{X}\rangle \subseteq M_n(\Delta)$, ver notação antes da Proposição 3.1.3. Exibiremos, explicitamente, o homomorfismo canônico pretendido na Proposição 3.1.3, ou seja, considere $\psi\colon k\langle X\rangle \to k\langle\mathcal{X}\rangle$ dado por

$$\psi(x_j) = X_j. \tag{3.1}$$

É claro que o par (Δ, ψ) satisfaz a condição 1) do Teorema 3.2.1, restando verificar o item 2). Tome F uma k-álgebra comutativa qualquer e $\sigma\colon k\langle X\rangle \to M_n(F)$ um homomorfismo dado por $\sigma(x_i) = (f^i_{\alpha\beta})$. Como Δ é a k-álgebra livre na classe das k-álgebras comutativas, temos a existência de um k-homomorfismo $\eta\colon \Delta \to F$ tal que $\eta(\xi^i_{\alpha\beta}) = f^i_{\alpha\beta}$. O k-homomorfismo anterior induz a aplicação $M_n(\eta)\colon M_n(\Delta) \to M_n(F)$ dada por $M_n(\eta)((\xi^i_{\alpha\beta})) = (f^i_{\alpha\beta})$. Note que:

$$M_n(\eta)\psi(x_j) = M_n(\eta)(X_j) = (\eta(\xi^i_{\alpha\beta})) = \sigma(x_j).$$

Em resumo, temos o seguinte resultado:

Proposição 3.2.4 *O par (Δ, ψ) é a $M_n(k)$-aplicação universal para $k\langle X\rangle$.*

Antes de provar a existência do par (S, ρ) para uma álgebra R em geral, iremos estabelecer a sua unicidade. Tal prova é comumente utilizada na literatura.

Proposição 3.2.5 *Sejam (S, ρ) e (S_0, ρ_0) pares satisfazendo as condições 1) e 2) do Teorema 3.2.1. Então existe um isomorfismo $\eta\colon S \to S_0$ tal que $\rho_0 = M_n(\eta)\rho$. Além disso a aplicação η é unicamente determinada quando (S, ρ) e σ são fixados. Em particular, (S, ρ) é unicamente determinado, a menos de isomorfismo descrito no enunciado.*

Demonstração: **Unicidade de (S, ρ):** Seja $\rho\colon R \to M_n(S)$ e $\rho_0\colon R \to M_n(S_0)$. Ao aplicar a condição 2) nestes homomorfismos, segue que existem $\eta : S \to S_0$ e $\eta_0 : S_0 \to S$, tais que $M_n(\eta)\rho = \rho_0$ e $M_n(\eta_0)\rho_0 = \rho$. Daí, substituindo a primeira igualdade na segunda,

$$M_n(\eta_0)M_n(\eta)\rho = \rho. \tag{3.2}$$

Afirmação 1: $M_n(\eta_0)M_n(\eta) = M_n(\eta_0\eta)$.

Com efeito, dada $(a_{ij})_{n\times n} \in M_n(S)$, temos

$$\begin{aligned} M_n(\eta_0)M_n(\eta)((a_{ij})_{n\times n}) &= M_n(\eta_0)((\eta(a_{ij}))_{n\times n}) \\ &= (\eta_0\eta(a_{ij}))_{n\times n} \\ &= M_n(\eta_0\eta)(a_{ij})_{n\times n}. \end{aligned}$$

A afirmação segue da arbitrariedade do elemento em $M_n(S)$ considerado.

Munidos da afirmação e da Igualdade (3.2), segue que, para cada $r \in R$, obtemos $\rho(r) = M_n(\eta_0\eta)\rho(r)$. O que implica em $\rho(r)_{\alpha\beta} = (\eta_0\eta)\rho(r)_{\alpha\beta}$. Portanto, $\eta_0\eta$ é a aplicação identidade nas entradas das matrizes de $\rho(R)$. Como a aplicação $\eta_0\eta$ é também um k-homomorfismo e essas entradas geram S (pela condição 1)), segue que $\eta_0\eta$ é a identidade em S. Fazendo procedimento análogo, obtemos que $\eta\eta_0$ é a identidade sobre S_0. Daí, η e η_0 são isomorfismos. Em particular, temos $\rho_0 = [M_n(\eta_0)]^{-1}\rho$. Concluindo que S é único a menos de isomorfismo e ρ é único a menos de múltiplo por um isomorfismo de S.

Unicidade de η: Se $\sigma : R \to M_n(B)$ é dado e existem $\eta, \eta' : S \to B$ satisfazendo 2), isto é, $M_n(\eta)\rho = M_n(\eta')\rho = \sigma$, então para todo $r \in R$,

$$M_n(\eta)\rho(r) = M_n(\eta')\rho(r).$$

Daí, para toda entrada $\rho(r)_{\alpha\beta}$ temos $\eta[\rho(r)_{\alpha\beta}] = \eta'[\rho(r)_{\alpha\beta}]$ e, como todos os $\rho(r)_{\alpha\beta}$ geram S, temos $\eta = \eta'$. ■

Observação 3.2.6 *Como consequência direta da proposição acima, $M_n(\eta)$ é também unicamente determinado, sempre que (S, ρ) e σ são fixados.*

Agora iremos provar o Teorema 3.2.1 e a fim de auxiliar a compreensão da demonstração, iremos apresentar sua demonstração em dois lemas.

Lema 3.2.7 *Seja R uma k-álgebra. Existe uma k-álgebra comutativa S e um homomorfismo $\rho : R \to M_n(S)$ tal que as entradas $\{[\rho(r)]_{\alpha\beta} \mid r \in R\}$ geram, junto com 1, o anel S.*

Demonstração: Definiremos o homomorfismo ρ e o anel S desejado da seguinte maneira: sendo $\{r_i\}_{i\in L}$ um conjunto de k-geradores de R, consideremos o homomorfismo

$$\begin{aligned} \varphi_0 : k^0\langle X\rangle &\to R \\ x_i &\mapsto \varphi_0(x_i) = r_i \end{aligned}$$

e denotemos por p o seu núcleo (caso R seja unitário e a unidade seja um dos geradores de R, então podemos considerar $k\langle X\rangle$ em vez de $k^0\langle X\rangle$ e a demonstração será análoga). Como, por construção, φ_0 é sobrejetivo, o Teorema Fundamental dos Isomorfismos nos dá um isomorfismo φ entre $k^0\langle X\rangle/p$ e R.

Sendo

$$\begin{aligned} \psi_0 : k^0\langle X\rangle &\to k^0\langle \mathcal{X}\rangle \\ x_i &\mapsto \psi_0(x_i) = X_i, \end{aligned} \tag{3.3}$$

$P = \psi_0(p)$ e como, por construção, ψ_0 é um homomorfismo sobrejetor, segue que P é ideal de $k^0\langle \mathcal{X}\rangle$. Nestas condições, podemos obter um homomorfismo, denotado por ψ, entre $k^0\langle X\rangle/p$ e $k^0\langle \mathcal{X}\rangle/P$.

