Felipe Yukihide Yasumura

Identidades polinomiais em álgebras de matrizes

CAMPINAS
2014

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Felipe Yukihide Yasumura

Identidades polinomiais em álgebras de matrizes

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

Orientador: Plamen Emilov Kochloukov

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO FELIPE YUKIHIDE YASUMURA, E ORIENTADA PELO PROF. DR PLAMEN EMILOV KOCHLOUKOV

Assinatura do Orientador

CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

Y26i

Yasumura, Felipe Yukihide, 1991-
Identidades polinomiais em álgebras de matrizes / Felipe Yukihide Yasumura. – Campinas, SP : [s.n.], 2014.

Orientador: Plamen Emilov Kochloukov.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. PI-álgebras. 2. Identidade polinomial. 3. Álgebra não-comutativa. 4. Representações de grupos. I. Kochloukov, Plamen Emilov,1958-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Polynomial identities in matrix algebras
Palavras-chave em inglês:
PI-algebras
Polynomial identity
Noncommutative algebra
Group representations (Mathematics)
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Plamen Emilov Kochloukov [Orientador]
Lucio Centrone
Dimas José Gonçalves
Data de defesa: 21-02-2014
Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 21 de fevereiro de 2014 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

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

Prof.(a). Dr(a). DIMAS JOSÉ GONÇALVES

Abstact

In this dissertation we present basic notions of the theory of algebras with polynomial identity (also called PI-algebras). Following the works of Razmyslov we prove the Specht property for the Lie algebra of 2x2 traceless matrices. We also find a minimal basis of identities of the 2x2 matrix algebra, based in the works of Dresnky.

To achieve these goals we develop the basic notions of the classical theory of non-commutative algebras. We develop techniques of the representations of the symmetric and of the general linear group. We also introduce basic notions of generic matrices.

In the proof of Specht property for the Lie algebra of 2x2 traceless matrices we use a method developed by Razmyslov (weak identities), and we use the structure of PI-algebras (theory of non-commutative algebras applied to PI-algebras; most of the results in this subject are due to Amitsur). Determining a minimal basis of identities of the 2x2 matrix algebra uses essentially the representation theory, and the results was obtained by Drensky.

We try to exhibit the necessary language and results for the presentation of the main theorems in this work. We expect that a reader will be acquainted with notions of some topics of non-commutative algebra, notions of basic theory of PI-algebras and ideas of the importance and simplification of the techniques using representations and generic matrices.

Resumo

Nesta dissertação, será apresentada noções básicas da teoria de álgebras com identidades polinomiais (denominados de PI-álgebras), e, seguindo o trabalho de Razmyslov, provaremos a propriedade de Specht para a álgebra de Lie de matrizes 2x2 de traço zero; e acharemos uma base minimal de identidades da álgebra associativa de matrizes 2x2, baseado nos trabalhos de Drensky.

Para esses objetivos, serão desenvolvidas noções da linguagem e teoria de álgebra não-comutativa clássica; serão desenvolvidas técnicas em representações do grupo simétrico e geral linear; e será abordada noções básicas de matrizes genéricas.

Na demonstração da propriedade de Specht para a álgebra de Lie de matrizes 2x2 de traço zero, utilizaremos uma ténica desenvolvida por Razmyslov (identidades fracas), e utilizaremos teoria de estrutura de PI-álgebras (teoria de álgebra não comutativa aplicada em PI-álgebras - a maioria dos resultados apresentados sobre este assunto são devido a Amitsur). Determinar uma base minimal de identidades para a álgebra de matrizes 2x2 utilizará fortemente a teoria de representações, e os resultados apresentados neste trabalho foram desenvolvidos principalmente por Drensky.

Na medida do possível, toda a linguagem e resultados necessários para a apresentação e demonstração dos teoremas principais serão apresentados neste trabalho, e espero que um leitor deste trabalho possa ter noções de alguns tópicos de álgebra não comutativa, noções da teoria básica de PI-álgebras e noções da importância e simplificação de contas das técnicas de representações e matrizes genéricas.

Sumário

À pessoa que me inspira e motiva os estudos e viver a vida

Agradecimentos

Agradeço ao prof. Plamen Kochloukov, meu orientador, pela paciência, orientação, pelos conhecimentos infinitos, dedicação, e tudo mais.

Aos professores Dimas José Gonçalvez e Lucio Centrone, professores da banca, por toda a paciência e dedicação na revisão da dissertação e presença na defesa, que, além de melhorarem muito o texto da dissertação, contribuíram enormemente com meus conhecimentos e experiência como (aspirante a) matemático.