Usando a notação já comentada no início deste capítulo e considerando $\Delta = k[\xi]$, o anel $k^0\langle \mathcal{X}\rangle$ uma subálgebra de $M_n(\Delta)$ e $\langle P\rangle$ o ideal gerado por P em $M_n(\Delta)$, tem-se, pelo resultado $i)$ da Observação 3.1.2, que existe um ideal I de Δ tal que $\langle P\rangle = M_n(I)$. Como Δ contém a unidade, podemos interpretar que I é o ideal de Δ gerado por todas as entradas das matrizes de $\langle P\rangle$.

Utilizando essa notação, tomemos $S = \dfrac{\Delta}{I}$ e definimos ρ como a seguinte composição:

$$R \xrightarrow{\varphi^{-1}} \frac{k^0\langle X\rangle}{p} \xrightarrow{\psi} \frac{k^0\langle \mathcal{X}\rangle}{P} \xrightarrow{v} \frac{M_n(\Delta)}{\langle P\rangle} \xrightarrow{\mu} M_n(\Delta/I) \tag{3.4}$$

onde μ é o isomorfismo natural dado no resultado $ii)$ da Observação 3.1.2 e a aplicação $v : \dfrac{k^0\langle \mathcal{X}\rangle}{P} \to \dfrac{M_n(\Delta)}{\langle P\rangle}$ é induzida pela inclusão $k^0\langle \mathcal{X}\rangle \subseteq M_n(\Delta)$. Veja que v está bem definida, uma vez que dados $X_i + P = X_j + P$, segue que $X_i - X_j \in P$. Daí, como $P \subseteq \langle P\rangle$, temos $X_i - X_j \in \langle P\rangle$. Logo, $v(X_i) = X_i + \langle P\rangle = X_j + \langle P\rangle = v(X_j)$.

Usando o fato de Δ ser gerado por $\xi^i_{\alpha\beta}$ e 1, segue que $\Delta/I = S$ é gerado por 1 e $\xi^i_{\alpha\beta} + I$, sendo o último as (α, β)-entradas das matrizes $\rho(r_i)$. De fato,

$$\begin{aligned} \varphi^{-1}(r_i) = x_i + p \;&\Rightarrow\; \psi\varphi^{-1}(r_i) = X_i + P \\ &\Rightarrow\; v\psi\varphi^{-1}(r_i) = v(X_i + P) = X_i + \langle P\rangle. \end{aligned}$$

E como $\rho = \mu v\psi\varphi^{-1}$, segue que $\rho(r_i)_{\alpha\beta} = \xi^i_{\alpha\beta} + I$, como desejávamos provar. ■

Neste próximo lema, utilizaremos as notações empregadas na demonstração acima.

Lema 3.2.8 *Sendo válida a condição* 1) *do Teorema 3.2.1, temos que para cada homomorfismo $\sigma : R \to M_n(B)$, com B uma k-álgebra comutativa com unidade, existe um homomorfismo $\eta : S \to B$ tal que, para a aplicação induzida $M_n(\eta) : M_n(S) \to M_n(B)$, a relação $M_n(\eta)\rho = \sigma$ é válida.*

Demonstração: Considere $\sigma : R \to M_n(B)$ um homomorfismo fixado, dado por $\sigma(r_i) = (b^i_{\alpha\beta}) \in M_n(B)$. Novamente, por Δ ser a k-álgebra livre na classe de todas as k-álgebras comutativas, livremente gerada pelo conjunto ξ, podemos considerar a especialização

$$\begin{aligned} \eta_0 : \Delta = k[\xi] \;&\to\; B \\ \xi^i_{\alpha\beta} \;&\mapsto\; b^i_{\alpha\beta}. \end{aligned}$$

Iremos construir η a partir de η_0 da seguinte forma: verificaremos que η_0 aplica I (I ideal de Δ encontrado na demonstração anterior) em zero e, disto, η será a aplicação induzida por $S = \Delta/I$ em B. Para isso, consideremos o diagrama

$$\begin{tikzcd} k^0\langle X\rangle \arrow[r, "\psi_0"] \arrow[d, "\varphi_0"'] & k^0\langle \mathcal{X}\rangle \arrow[d] \\ R \arrow[r, "\sigma"'] & M_n(B) \end{tikzcd} \tag{I}$$

onde a aplicação da segunda coluna é a composição:

$$k^0\langle\mathcal{X}\rangle \to M_n(\Delta) \to M_n(B), \tag{3.5}$$

sendo, nesta sequência de homomorfismos, a primeira aplicação é a inclusão e a segunda $M_n(\eta_0)$. Por abuso de notação, a composição dada em (3.5) será denotada também por $M_n(\eta_0)$.

Note que o Diagrama (I) é comutativo, uma vez que $\sigma\varphi_0(x_i) = \sigma(r_i) = (b^i_{\alpha\beta})$ e

$$M_n(\eta_0)\psi_0(x_i) = M_n(\eta_0)(X_i) = (\eta_0(\xi^i_{\alpha\beta})) = (b^i_{\alpha\beta}).$$

Como $\sigma\varphi_0 = M_n(\eta_0)\psi_0$ vale para os geradores, segue por k-linearidade que vale para todo $k^0\langle X\rangle$. Logo, o diagrama é de fato comutativo. Em particular, dado $f = f(x_1, \dots, x_t) \in k^0\langle X\rangle$, temos que $f \in p = ker\varphi_0$, então

$$0 = \sigma\varphi_0(f) = M_n(\eta_0)\psi_0(f)$$

o que mostra que $P = \psi_0(p) \subseteq kerM_n(\eta_0)$.

Consequentemente, do diagrama anterior, obtemos o diagrama comutativo:

$$\begin{tikzcd} k^0\langle X\rangle/p \arrow[r, "\psi"] \arrow[d, "\varphi"'] & k^0\langle\mathcal{X}\rangle/P \arrow[d] \\ R \arrow[r, "\sigma"'] & M_n(B) \end{tikzcd} \tag{II}$$

Seja $\bar{\eta} : k^0\langle\mathcal{X}\rangle/P \to M_n(B)$ o homomorfismo da segunda coluna do diagrama anterior, o qual é induzido por $M_n(\eta_0)$. Na teoria de anéis, tal aplicação é comumente denotada por $\overline{M_n(\eta_0)}$, porém aqui decidimos denotar por $\bar{\eta}$ para estabelecer um notação mais econômica, mas deixamos claro que não tem nada a ver com aplicação η dada no item 2) do Teorema 3.2.1. Continuando com o Diagrama (II), temos que tal diagrama é de fato comutativo, uma vez que

$$\bar{\eta}(X_i + P) = \bar{\eta}\psi(x_i + p) = \sigma\varphi(x_i + p) = \sigma(r_i).$$

Para obter o estágio final da nossa aplicação ρ consideremos o diagrama:

$$\begin{tikzcd} k^0\langle\mathcal{X}\rangle \arrow[r, "\lambda_0"] \arrow[d, "r"'] & M_n(\Delta) \arrow[d, "M_n(\eta_0)"] \\ k^0\langle\mathcal{X}\rangle/P \arrow[r, "\bar{\eta}"'] & M_n(B) \end{tikzcd} \tag{III}$$

onde λ_0 é a injeção (ou seja, a aplicação induzida pela inclusão) e r é a projeção. Esse diagrama é também comutativo, uma vez que $\bar{\eta}r(x_i) = \bar{\eta}(X_i + P) = \sigma(r_i)$ e

$$M_n(\eta_0)\lambda_0(X_i) = M_n(\eta_0)(X_i) = (\eta_0(\xi^i_{\alpha\beta})) = (b^i_{\alpha\beta}) = \sigma(r_i).$$

Como é válido para os geradores, segue que $M_n(\eta_o)\lambda_0 = \bar{\eta}r$.