À CAPES (programa PICME), pelo apoio financeiro.

A todos os professores, que contribuíram no meu caminho como estudante de matemática.

A todos os colegas e amigos.

Aos familiares, principalmente ao meu irmão.

E finalmente à minha namorada Kally, por toda paciência, todo carinho, companheirismo, apoio e por me fazer feliz e me animar aos estudos durante todo esse tempo de mestrado.

“Ué... Se não sabe,
aprende!”
Sheng Ly

Introdução

Cito inicialmente as palavras na dissertação de Diogo Diniz P. Silva [46]:

> A teoria das álgebras que satisfazem identidades polinomiais, denominadas também PI-álgebras, é uma parte importante da teoria de anéis. Os primeiros trabalhos que envolviam PI-álgebras apareceram, embora de forma implícita, na década de 1920-1930, nas pesquisas de Wagner e Dehn (poderíamos voltar às pesquisas de Sylvester, publicadas em 1852 e 1853, mas preferimos não entrar em assuntos históricos). O verdadeiro desenvolvimento da PI teoria começou com os trabalhos de N. Jacobson e I. Kaplansky, nos anos de 1950, e atualmente é uma área da álgebra bem desenvolvida e em expansão rápida. São três as principais linhas de pesquisa sobre PI-álgebras. A primeira (e a mais clássica) estuda as propriedades de uma álgebra (ou um anel) sabendo-se que ela satisfaz alguma identidade polinomial. A segunda representa-se por pesquisas sobre as classes de álgebras que satisfazem um dado sistema de identidades polinomiais (essas classes são chamadas de variedades de álgebras). A terceira estuda as identidades polinomiais satisfeitas por uma álgebra interessante. Gostaríamos de deixar claro que tal divisão não é definitiva nem exata e que os problemas na PI teoria, na maioria das vezes, estão interligados.

Para um pouco mais de história, indico para leitura o prefácio dos livros de Drensky [9] e o livro de Giambruno e Zaicev [15] - que, além de apresentarem uma intrudução histórica, são muito motivadores ao estudo de PI-álgebras.

Neste trabalho, o objetivo proposto inicialmente é estudar os artigos de Razmyslov [31] e o artigo de Drensky [11]. O primeiro estuda as identidades polinomiais das álgebras de matrizes 2×2 sobre um corpo de característica zero, e prova que a álgebra de Lie $\mathfrak{sl}(2, K)$ satisfaz a propriedade de Specht e exibe uma base para as identidades da álgebra associativa de matrizes $M_2(K)$ (todas as noções e linguagem são definidas no trabalho). O artigo de Drensky refina a base obtida por Razmyslov, exibindo uma base de identidades de $M_2(K)$ contendo apenas 2 elementos.

Para a demonstração desses teoremas, basicamente as técnicas utilizadas foram:

1. Teoria de estrutura de álgebras não-comutativas e PI-álgebras,
2. Identidades fracas - técnica desenvolvida por Razmyslov;
3. Teoria de representações do grupo simétrico, representações do Grupo Geral Linear, uma forma inteligente de aplicar isso na teoria de PI-álgebras, como refinar tudo isso, etc - muito da teoria estudada nesta dissertação foi desenvolvida por Drensky.

Esta dissertação é organizada da seguinte maneira:

No primeiro capítulo, serão apresentadas noções de definições e propriedades básicas das estruturas algébricas (grupos, anéis, módulos, produto tensorial e teoria de representações), e será também apresentada uma visão geral de álgebras, e introduzido o conceito principal de estudo neste trabalho: as PI-álgebras. Serão apresentadas várias definições e citadas propriedades básicas que serão muito importantes e utilizadas frequentemente neste trabalho.

No capítulo 2, apresentaremos noções básicas da teoria clássica de álgebras - noções básicas sobre a estrutura de álgebras não-comutativas, teoria de representações do grupo simétrico S_n, algumas definições na álgebra comutativa, e a construção de comutadores básicos. Finalizaremos o capítulo apresentando algumas consequências da teoria desenvolvida sobre a estrutura de PI-álgebras. A estrutura de PI-álgebras, em muitos casos, se comporta de uma forma muito próxima das álgebras comutativas - existem resultados na álgebra comutativa que valem para PI-álgebras (mas não são generalizações triviais, e quase sempre são difíceis). As PI-álgebras também parecem ser as álgebras não-comutativas mais próximas das matrizes (e da estrutura da álgebra não-comutativa, a experiência mostra que as álgebras de matrizes podem ser consideradas como as álgebras "mais simples").