Agora, como $r(P) = 0$, então $M_n(\eta_0)\lambda_0(P) = \bar{\eta}r(P) = 0$ e, como $\lambda_0(P) = P$ (por ser uma injeção), segue que $P \subseteq kerM_n(\eta_0)$. Como $kerM_n(\eta_0)$ é um ideal de $M_n(\Delta)$, do resultado *iii)* da Observação 3.1.2, $\langle P\rangle \subseteq kerM_n(\eta_0)$. Consequentemente, $M_n(\eta_0)$ induz um homomorfismo $\tilde{\eta} : M_n(\Delta)/\langle P\rangle \to M_n(B)$ e obtemos o seguinte diagrama comutativo:

$$\begin{tikzcd} k^0\langle\mathcal{X}\rangle/P \arrow[rr, "v"] \arrow[dr, "\bar{\eta}"'] & & M_n(\Delta)/\langle P\rangle \arrow[dl, "\tilde{\eta}"] \\ & M_n(B) & \end{tikzcd} \tag{IV}$$

onde v é uma aplicação induzida pela injeção $\lambda_0 : k^0\langle\mathcal{X}\rangle \to M_n(\Delta)$. Veja que v está bem definida já que $v(P) \subseteq \langle P\rangle$. O diagrama anterior é comutativo, pois

$$\tilde{\eta}v(X_i + P) = \tilde{\eta}(X_i + \langle P\rangle) = M_n(\eta_0)(X_i) = (\eta_0(\xi^i_{\alpha\beta})) = (k^i_{\alpha\beta}) = \sigma(r_i)$$

e $\bar{\eta}(X_i + P) = \sigma(r_i)$ como mostrado acima.

Outra consequência da existência de $\tilde{\eta}$ é o fato de que se $\langle P\rangle = M_n(I)$, então $\eta_0(I) = 0$. De fato, como foi mostrado $\langle P\rangle \subseteq kerM_n(\eta_0)$, assim segue que $M_n(\eta_0)(\langle P\rangle) = M_n(\eta_0(I)) = 0$. Portanto, $\eta_0 : \Delta \to B$ induz um homomorfismo $\eta : \Delta/I \to B$ e, daí, o homomorfismo $M_n(\eta) : M_n(\Delta/I) \to M_n(B)$. Assim, temos o diagrama comutativo:

$$\begin{tikzcd} M_n(\Delta)/\langle P\rangle \arrow[rr, "\mu"] \arrow[dr, "\tilde{\eta}"'] & & M_n(\Delta/I) \arrow[dl, "M_n(\eta)"] \\ & M_n(B) & \end{tikzcd} \tag{V}$$

onde μ é o isomorfismo $M_n(\Delta)/\langle P\rangle = M_n(\Delta)/M_n(I) \simeq M_n(\Delta/I)$. Esse diagrama é também comutativo, já que $\tilde{\eta}(X_i + P) = M_n(\eta_0)(X_i) = \sigma(r_i)$ como visto já antes e, $M_n(\eta)\mu(X_i + P) = M_n(\eta)((\xi^i_{\alpha\beta} + I)) = (\eta(\xi^i_{\alpha\beta} + I)) = (\eta_0(\xi^i_{\alpha\beta})) = \sigma(r_i)$.

Dos Diagramas (II), (IV) e (V), e por φ ser um homomorfismo, utilizando a notação compatível com o lema anterior, podemos considerar

$$\rho = \mu v\psi\varphi^{-1}, \tag{3.6}$$

obtemos assim:

$$M_n(\eta)\rho = (M_n(\eta)\mu)v\psi\varphi^{-1} = (\tilde{\eta}v)\psi\varphi^{-1} = (\bar{\eta}\psi)\varphi^{-1} = \sigma\varphi\varphi^{-1} = \sigma.$$

E, deste modo, temos o desejado. ■

Daí, pelos dois lemas demonstrados, temos o Teorema 3.2.1, já enunciado no início desta subseção.

Munidos destes resultados e sendo $S = \Delta/I$, se R é finitamente gerado, então podemos escolher o conjunto $\{x_i\}$ sendo finito e, portanto, Δ é um anel polinomial, sobre k, com um número finito de indeterminadas comutativas. Daí, S é um anel finitamente gerado. Em resumo podemos concluir que:

Corolário 3.2.9 *Assumindo as condições do Teorema 3.2.1, se R é finitamente gerado, como k-álgebra então $S = \Delta/I$ também é. Assim, k sendo noetheriano, implica que S também será noetheriano.*

A seguir listaremos outras consequências que seguem do Teorema 3.2.1.

Corolário 3.2.10 *O anel R pode ser mergulhado no anel das matrizes $M_n(B)$ sobre algum anel comutativo B se, e somente se, o morfismo $\rho : R \to M_n(S)$ do Teorema 3.2.1 é um monomorfismo.*

Demonstração: Se ρ é um monomorfismo, então claramente R pode ser mergulhado no anel de matrizes sobre algum anel comutativo, neste caso, em $M_n(S)$. Reciprocamente, consideremos a existência de um mergulho $\sigma : R \to M_n(B)$, com B um anel comutativo. Pelo Teorema 3.2.1, temos $\sigma = M_n(\eta)\rho$. Segue que ρ é um monomorfismo, pois do contrário existiria $x, y \in R$, com $x \neq y$, tais que $\rho(x) = \rho(y)$, implicando que

$$M_n(\eta)\rho(x) = M_n(\eta)\rho(y) \Rightarrow \sigma(x) = \sigma(y),$$

o que é uma contradição, já que σ é um mergulho. ■

Corolário 3.2.11 *Uma condição necessária e suficiente para valer o Corolário 3.2.10, é que exista um epimorfismo g de $k^0\langle\mathcal{X}\rangle$ em R, e que se $P = kerg$, então a igualdade $\langle P\rangle \cap k^0\langle\mathcal{X}\rangle = P$ é válida. Se isso vale para tal representação de R, então vale para todos.*

Demonstração: Por aplicação definida em (3.6), temos $\rho = \mu v\psi\varphi^{-1}$, onde μ e φ^{-1} são isomorfismos e ψ é um epimorfismo. Segue que ρ é um monomorfismo se, e somente se, ψ é um isomorfismo e v é um monomorfismo. O fato de ψ ser um isomorfismo significa que

$$\frac{k^0\langle \mathcal{X} \rangle}{P} \simeq \frac{k^0\langle X \rangle}{p} \simeq R. \tag{3.7}$$

Considere $g = \psi r$, onde ψ denotará, por economia de notação, a composição dada em (3.7) e r a projeção de $k^0\langle \mathcal{X} \rangle$ em $k^0\langle \mathcal{X} \rangle/P$. Temos o seguinte diagrama:

$$\begin{tikzcd}
 & k^0\langle \mathcal{X} \rangle/P \arrow[d, "\psi"'] \arrow[dr] & \\
k^0\langle \mathcal{X} \rangle \arrow[ur, "r"] \arrow[r, "g"'] & R \arrow[r, "v"'] & M_n(\Delta)/\langle P \rangle
\end{tikzcd}.$$

Tendo como hipótese que v é um monomorfismo, queremos mostrar a igualdade $\langle P \rangle \cap k^0\langle \mathcal{X} \rangle = P$. É claro que $P \subseteq \langle P \rangle \cap k^0\langle \mathcal{X} \rangle$. Devemos agora nos dedicar a inclusão contrária. Tomando $y \in \langle P \rangle \cap k^0\langle \mathcal{X} \rangle$, temos $v(g(y)) = v\psi r(y) = \bar{0}$, pois $y \in \langle P \rangle$. Assim, como v é monomorfismo, segue que $g(y) = \bar{0}$ em $k^0\langle \mathcal{X} \rangle/P$. Deste modo, $y \in P$. Com isso, segue a primeira parte.