No capítulo 3 apresentaremos vários resultados sobre PI-álgebras e algumas aplicações da teoria desenvolvida. Esses resultados serão essenciais para a demonstração dos teoremas principais desta dissertação.

No capítulo 4 são demonstrados os resultados principais.

Este trabalho foi escrito com o objetivo de ser acessível (no sentido de conter tudo o que precisaremos, ou pelo menos o enunciado - me esforcei para esse objetivo; o leitor poderá decidir) para qualquer pessoa interessada. Assumimos como conhecimentos prévios somente noções básicas em álgebra linear (incluindo noções básicas de polinômio característico e conhecer o enunciado do Teorema de Cayley–Hamilton), e em geral, trabalhamos com espaços vetoriais sobre álgebras de divisão (a maior parte da teoria de espaços vetoriais sobre corpos vale sobre anéis de divisão, para mais detalhes, ver o livro de Van der Waerden [36]). Algumas raras demonstrações utiliza-se também o *lema de Zorn*, e a única coisa que precisamos saber desse enunciado é que, em certas condições e em certos contextos, existem elementos maximais. Ter visto uma vez na vida noções básicas de teoria de grupos e teoria de anéis seria suficiente (ou pelo menos me esforcei para esse objetivo) para a leitura desta dissertação.

Quando uma seção é trabalhada para provar somente um teorema, tentei ao máximo facilitar a possibilidade de pular esta seção e tomar conhecimento apenas desse resultado principal - e para isso, em geral, o teorema principal de uma seção é enunciado re-apresentando (ou evitando de citar) a linguagem necessária para enunciar o tal teorema, que foi desenvolvida exclusivamente para esta seção (exceto, claro, quando os objetos definidos são constantemente utilizados, por exemplo, conceitos envolvendo PI-álgebras, radical de Jacobson, entre outros). Um preço para se pagar é que a leitura pode parecer mais repetitiva do que realmente poderia ser.

Capítulo 1

Conceitos Básicos

Neste capítulo serão apresentadas as ferramentas e noções básicas para a leitura desta dissertação. Com o objetivo de manter este trabalho auto contido, todas as definições e teoremas (ou quase todos) serão enunciados. A maioria das demonstrações aqui será omitida - por serem canônicas na álgebra, encontradas em qualquer livro sobre o assunto, por serem muito fáceis ou por serem muito trabalhosas e longo. Não irei me preocupar em expor muito detalhadamente os objetos, e essas seções devem, preferencialmente, serem lidas com o objetivo de fixar notações, referências para definições e enunciados de teoremas, referências para outros textos, e relembrar conceitos (com exceção da teoria de álgebras, onde apresento os conceitos de identidades polinomiais, e a teoria de módulos - ambos trabalhados um pouco mais detalhadamente, em relação às outras seções deste capítulo).

Na seção 1.1 discutimos algumas poucas noções básicas de teoria de grupos, e estudamos algumas propriedades do grupo simétrico S_n, que serão muito úteis aos propósitos desta dissertação.

Nas seções 1.2, 1.3, 1.5, 1.6, serão introduzidas algumas noções básicas de teoria de anéis, módulos, produto tensorial e teoria de representações. Na seção 1.4 será introduzidas algumas noções básicas em teoria de álgebras e apresentados objetos importantes e elementares no estudo de identidades polinomiais.

§1.1 Grupos

Nesta seção, introduzimos noções e propriedades básicas de grupos, e encerraremos definindo e estudando propriedades do grupo simétrico S_n. Tudo isso será importante nos métodos utilizados neste trabalho. Para leitura mais completa desta vasta teoria, o leitor pode consultar os livros de Cameron [7] ou Garcia e Lequain [14].

Começaremos definindo as estruturas básicas algébricas de grupos:

Definição 1.1.1. (a) Sejam G um conjunto não vazio e $\circ : G \times G \to G$ uma aplicação, e denote-a por $\circ(g,h) \mapsto g \circ h$, para $g, h \in G$. Diremos que o par $(G, \circ)$ é um **grupo** se vale:

(i) associatividade: $(g \circ h) \circ k = g \circ (h \circ k)$, para todo $g, h, k \in G$,

(ii) **elemento neutro**: existe um elemento, normalmente denotado por $e \in G$, tal que $g \circ e = e \circ g = g$, para todo $g \in G$,

(iii) existência de **inverso**: para todo $g \in G$, existe $h \in G$ tal que $g \circ h = h \circ g = e$. Normalmente, denota-se um tal elemento com a propriedade de h por g^{-1}.

Ainda, se a operação satisfazer a seguinte propriedade, diremos que o grupo é **abeliano**:

(iv) comutatividade: $g \circ h = h \circ g$, para todo $g, h \in G$.

Por comodidade, quando não houver ambiguidades, diremos "o grupo G" ao invés de "o grupo $(G, \circ)$", omitindo a operação $\circ$. Ainda, quando não houver ambiguidades com relação a operação, denotaremos o produto por justaposição, isto é, denotaremos $gh := g \circ h$, para $g, h \in G$.

(b) Um conjunto $G \neq \emptyset$ com uma aplicação $\circ : G \times G \to G$ é denominado **semigrupo** se $\circ$ satisfazer a associatividade. Ainda, diremos que $\circ$ admite identidade se satisfazer a propriedade (ii) da definição de grupo.

(c) Seja $S \subset G$ um subconjunto não vazio. Diremos que S é um **subgrupo** de G se S for um grupo.

(d) Seja $N \subset G$ um subgrupo. Diremos que N é **subgrupo normal** se, para todo $g \in G$, $gNg^{-1} := \{gng^{-1} : n \in N\} \subset N$.

(e) Sejam $(G, \circ), (H, *)$ grupos e $f : G \to H$ função. Diremos que f é **homomorfismo de grupos** se $f(g \circ h) = f(g) * f(h)$, para todo $g, h \in G$. Denota-se por $\mathrm{Hom}(G, H)$ o conjunto de todos os homomorfismos de grupos de G em H. Denota-se simplesmente por $\mathrm{End}(G) := \mathrm{Hom}(G, G)$.

(f) Sejam G, H grupos e $f : G \to H$ homomorfismo de grupos. Define-se o **núcleo** e a **imagem** de f por

$$\mathrm{Ker}\, f := \{g \in G : f(g) = e_H\} \quad \mathrm{Im}\, f := \{f(g) : g \in G\}$$

respectivamente, em que e_H é o elemento neutro de H.

(g) Sejam G, H grupos e $f : G \to H$ homomorfismo de grupos. Dizemos que f é:

(i) **epimorfismo** se for sobrejetora,

(ii) **monomorfismo** se for 1-1,

(iii) **isomorfismo** se for sobrejetora e 1-1. Neste caso, dizemos que G e H são isomorfos e indicamos por $G \simeq H$.

As seguintes propriedades são de fácil demonstração (ou nem tanto, na primeira vez) e podem ser encontradas em qualquer livro de introdução a teoria de grupos, não restrito somente aos livros citados:

Lema 1.1.2. *Sejam G, H grupos e $f : G \to H$ homomorfismo de grupos.*

(a) existe um único elemento neutro em G,

(b) para cada $g \in G$, existe um único inverso de g,

(c) dados $g, x, y \in G$, se $gx = gy$, então $x = y$. Da mesma forma, se $xg = yg$, então $x = y$,

(d) $Ker\, f$ é um subgrupo normal de G e $Im\, f$ é um subgrupo de H,

(e) São equivalentes, para um subgrupo de $N \subset G$:

(i) N é normal,

(ii) $gN = Ng, \forall g \in G$. (em que definimos $gN = \{gn : n \in N\}$ e $Ng = \{ng : n \in N\}$, para cada $g \in G$)

(f) $f(e_G) = e_H, f(g^{-1}) = (f(g))^{-1}$, para todo $g \in G$.

Existe uma quantidade muito grande de exemplos de grupos importantes, e seus axiomas são tão gerais que existem exemplos muito diferentes, e em geral, não há um "modelo de grupo" que pode ser seguido para intuição básica e para conjecturar resultados.

Também devido a essa grande quantidade de exemplos importantes de grupos, denotamos por e o elemento neutro de um grupo G e seu produto por justaposição, pois temos tantos grupos que são multiplicativos e grupos que são aditivos ("multiplicativo" e "aditivo" no sentido de senso comum). Quando estivermos trabalhando especificamente com grupos multiplicativos, iremos denotar o elemento neutro por 1. Quando trabalhamos com grupos abelianos, costuma-se denotar a operação por $+$, o elemento neutro por 0 e o inverso de um elemento $g \in G$ por $-g$.

Durante o resto deste trabalho, ao trabalharmos com mais de um grupo, a menos que tenha ambiguidades, não iremos utilizar uma notação com subíndices para indicar a operação do subgrupo ou o elemento neutro. Por exemplo, no item (f) do lema anterior, podemos escrever simplesmente $f(e) = e$.