Reciprocamente, suponha que existe um epimorfismo g de $k^0\langle \mathcal{X} \rangle$ em R, de modo que $P = kerg$ e $\langle P \rangle \cap k^0\langle \mathcal{X} \rangle = P$. Podemos identificar R como sendo $k^0\langle X \rangle/I$, para algum ideal I de $k^0\langle X \rangle$, e do Teorema Fundamental dos Isomorfismos temos que $k^0\langle \mathcal{X} \rangle/P \simeq k^0\langle X \rangle/I$. Como P é o núcleo de g e $\langle P \rangle \cap k^0\langle \mathcal{X} \rangle = P$, segue que podemos mergulhar a álgebra R em $M_n(S)$, onde $S = \Delta/J$ para algum ideal J de Δ tal que $M_n(J) = \langle P \rangle$.

Além disso, se a condição do nosso teorema vale para uma representação de R como quociente $k^0\langle X \rangle$, segue da unicidade de (S, ρ), a $M_n(k)$-aplicação universal de R, e da equivalência do Corolário 3.2.10 que esse resultado continua válido para qualquer outra representação de R. ■

Observação 3.2.12 *Os Corolários 3.2.10 e 3.2.11 também são válidos para mergulhos unitários, sendo tal prova baseada nos mesmos argumentos.*

Corolário 3.2.13 *Toda k-álgebra R contém um único ideal Q tal que R/Q pode ser mergulhado em um anel de matrizes $M_n(B)$, B anel comutativo. Além disso, se R/Q_0 pode ser mergulhado em $M_n(B)$, então $Q \subseteq Q_0$.*

Demonstração: Seja $\rho : R \to M_n(S)$ e seja $Q = ker\rho$. Então ρ induz um monomorfismo de R/Q em $M_n(S)$. Caso exista um outro ideal Q_0 de R, tal que R/Q_0 possa ser mergulhado em um anel de matrizes sobre um anel comutativo, digamos $M_n(B)$, pode-se construir um homomorfismo σ: $R \to M_n(B)$ tal que $ker\sigma = Q_0$. Do Teorema 3.2.1 temos que $M_n(\eta)\rho = \sigma$. Deste modo $ker\sigma \supseteq ker\rho = Q$. Daí, obtemos o desejado.

■

A partir de agora, consideraremos k como sendo um corpo de característica zero e nos concentraremos em definir uma representação do grupo de automorfismos de $M_n(k)$. Ademais, afim de não haver dúvida de notação, iremos trocar a notação de k por K.

Recordando o fato de que $M_n(S) \simeq M_n(K) \otimes S$, iremos analisar uma estrutura extra associada à ρ, utilizando produto tensorial. Para isso, seja G o grupo dos automorfismos de $M_n(K)$, que, pelo Teorema de Skolem-Noether (ver Teorema 1.1.33), é o grupo geral linear de ordem n denotado por $G = GL_n(K)$. Para cada $g \in G$, consideremos a aplicação

$$\begin{array}{rcl} \psi_g : M_n(K) \otimes S & \to & M_n(K) \otimes S \\ a \otimes s & \mapsto & \psi_g(a \otimes s) = (g \cdot a) \otimes s. \end{array}$$

Por outro lado, por toda teoria já desenvolvida até o momento, sabemos que existe uma aplicação estendendo η, dada por (agora em linguagem de tensores)

$$M_n(\eta^g)\left(\sum_{i=1}^{n} a_i \otimes s_i\right) = \sum_{i=1}^{n} a_i \otimes \eta^g(s_i),$$

de modo que $\psi_g \cdot \rho = M_n(\eta^g) \cdot \rho$. É importante notarmos que como ψ_g e $M_n(\eta^g)$ fixam os elementos de S e $M_n(K)$, respectivamente. É fácil observar que tais aplicações comutam entre si. Ademais, para todo $g, h \in G$, temos:

$$\begin{aligned} M_n(\eta^{gh}) \cdot \rho &= \psi_{gh} \cdot \rho = \psi_g \cdot \psi_h \cdot \rho \\ &= \psi_g \cdot M_n(\eta^h) \cdot \rho \\ &= M_n(\eta^h)\psi_g \cdot \rho \\ &= M_n(\eta^h) \cdot M_n(\eta^g) \cdot \rho \\ &= M_n(\eta^h \eta^g) \cdot \rho. \end{aligned}$$

Da unicidade do Teorema 3.2.1, $\eta^{gh} = \eta^h \eta^g$.

Portanto, dos comentários feitos acima e definindo $\zeta_g = \psi_g \circ (M_n(\eta^g))^{-1}$, temos a seguinte proposição:

Proposição 3.2.14 *G age, via a representação ζ_g, como um grupo de automorfismos de $M_n(S)$ e $\rho(R)$ está contido no anel dos invariantes.*

Corolário 3.2.15 *Seja (S, ρ) a $M_n(K)$-aplicação universal de alguma álgebra R. Para todo ideal J de S, a aplicação projeção $\pi_J : M_n(S) \to M_n(S/J)$ é G-concomitante.*

Demonstração: Usaremos a notação com tensorial em nossa demonstração. Neste caso, consideraremos $M_n(S) \simeq M_n(K) \otimes S$ e $M_n(S/J) \simeq M_n(K) \otimes (S/J)$. Seja I um ideal de R tal que $(\rho(I)) = M_n(K) \otimes J$. Por abuso de notação, usaremos o mesmo símbolo ψ_g para denotar a aplicação

$$\psi_g : M_n(K) \otimes (S/J) \to M_n(K) \otimes (S/J)$$

dada por $\psi_g(a \otimes \bar{s}) = (g \cdot a) \otimes \bar{s}$, para todo $g \in G$. Para demonstrar que a aplicação $\pi_{\rho(I)}$ é G-concomitante é suficiente provar que $\pi_{\rho(I)} \psi_g M_n(\eta^g)^{-1} = \psi_g M_n(\bar{\eta}^g)^{-1} \pi_{\rho(I)}$, onde $\bar{\eta}^g = p_J \circ \eta^g$. Aqui p_J é a aplicação projeção de S em S/J. Primeiramente, considere $\{r_i\}_{i>0}$ um conjunto gerador de R e defina $\pi_{\rho(I)} : M_n(K) \otimes S \to M_n(K) \otimes (S/J)$ dado por $\pi_{\rho(I)}(\rho(r_i)) = \sum_{\alpha,\beta=1}^{n} E_{\alpha\beta} \otimes (s^i_{\alpha\beta} + J)$, aqui $s^i_{\alpha\beta} = \rho(r_i)_{\alpha\beta}$. Por $I \subseteq ker\pi_{\rho(I)}\rho$, definamos $\rho' : R/I \to M_n(K) \otimes (S/J)$, onde $\rho'(r_i + I) = \sum_i a_j \otimes (s^i_{\alpha\beta} + J)$. Observemos que o diagrama