Deixamos à verificação (ou busca por referências) do leitor, que os seguintes exemplos são de fato grupos.

Exemplo:

1. *Os números inteiros com a operação soma é um grupo abeliano,*
2. *Os números racionais não nulos com o produto usual de racionais é um grupo abeliano,*
3. *Seja $n \geq 1$, então, $(M_n(\mathbb{R}), \cdot)$, o conjunto das matrizes quadradas $n \times n$ com entradas reais e o produto usual de matrizes não é grupo (pois o elemento neutro necessariamente é a identidade e nem toda matriz admite inversa com relação ao produto). Mas, como uma matriz é invertível se e só se o determinante é não nulo (vale somente no caso de corpos; e para mais detalhes, ver, por exemplos, o livro de Hoffman [23], ou um livro de geometria analítica ou álgebra linear que comente sobre isso), tomando $Gl(n, \mathbb{R}) := \{a \in M_n(\mathbb{R}) : det\, a \neq 0\}$, temos $(Gl(n, \mathbb{R}), \cdot)$ grupo (não abeliano quando $n > 1$).*

4. *Seja X um conjunto e considere $Bij(X) = \{f : X \to X \text{ bijetora}\}$. Temos que $Bij(X)$ é um grupo com a operação usual de composição de funções. No caso especial em que X é finito e possui n elementos, denotaremos $Bij(X)$ por S_n e denominaremos de* ***grupo de permutações*** *de n elementos ou* ***grupo simétrico****. Em casos particulares de $X = \{a_1, \cdots, a_n\}$, denota-se também por $S_n(a_1, \cdots, a_n)$, para explicitar que estamos considerando o grupo que permuta os símbolos $a_1, \cdots, a_n$. Este exemplo será retomado no fim desta seção.*

5. *Seja X um conjunto e considere o conjunto das partes de X, $\mathscr{P}(X) = \{A \subset X \text{ subconjunto}\}$ e considere a operação diferença simétrica, isto é, $A \triangle B := (A \setminus B) \cup (B \setminus A)$, para $A, B \in \mathscr{P}(X)$. Então $(\mathscr{P}(X), \triangle)$ é um grupo abeliano.*

6. *Grupo diedral D_n (ver livro de Garcia e Lequain [14] para construção detalhada de D_3 e D_4, e para construção geral de D_n).*

□

Uma construção importantíssima na álgebra são os quocientes (e importantes em outras áreas da matemática, inclusive), e podem ser feitos em grupos:

Definição 1.1.3. Sejam G um grupo e $S \subset G$ um subconjunto não vazio (não necessariamente subgrupo). Dado $g \in G$, define-se (notação já utilizada anteriormente):

$$gS := \{gs : s \in S\}, \quad Sg := \{sg : s \in S\}.$$

Dados S_1, S_2 subconjuntos, define-se o produto por $S_1 S_2 := \{s_1 s_2 : s_1 \in S_1, s_2 \in S_2\}$.

Os próximos resultados podem ser encontrados em qualquer livro introdutório em teoria de grupos, e são canônicos (e não difíceis de demonstrar) na álgebra:

Lema 1.1.4. *Sejam G um grupo e $N \subset G$ um subgrupo:*

(a) dados $g, h \in G$, $gN = hN$ ou $gN \cap hN = \emptyset$,

(b) dados $g, h \in G$, $gN = hN$ se e só se $gh^{-1} \in N$,

(c) Denote por $G/N := \{gN : g \in G\}$ e considere o produto em G/N dado por produto de subconjuntos. Denomina-se os elementos de G/N de ***classes laterais*** *e dado $gN \in G/N$, denomina-se g um representante da classe gN. São equivalentes:*

(i) N é subgrupo normal,

(ii) $(gN)(hN) = (gh)N$, para todo $g, h \in G$,

(iii) G/N com essa operação é grupo,

(iv) o produto $(gN)(hN) = (gh)N$ está bem definido, isto é, não depende do representante g e h.

(d) Sejam H um grupo e $f : G \to H$ um homomorfismo de grupos. Então $G/Ker\, f \simeq Im\, f$.