$$\begin{tikzcd}
M_n(K) \otimes S \arrow[r, "\psi_g"] & M_n(K) \otimes S \\
R \arrow[u, "\rho"] \arrow[r, "\rho"] \arrow[d, "\pi_I"'] & M_n(K) \otimes S \arrow[u, "M_n(\eta^g)"'] \arrow[d, "\pi_{\rho(I)}"] \\
R/I \arrow[r, "\rho'"] \arrow[d, "\rho'"'] & M_n(K) \otimes (S/J) \arrow[d, "M_n(\bar{\eta}^g)"] \\
M_n(K) \otimes (S/J) \arrow[r, "\psi_g"] & M_n(K) \otimes (S/J)
\end{tikzcd}$$

é comutativo. Daí,

$$\begin{aligned}
\pi_{\rho(I)}\psi_g M_n(\eta^g)^{-1}\rho &= \pi_{\rho(I)}M_n(\eta^g)^{-1}\psi_g\rho \\
&= \pi_{\rho(I)}\rho \\
&= \rho'\pi_I \\
&= (M_n(\bar{\eta}^g))^{-1}\psi_g\rho'\pi_I \\
&= (M_n(\bar{\eta}^g))^{-1}\psi_g\pi_{\rho(I)}\rho \\
&= \psi_g(M_n(\bar{\eta}^g))^{-1}\pi_{\rho(I)}\rho.
\end{aligned}$$

O resultado segue aplicando a Proposição 3.2.5. ■

3.3 Aplicação da Identidade de Cayley-Hamilton

Neste capítulo, até o presente momento, estudamos ferramentas para que um dado anel fosse mergulhado em uma anel de matrizes. Diante de tudo isso, nosso objetivo agora é estabelecer condições para que possamos mergulhar um anel R como subanel do anel $M_n(A)$ das matrizes sobre um anel comutativo A. Tal estudo será realizado tendo por base o artigo "A Formal Inverse to the Cayley-Hamilton Theorem" de C. Procesi ([30]).

Consideremos, nesta seção, K um corpo de característica zero. Além disso, consideremos a categoria das álgebras com traço que satisfaz a Identidade de Cayley-Hamilton de grau n. Desejamos provar o seguinte resultado:

Teorema 3.3.1 *Uma álgebra com traço pode ser mergulhada em $M_n(A)$, sendo A uma álgebra comutativa, se, e somente se, satisfaz a identidade de Cayley-Hamilton de grau n.*

Como já sabemos, dada uma álgebra R existe uma $M_n(K)$-aplicação universal de R dada por $\rho : R \to M_n(S)$, com S anel comutativo, onde o par (S, ρ) satisfaz as condições do Teorema 3.2.1. Além disso, em preparação para a demonstração do Teorema 3.3.1, faremos alguns comentários que serão importantes, como também demonstraremos alguns resultados que serão utilizados na demonstração.

Dada $a \in M_n(K)$, podemos definir seu polinômio característico pela fórmula $\chi_a^{(n)}(t) = \det(a - tI)$. Pelo Corolário 1.4.3, o polinômio característico pode ser calculado usando os elementos $tr(a^i)$, $i = 1, 2, \ldots, n$, e também segue que $\chi_a(a) = 0$. Por exemplo, como já comentando no capítulo anterior, quando $n = 2$ temos

$$\chi_a^{(2)}(t) = t^2 - tr(a)t + \frac{1}{2}(tr(a)^2 - tr(a^2)).$$

Definição 3.3.2 *Uma álgebra A com traço $\tau\colon A \to A$ é uma álgebra de* **Cayley-Hamilton de grau** *n se as seguintes propriedades são satisfeitas:*

(i) $\tau(1) = n$;

(ii) Para todo $a \in A$ temos que $\chi_a^{(n)}(a) = 0$ em A.

Denotaremos tal conjunto por $alg@_n$.

A partir de agora veremos as álgebras com traço como uma categoria e seus morfismos serão os homomorfismos de álgebras que preservam o traço. O anel $M_n(A)$ de matrizes sobre um anel comutativo é considerado com seu traço natural, aquele que é definido como a soma dos elementos de sua diagonal principal. Assim, para o problema do mergulho teremos uma nova restrição: o mergulho deve preservar o traço.

Munidos dos comentários acima, provaremos uma versão mais geral do Teorema 3.3.1. Mais precisamente, provaremos o seguinte resultado:

Teorema 3.3.3 *Seja (S, ρ) o par da $M_n(K)$-aplicação universal de uma álgebra com traço R. Se R satisfaz todas as identidades da álgebra $M_n(K)$, então $\rho : R \to M_n(S)^G$ é um isomorfismo.*

Observação 3.3.4 *O resultado mais importante desta seção será obtido como consequência do teorema anterior.*

Observação 3.3.5 *Note que no Teorema 3.3.3 nós não temos apenas uma solução para o problema do mergulho, mas também temos explicitamente quem será o anel comutativo e qual é o subanel das matrizes sobre esse anel que é isomorfa à álgebra R.*

Na Proposição 3.2.4), observamos que o par (S, ρ) é dado da seguinte forma: S é um anel de polinômios nas variáveis ξ, denotado por Δ, e $\rho(x_i)$ é a matriz genérica cujas as entradas (α, β) são as variáveis $\xi_{\alpha\beta}^{(i)}$. Um caso importante a considerar na construção realizada no final da seção anterior (mais precisamente, antes da Proposição 3.2.14) é quando $R = K\langle X\rangle$ é a álgebra livre, livremente gerada pelo conjunto enumerável $X = \{x_1, x_2, \ldots\}$. Com o intuito de interpretar a ação do grupo G, dada na Proposição 3.2.14, de modo diferente, recordaremos a noção de matrizes concomitantes dada na Seção 2.2. Usando essa notação identifiquemos $M_n(\Delta)$ com o anel das aplicações polinomiais $f\colon M_n(C)^\infty \to M_n(C)$ definido sobre uma álgebra comutativa C qualquer, onde $M_n(C)^\infty$ é o espaço de sequências quase todas nulas $(A_1, \ldots, A_n, \ldots)$ de elementos de $M_n(C)$. Além disso, denotaremos por X_i as projeções concomitantes $(A_1, A_2, \ldots) \mapsto A_i$. Na seção antes mencionada, temos que a ação de grupo é dada de maneira natural $f^g((x_i)_{i\in I}) = g \cdot f((g^{-1} \cdot x_i)_{i\in I})$, onde $f = f^g$ significa que f é uma aplicação concomitante. Diante disso, denotando por T a subálgebra de $M_n(\Delta)$ gerada pelas aplicações concomitantes, isto é, $T = (M_n(\Delta))^G$, obtemos que $X_i \in T$, para todo $i \in I$.

O principal fato sobre T é o primeiro teorema fundamental, já provado no Capítulo 2 (ver Teorema 2.1.9), e o seguinte resultado:

Teorema 3.3.6 *A álgebra T é a álgebra livre na variedade das álgebras com traço satisfazendo todas as identidades com traço da álgebra $M_n(K)$.*

Demonstração: Devemos mostrar que $T \simeq G\langle X\rangle / T_{Tr}(M_n(K))$, onde $G\langle X\rangle$ é a álgebra livre na variedade das álgebras com traço. Inicialmente, mostremos a seguinte afirmação:

Afirmação: $T_{Tr}(M_n(\Delta)) = T_{Tr}(M_n(K))$.

É claro que $T_{Tr}(M_n(\Delta)) \subseteq T_{Tr}(M_n(K))$. Para mostrarmos a inclusão oposta, tomemos $f \in T_{Tr}(M_n(K))$, e como K tem característica zero, podemos supor que $f = f(x_1, \ldots, x_n)$ é multilinear. Daí,

$$f(p_1, \ldots, p_n)(a_1, a_2, \ldots) = f(p_1(a_1, a_2, \ldots), \ldots, p_n(a_1, a_2, \ldots)) = 0,$$

para toda substituição por elementos $(p_1, \ldots, p_n)$ de $M_n(\Delta)$ e quaisquer elementos a_j em $M_n(K)$, para todo j. Logo, $f \in T_{Tr}(M_n(\Delta))$.

Munidos da afirmação acima, se considerarmos o epimorfismo com traço φ de $G\langle X\rangle$ em T dado por $\varphi(x_i) = X_i$, e lembrando que T é uma subálgebra de $M_n(\Delta)$, temos que $T_{Tr}(M_n(K)) = T_{Tr}(M_n(\Delta)) \subseteq ker\varphi$.

Por outro lado, seja $f \in ker\varphi$. Para quaisquer projeções concomitantes $X_1, \ldots, X_n$ em $M_n(K)$, temos que para toda n-upla $(a_1, \ldots, a_n)$ de elementos em $M_n(K)$ vale

$$0 = (f(X_1, \ldots, X_n))(a_1, \ldots, a_n) = f(a_1, \ldots, a_n).$$

Assim, obtemos que f é uma identidade com traço para $M_n(K)$ e consequentemente $ker\varphi = T_{Tr}(M_n(K))$. Ademais, concluímos pelo Teorema dos Isomorfismos que $T \simeq G\langle X\rangle / T_{Tr}(M_n(K))$. ■

Observação 3.3.7 *Lembramos que o T-ideal com traço da álgebra de matrizes é gerado apenas pela identidade de Cayley-Hamilton, ver Teorema 2.4.6.*

Utilizaremos na demonstração o **operador de Reynold**, denotado aqui por r, o qual é a projeção canônica de B para B^G. Este operador é uma importante ferramenta no estudo de G-módulos racionais, além de ser um funtor para tal categoria (isto é, é um homomorfismo entre categorias).

Usando o fato de toda representação racional sobre $G = GL_n(K)$ ser semissimples (ver Teorema 1.6.16) para garantir a boa definição do operador. Dados dois G-módulos racionais M, N e uma G-aplicação $f : M \to N$, temos o diagrama comutativo:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "r"] & N \arrow[d, "r"] \\ M^G \arrow[r, "f|_{M^G}"] & N^G \end{tikzcd}$$

Em particular, para uma álgebra com traço B (que é um G-módulo racional) valem as seguintes identidades:

(i) Se $a \in B^G$ e $b \in B$, então $r(ab) = ar(b)$ e $r(ba) = r(b)a$;

(ii) $r(tr(a)) = tr(r(a))$.

Estamos preparados para a demonstração do Teorema 3.3.3.

Demonstração: Como por hipótese R satisfaz todas as identidades com traço de $M_n(K)$, segue do Teorema 3.3.6 que podemos identificar R por T/I, onde I é algum ideal com traço de T. Além disso, considerando $B = M_n(\Delta)$, temos $T \subseteq B$, uma vez que $T = B^G$ subálgebra de B.

Assumiremos, por razões técnicas, que T tem infinitas indeterminadas, mas isso não é uma restrição, e consideremos o ideal $\langle I\rangle$ sendo o ideal gerado por I, como conjunto, de B. Pelo item i) da Observação 3.1.2, existe J um ideal G-invariante de Δ tal que $\langle I\rangle = M_n(J)$ (onde J é visto como um conjunto de matrizes escalares com entradas em J).

A aplicação induzida $R = T/I \to B/\langle I\rangle = M_n(\Delta/J)$, a qual será denotada por ψ_R, é a aplicação do par da $M_n(K)$-aplicação universal de R (veja sequência de homomorfismos em 3.4).

O Corolário 3.2.15 implica que a projeção $p_J : M_n(\Delta) \to M_n(\Delta/J)$ é uma aplicação G-concomitante. Daí, temos que p_J leva invariantes de $M_n(\Delta)$ em invariantes de $M_n(\Delta/J)$, isto é, $T \to (M_n(\Delta/J))^G$ é um epimorfismo (lembre que $M_n(\Delta)$ e $M_n(\Delta/J)$ são G-módulos racionais). Mas $\langle I\rangle$ é o núcleo de p_J, então temos $\psi_R(R) = (M_n(\Delta/J))^G$. Então nós precisamos apenas mostrar que ψ_R é injetivo, isto é, $\langle I\rangle \cap T = I$ (ver Corolário 3.2.11). Como I é um ideal, segue que $I \subseteq \langle I\rangle \cap T$. Para provar a inclusão contrária, utilizaremos o operador de Reynold.

Seja $a = \sum a_i u_i b_i \in \langle I\rangle \cap T, u_i \in I, a_i, b_i \in B$. Sendo x uma variável algébricamente independente com respeito as variáveis das parcelas de a, temos

$$tr(ax) = tr((\sum a_i u_i b_i)x) = tr(\sum b_i x a_i u_i).$$

Aplicando o operador de Reynold obtemos,

$$tr(ax) = tr(\sum r(b_i x a_i)u_i).$$

Agora, para cada i, $r(b_i x a_i)$ é uma invariante e linear em x, então pelo Teorema 2.1.9, temos

$$r(b_i x a_i) = \sum_j s_{ij} x t_{ij} + \sum_k tr(m_{ik}x)n_{ik}$$

com $s_{ij}, t_{ij}, m_{ik}, n_{ik} \in T$. Assim,

$$\begin{aligned} tr(ax) &= tr\big(\sum_{ij}\big(\sum_j s_{ij} x t_{ij} + \sum_k tr(m_{ik}x)n_{ik}\big)u_i\big) \\ &= tr(\sum_{ij} t_{ij} u_i s_{ij} x + \sum_{ik} tr(n_{ik}u_i)m_{ik}x) \\ &= tr((\sum_{ij} t_{ij} u_i s_{ij} + \sum_{ik} tr(n_{ik}u_i)m_{ik})x), \end{aligned}$$

donde, pela não degeneralidade do traço,

$$a = \sum t_{ij} u_i s_{ij} + \sum tr(n_{ik}u_i)m_{ik}.$$

Como I é fechado sobre a operação traço, segue que $a \in I$. Isto completa a demonstração do teorema. ∎