Exemplo: *Os seguintes exemplos podem ser encontrados com mais detalhes nos livros citados: alguns são triviais, outros muito importantes e alguns não são imediatos (à primeira vista).*

1. *Sejam G e H grupos, com $e \in H$ o elemento neutro. Então $id : x \in G \mapsto x \in G$ e $f : x \in G \mapsto e \in H$ são homomorfismos de grupos, denominados de identidade e trivial, respectivamente.*

2. *Se $\{H_\alpha\}_{\alpha \in I}$ é família de subgrupos de um grupo G, então $H := \cap_{\alpha \in I} H_\alpha$ é um subgrupo de G. Se todos os H_α são normais, então H é normal.*

3. *Sejam G grupo e $S \subset G$ subconjunto qualquer. Defina $S^{-1} := \{s^{-1} : s \in S\}$. Então o conjunto $\langle S \rangle := \{s_1 \cdots s_n : n \in \mathbb{N}, s_1, \cdots, s_n \in S \cup S^{-1}\}$ é um subgrupo de G (denominado de **subgrupo gerado** por S); é o menor subgrupo de G contendo S e é a intersecção de todos os subgrupos de G que contem S.*

4. *Sejam G grupo e $N \subset G$ subgrupo normal. Então $\pi : x \in G \mapsto xN \in G/N$ é um homomorfismo de grupos (denominado **projeção canônica**).*

□

Finalizaremos a seção com uma definição importante e uma propriedade do grupo simétrico S_n.

Definição 1.1.5. Seja G um grupo. Dados $x, y \in G$, dizemos que x e y são **conjugados** se existe $g \in G$ tal que $y = gxg^{-1}$. Define-se a **classe de conjugação** de $x \in G$ como o conjunto $\{y \in G : y \text{ é conjugado a } x\} = \{gxg^{-1} : g \in G\}$.

Observação. (i) A relação "ser conjugado" é uma relação de equivalência.

(ii) Duas classes de conjugação podem ter quantidades diferentes de elementos. Por exemplo, a classe de conjugação do elemento neutro $e \in G$ sempre contém um único elemento.

(iii) Se C é uma classe de conjugação e $x \in C$, então $gxg^{-1} \in C, \forall g \in G$.

Seja $\sigma \in S_n$, o grupo simétrico. Normalmente, utiliza-se a notação

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_i & i_2 & \cdots & i_n \end{pmatrix}$$

em que $i_1, \cdots, i_n$ são os números $1, 2, \cdots, n$ e σ satisfaz $\sigma(m) = i_m, m = 1, \cdots, n$. Utiliza-se também a notação

$$\sigma = (j_{11} \quad j_{12} \quad \cdots \quad j_{1n_1})(j_{21} \quad j_{22} \quad \cdots \quad j_{2n_2}) \cdots (j_{m1} \quad j_{m2} \quad \cdots \quad j_{mn_m})$$

em que não há repetições de números, e σ é tal que $\sigma(j_{ki}) = j_{k,i+1}, k = 1, \cdots, m, i = 1, \cdots, n_k - 1$ e $\sigma(j_{kn_k}) = j_{k1}$. No caso de $n_i = 1$, costuma-se omitir o (j_{i1}) (exceto para a permutação identidade).

Definição 1.1.6. Um **r-ciclo** (com $1 \leq r \leq n$) é uma permutação da forma $(j_1 \quad j_2 \quad \cdots \quad j_r)$. Um 2-ciclo é denominado **transposição**. Dois ciclos são denominados **disjuntos** se cada símbolo é movido por no máximo um desses ciclos, isto é, σ e τ em S_n são disjuntos se $\sigma(m) = m$ ou $\tau(m) = m$, para cada $m = 1, \cdots, n$.

Observação. Se τ e σ em S_n são ciclos disjuntos, então $\sigma\tau = \tau\sigma$.

Os próximos resultados são não tão fáceis de demonstrar (e de natureza combinatória), e podem ser encontrados nas referências:

Proposição 1.1.7. *1. Todo elemento de S_n pode ser escrito de forma única como produto de ciclos disjuntos (a menos de omissão de 1-ciclos e a menos de ordem).*

2. *Todo elemento de S_n pode ser escrito como produto de transposições (não necessariamente disjuntas). Em geral, a decomposição não é única, mas, se $\sigma \in S_n$ é da forma $\sigma = \tau_1 \cdots \tau_r = \theta_1 \cdots \theta_m$, com $\tau_1, \cdots, \tau_r, \theta_1, \cdots, \theta_m$ transposições, então $r \equiv m(mod 2)$, ou seja, r e m têm sempre a mesma paridade.*

Essa última proposição prova que a seguinte noção está bem definida:

Definição 1.1.8. Seja $\sigma \in S_n$.