Podemos reescrever o enunciado do Teorema 3.3.3 da seguinte maneira:

Teorema 3.3.8 *Se R é uma álgebra em $alg@_n$, então existe uma álgebra comutativa C, tal que R pode ser mergulhada em $M_n(C)$, como K-álgebra. Além disso, se (S,ρ) é a aplicação $M_n(K)$-universal para R, então $R \overset{\rho}{\simeq} (M_n(S))^G$, onde $G = GL_n(K)$.*

A seguir demonstraremos o resultado que desejávamos, o qual motivou este capítulo. Tal resultado é a resposta da pergunta inicial sobre a classe das álgebras nil de índice limitado. Mais precisamente,

Corolário 3.3.9 *Se R é uma F-álgebra na qual $r^n = 0$, para todo $r \in R$ e um $n \in \mathbb{N}$ fixado, então R pode ser mergulhada nas matrizes de ordem n sobre um anel comutativo.*

Demonstração: Considerando R como uma álgebra com traço, onde $tr(r) = 0$, para todo $r \in R$. Segue que a equação $r^n = 0$ é agora a n-ésima identidade de Cayley-Hamilton. Assim, aplicando o Teorema 3.3.3, temos o desejado. ∎

O nosso próximo objetivo, e último, é mostrar que o ideal das identidades com traço para $(M_n(K), tr)$ satisfaz um análogo a propriedade de Specht para álgebras com traço. O problema clássico foi proposto por Specht [38] em 1950 e provado por Kemer [26] em 1987, no caso associativo. Mais precisamente, iremos provar que todo T-ideal com traço contendo $T_{Tr}(M_n(K), tr)$ admite uma base finita, como T-ideal com traço. Com esse objetivo em mente iremos considerar alguns comentários adicionais para demonstrar esse resultado.

Mas antes de prosseguir é importante notar a importância de tal propriedade ser satisfeita. Tendo a base finita, a mesma é, em particular, finitamente gerada, logo dada uma álgebra A que possa ser mergulhada na álgebra das matrizes, como esta última satisfaz a propriedade de Specht, segue que A tem base para suas identidades finitamente gerada também.

Definição 3.3.10 *Um polinômio em $G\langle X\rangle$ é dito do tipo-Capelli de ordem k se ele é linear e alternante em k variáveis.*

O conjunto dos polinômios do tipo-Capelli de ordem k será denotado por C_k. Além disso, é claro que $f \in C_k$ se anula sempre num conjunto de variáveis alternates quando é substituído por elementos linearmente dependente. Portanto, se (A,τ) é uma álgebra com traço de dimensão n, então $C_{n+1} \subseteq T_{Tr}(A,\tau)$.

Lema 3.3.11 *Sejam I e J dois T_{Tr}-ideais em $G\langle X\rangle$. Então I e J são iguais, módulo os polinômios do tipo-Capelli de ordem $(k+1)$ se, e somente se, $I^{(k)} = J^{(k)}$, onde $I^{(k)} = I \cap G\langle x_1,\ldots,x_k\rangle$ e $J^{(k)} = J \cap G\langle x_1,\ldots,x_k\rangle$.*

Demonstração: A prova é análoga à [33, Proposição 37.1, pág. 176] com pequenas modificações. ■

Estamos prontos para provar o nosso teorema. Achamos importante mencionar que tal resultado já era estabelecido por Razmyslov em [32, Teorema 4] desde 1974, porém decidimos fazer um adaptação do resultado apresentado recentemente por Fidelis, Diniz e Koshlukov em [15].

Teorema 3.3.12 *Sobre um corpo de característica zero, o T_{Tr}-ideal das identidades com traço para $M_n(K)$ satisfaz a propriedade de Specht.*

Demonstração: Como $T_{Tr}(M_n(K))$ é gerado pela identidade de Cayley-Hamilton de grau n, como T_{Tr}-ideal, é suficiente provar que, em $G\langle X\rangle$, cada cadeia acedente de T_{Tr}-ideais que contém $T_{Tr}(M_n(K))$ se estabiliza. Seja

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_k \subseteq \ldots \tag{3.8}$$

uma cadeia de T_{Tr}-ideais onde $I_0 = T_{Tr}(M_n(K))$.

Os comentários anteriores informa que a Cadeia (3.8) se estabiliza se, e somente se, a cadeia

$$I_0^{(n^2)} \subseteq I_1^{(n^2)} \subseteq \ldots \subseteq I_k^{(n^2)} \subseteq \ldots \tag{3.9}$$

onde $I_i^{(n^2)} = I_i \cap G\langle x_1, \ldots, x_{n^2}\rangle$, também se estabiliza. Considere a base de matrizes unitárias em matrizes e denote por $X_r = \sum_{i,j=1}^{n} \xi_{ij}^r E_{ij}$ a matriz genérica sobre K. Os elementos $\{\xi_{ij}^r \mid 1 \leq i, j \leq n, r > 0\}$ são variáveis comutativas independentes sobre K. Seja Δ_{n^2} o anel de polinômios sobre essas variáveis. Denotemos, como de costume, por $K_{Tr}\langle \mathcal{X}\rangle$ a subálgebra com traço de $M_n(K) \otimes_K \Delta_{n^2}$ gerada pelas matrizes genéricas X_r, $r = 1, \ldots, n^2$ sobre K, com o traço herdado pela soma dos elementos de sua diagonal principal. Além disso, defina o homomorfismo

$$\psi \colon G\langle x_1, \ldots, x_{n^2}\rangle \to K_{Tr}\langle \mathcal{X}\rangle$$

dado por $\psi(x_r) = X_r$, $r = 1, \ldots, n^2$ (ver Lema 3.2.4). Denote $P_i^{(n^2)} = \psi(I_i^{(n^2)})$, para $i \geq 0$. Então $P_i^{(n^2)}$ é um ideal com traço de $K_{Tr}\langle \mathcal{X}\rangle$. Como $ker\psi = I_0^{(n^2)}$, concluímos que a Cadeia (3.9) se estabiliza se, e somente se, a cadeia

$$P_0^{(n^2)} \subseteq P_1^{(n^2)} \subseteq \ldots \subseteq P_k^{(n^2)} \subseteq \ldots \tag{3.10}$$

também se estabiliza. Seja $(P_i^{(n^2)})$ o ideal em $M_n(K)\otimes\Delta_{n^2}$ gerado pelo conjunto $P_i^{(n^2)}$. A Observação 3.1.2, item (ii), implica que $(P_i^{(n^2)}) = M_n(K)\otimes_K J_i^{n^2}$ para algum ideal $J_i^{n^2}$ em Δ_{n^2}. Assim, obtemos a cadeia ascendente

$$J_0^{n^2} \subseteq J_1^{n^2} \subseteq \ldots \subseteq J_k^{n^2} \subseteq \ldots$$

em Δ_{n^2}. Note que o anel Δ_{n+1} é noetheriano, portanto existe n_0 tal que $J_i^{n^2} \subseteq J_{n_0}^{n^2}$ para todo $i \geq n_0$. Isto implica que $(P_i^{(n^2)}) = (P_{n_0}^{(n^2)})$, sempre que $i \geq n_0$. Segue da prova do Teorema 3.3.3, com $T = K_{Tr}\langle\mathcal{X}\rangle$, que $(I)\cap\mathcal{T} = I$, para todo ideal com traço I de $\mathcal{T}$. Em particular, $P_i^{(n^2)} = P_{n_0}^{(n^2)}$. Assim a Cadeia (3.10), e consequentemente a Cadeia (3.8), se estabiliza. ■

Terminamos esta seção enfatizando a importância do resultado anterior. A propriedade de Specht para álgebras com traço é uma maneira rápida de verificar se uma dada álgebra com traço possui ideal de suas identidades com traço finitamente gerado. Mais precisamente se tal álgebra satisfaz a identidade de Cayley-Hamilton então podemos garantir que o ideal de suas identidades com traço tem base finita, como T_{Tr}-ideal. É claro que não podemos afirmar nada se tal álgebra não satisfaz a dita identidade.

Bibliografia

[1] Amitsur, S.A. **A noncommutative Hilbert basis theorem and subrings of matrices.** Trans. Amer. Math. Soc. **149 (1)** (1970), 133 - 142.

[2] Amitsur, S. A. **Embeddings in matrix rings.** Pacific J. Math. 36 (1971), 21 - 29.

[3] Amitsur, S. A.; Levitzki, J. **Minimal identities for algebras**. Proc. Amer. Math. Soc. 1 (1950), 449-463.

[4] Artin, M. **On Azumaya algebras and finite dimensional representations of rings.** J. Algebra **11 (4)** (1969), 532-563.

[5] Berele, A. **Trace identities and $\mathbb{Z}/\mathbb{Z}_2$-graded invariants.** Trans. Amer. Math. Soc. **309** (1988), 581-589.

[6] Berele, A. **Matrices with involution and invariant theory.** J. Algebra **135 (1)** (1990), 139 - 164.

[7] Berele, A. **Invariant theory and trace identities associated with Lie color algebras.** J. Algebra **310 (1)** (2007), 194-206.

[8] Berele, A. **Invariant theory for matrices over the Grassmann algebra.** Adv. Math. **237** (2013), 33 - 61.

[9] Costa, N. L. **Identidades polinomiais e polinômios centrais para álgebra de Grassmann.** Dissertação (Dissertação em Matemática) - UFCG. Campina Grande, 2012.

[10] Curtis, C. W.; Reiner, I. **Representation theory of finite groups and associative algebras.** Interscience Publishers, 1962.

[11] Dehn, M. **Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme.** Festschrift. Springer, Berlin, Heidelberg, 1982

[12] Drensky, V. S.; Formanek, E. W. **Polynomial identity rings.** Basel: Birkhäuser, Advanced Courses in Mathematics CRM Barcelona), 2004.

[13] Drensky, V. **Free algebras and PI algebras, Graduate course in algebra**. Springer-Verlag Singapore, Singapore, 2000.

[14] Etingof, P. I.; Golberg, O.; Hensel, S.; Liu, T.; Schwendner, A.; Vaintrob, D.; Yudovina, E. **Introduction to representation theory**, vol. 59. American Mathematical Soc., 2011.

[15] Fidelis, C; Diniz, D.; Koshlukov, P. **Embeddings for the Jordan algebra of a bilinear form.** Adv. Math. **337** (2018), 294-316.

[16] Fraleigh, J. **A first course in Abstract Algebra.**. Pearson, 7th Edition, 2002.

[17] Fulton, W.; Harris, J. **Representation theory:** a first course. Springer Science & Business Media, 1991.

[18] Giambruno, A.; Zaicev, M. **Polynomial identities and asymptotic methods.** American Mathematical Society, 2005.

[19] Grace, J. H.; Young A. **The algebra of invariants**. Cambridge Univ. Press, New York, 1903.

[20] Hoffman, K.; Kunza, R. **Álgebra linear.** Prentice Gall, 2º. ed., 1971.

[21] Jacobson, N. **Basic Algebra I.** Courier Corporation, 2012.

[22] Jacobson, N. **Basic Algebra II:** Second Edition. Dover Publications, 2012. (Dover Books on Mathematics).

[23] Le Bruyn, L. **Noncommutative geometry and Cayley-smooth orders.** Pure and Applied Mathematics (Boca Raton), 290, 2008.

[24] Kaplansky, I. **Rings with a polynomial identity.** Bull. Amer. Math. Soc. **54 (6)** (1948), 575 - 580.

[25] Kemmer, A. R. **Varieties and $\mathbb{Z}_2$-Graded Algebras**. Mathematics of the USSR-Izvestiya **25 (2)** (1985), 359–374.

[26] Kemer, A. R. **Finite basis property of identities of associative Algebras.** Algebra Logic. **26 (5)** (1987), 362 - 397.

[27] Kraft, H.; Procesi, C. **Classical Invariant theory.** Preliminary Version, 1996.

[28] Pierce, R. S. **Associative algebras.** Graduate Texts in Mathematics, vol. 88, Springer- Verlag, Berlin Heidelberg New York, 1982.

[29] Procesi, C. **The Invariant theory of $n \times n$ matrices.** Adv. in Math. **19 (3)** (1976), 306-391.

[30] Procesi, C. **A Formal inverse to the Cayley-Hamilton theorem.** J. Algebra **107 (1)** (1987), 63 - 74.

[31] Procesi, C; **Lie groups. An approach through invariants and representations.** Universitext. Springer, New York, 2007.

[32] Razmyslov, J. P. **Trace identities of full matrix algebras over a field of characteristic zero.** Math. USSR-Izv. **8 (4)** (1974), 727 - 760.

[33] Razmyslov, Yu P. **Identities of algebras and their representations**. Trans. of Math. Monog., Am. Math. Soc., Providence, 138, 1994.

[34] Small, L. W. **An example in PI-ring.** J. Algebra **17** (1971), 434-436.

[35] Spencer, A. J. M. **Theory of invariants**. Continuum Physics, Vol. I; Academic Press, New York, 1971.

[36] Spencer, A. J. M.; Rivlin R. S. **The theory of matrix polynomials and its applications to the mechanics of isotropic continua.** Arch. Ration. Mech. Anal. **2** (1958), 309-336.

[37] Spencer, A. J. M.; Rivlin, R. S., **Finite integrity bases for five of fewer symmetric 3 x 3 matrices.** Arch. Ration. Mech. Anal. **2** (1958), 435-446.

[38] Specht, W. **Gesetze in Ringen. I.** Math. Z. **52 (1)** (1950), 557 - 589.

[39] Valverde, W.. **Álgebra parcial de grupo**. Dissertação (Dissertação em Matemática) - UFP. Curitiba, 2016.

[40] Vinciguerra, R W. **Involuções sobre álgebras de grupo semissimples.** Dissertação (Dissertação em Matemática) - UEM. Margingá, 2009.

[41] Wagner, W. **Über Die Grundlagen der Projektiven Geometrie und Allgemeine Zahlensysteme.** Math. A. **113 (1)** (1937), 528 - 567.