(i) Se $\sigma = (j_{11} \quad \cdots \quad j_{1n_1}) \cdots (j_{m1} \quad \cdots \quad j_{mn_m})$ é a representação de σ como produto de ciclos disjuntos, sem omitir os 1-ciclos, com $n_1 \geq n_2 \geq \cdots \geq n_m$, define-se o **tipo** de σ por $(n_1, n_2, \cdots, n_m)$.

(ii) Se $\sigma = \tau_1 \cdots \tau_l$ é um produto de transposições, define-se o **sinal** de σ como $(-1)^l$, e denota-se por ϵ_σ, $(-1)^\sigma$, $\text{sgn}(\sigma)$ ou $\text{sinal}(\sigma)$.

Nosso objetivo agora será caracterizar as classes de conjugação de S_n. Note que para cada tipo de permutação $(n_1, n_2, \cdots, n_m)$, temos $n_1 + n_2 + \cdots + n_m = n$, e reciprocamente, para cada conjunto de números inteiros $n_1, \cdots, n_m$ tais que $n_1 \geq n_2 \geq \cdots \geq n_m \geq 1$, com $n_1 + \cdots + n_m = n$, existe pelo menos uma permutação $\sigma \in S_n$ de tipo $(n_1, \cdots, n_m)$.

Definição 1.1.9. Uma **partição** de n (com n inteiro positivo) é um conjunto de números inteiros $(n_1, n_2, \cdots, n_m)$ tais que $n_1 \geq \cdots \geq n_m \geq 1$ e $n_1 + \cdots + n_m = n$. Denota-se por $(n_1, n_2, \cdots, n_m) \vdash n$.

Para iniciar estudos mais profundos nessa vasta teoria de partições, consultar o livro de Santos [34]. Provaremos que as classes de conjugação de S_n são exatamente as partições de n (as partições relacionadas com as classes de conjugação por meio do tipo de permutação):

Proposição 1.1.10. *Sejam $\sigma, \tau \in S_n$ e escreva $\sigma = (j_{11} \quad \cdots \quad j_{1n_1}) \cdots (j_{m1} \quad \cdots \quad j_{mn_m})$ produto de ciclos disjuntos. Então $\tau\sigma\tau^{-1} = (\tau(j_{11}) \quad \cdots \quad \tau(j_{1n_1})) \cdots (\tau(j_{m1}) \quad \cdots \quad \tau(j_{mn_m}))$.*

Demonstração. Provaremos a validade da afirmação para $\sigma = (j_1 \quad \cdots \quad j_r)$ um r-ciclo, e a validade para ciclos implicará na validade para σ qualquer, pois se $\sigma = \theta_1 \cdots \theta_m$ é a representação de σ como produto de ciclos disjuntos, então $\tau\sigma\tau^{-1} = \tau\theta_1\tau^{-1}\tau\theta_2\tau^{-1} \cdots \tau\theta_m\tau^{-1}$.

Como τ é uma permutação dos números $1, 2, \cdots, n$, podemos representar os inteiros de 1 a n das seguintes maneiras:

$$\{1, 2, \cdots, n\} = \{j_1, \cdots, j_r, i_1, \cdots, i_k\} = \{\tau(j_1), \cdots, \tau(j_r), \tau(i_1), \cdots, \tau(i_k)\}$$

(em que $i_1, \cdots, i_k$ são os números restantes para completar o conjunto $1, 2, \cdots, n$). Então, basta verificar a ação de $\tau\sigma\tau^{-1}$ sobre $\{\tau(j_1), \cdots, \tau(j_r), \tau(i_1), \cdots, \tau(i_k)\}$ e verificar que coincide com a ação do r-ciclo $\sigma_0 := (\tau(j_1) \quad \cdots \quad \tau(j_r))$:

Para $l = 1, \cdots, k$, temos $\tau\sigma\tau^{-1}(\tau(i_l)) = \tau\sigma(i_l) = \tau(i_l) = \sigma_0(\tau(i_l))$.

Para $l = 1, \cdots, r-1$, temos $\tau\sigma\tau^{-1}(\tau(j_l)) = \tau\sigma(j_l) = \tau(j_{l+1}) = \sigma_0(\tau(j_l))$.

Por fim, $\tau\sigma\tau^{-1}(\tau(j_r)) = \tau\sigma(j_r) = \tau(j_1) = \sigma_0(\tau(j_r))$.

Daí vale a igualdade e isso prova a afirmação. □

Corolário 1.1.11. *Duas permutações com o mesmo tipo são conjugadas.*

Assim, obtemos a caracterização das classes de conjugação de S_n, que será importantíssimo para esta dissertação.

Corolário 1.1.12. *As classes de conjugação do grupo de permutações de n elementos S_n são determinadas exatamente pelo tipo de permutação, isto é, existe uma bijeção natural entre as classes de conjugação de S_n e as partições de n (no sentido da definição 1.1.9).*

§1.2 Anéis e Extensão de Corpos

Nesta seção, serão relembradas definições clássicas, e fixadas terminologia e notações. Para referências mais detalhadas, indicamos os livros de Cameron [7] e Herstein [21]. Para uma abordagem mais voltada à teoria dos números algébricos e geometria algébrica (não será nosso foco aqui), indicamos o livro de Garcia e Lequain [14].

Começaremos com a definição básica de anéis:

Definição 1.2.1. Seja $(A, +, \cdot)$, em que $A \neq \emptyset$ é um conjunto e

$$\begin{aligned} + : (a, b) \in A \times A &\mapsto a + b \in A \\ \cdot : (a, b) \in A \times A &\mapsto a \cdot b \in A \end{aligned}$$

são duas operações em A, denominadas de soma e produto. Dizemos que $(A, +, \cdot)$ é um **anel** se valem:

(i) $(a + b) + c = a + (b + c), \forall a, b, c \in A$,

(ii) $a + b = b + a, \forall a, b \in A$,

(iii) existe $0 \in A$ tal que $a + 0 = a, \forall a \in A$,

(iv) para todo $a \in A$, existe $b \in A$ tal que $a + b = 0$,

(v) $(a + b) \cdot c = (a \cdot c) + (b \cdot c), c \cdot (a + b) = (c \cdot a) + (c \cdot b), \forall a, b, c \in A$.

Ainda, diremos que o anel A é associativo se

(vi) $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in A$.

Diremos que A admite unidade se

(vii) existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a, \forall a \in A$.

Diremos que A é comutativo se satisfaz

(viii) $a \cdot b = b \cdot a, \forall a, b \in A$.

Diremos que A é anel de divisão se A admite unidade 1 e se:

(ix) para todo $a \in A, a \neq 0$, existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$.

Por fim, diremos que A é corpo se A for anel de divisão comutativo. Quando não houver ambiguidades, omitiremos o produto $\cdot$ e denotaremos o produto por justaposição, isto é, $ab := a \cdot b$. Ainda, quando não houver ambiguidades com relação às operações, diremos simplesmente "anel A" ao invés de "anel $(A, +, \cdot)$".

Nesta dissertação, ao mencionarmos apenas "anel", entenderemos como **anel associativo, não necessariamente comutativo e não necessariamente com unidade**.

As seguintes propriedades são fáceis de demonstrar e podem ser encontradas nas referências:

Lema 1.2.2. *Seja A um anel:*

(i) o elemento neutro da soma é único, e será denotado por 0,

(ii) *o inverso aditivo é único, e será denotado por* $-a$ *o inverso de* $a \in A$,

(iii) *se* A *admite unidade, então ele é único, e será denotado por* 1,

(iv) *se* A *admite unidade e* $a \in A$ *admite inverso multiplicativo, então esse inverso é único, e será denotado por* a^{-1},

(v) $a \cdot 0 = 0, \forall a \in A$.

A seguir, apresentarei as estruturas básicas que acompanham anéis:

Definição 1.2.3. Seja $(A, +, \cdot)$ um anel.

(i) Um subconjunto não vazio $S \subset A$ é denominado **subanel** se as operações $+$ e $\cdot$ são fechadas em S e S for um anel (isto é, $s_1 + s_2, s_1 \cdot s_2 \in S, \forall s_1, s_2 \in S$).

(ii) Um subconjunto não vazio $I \subset A$ é denominado **ideal** (ou ideal bilateral) se I for subanel e $ai, ia \in I, \forall a \in A, \forall i \in I$. Denota-se por $I \lhd A$.

(iii) Um subconjunto não vazio $I \subset A$ é denominado **ideal à direita** se I for subanel e $ia \in I, \forall i \in I, \forall a \in A$. Denota-se por $I \lhd_r A$. Da mesma forma, define-se **ideal à esquerda**, denotado por $I \lhd_r A$, se I for subanel e $ai \in I, \forall i \in I, \forall a \in A$.

(iv) Seja $(B, \oplus, \odot)$ um anel. Uma função $f : A \to B$ é denominada **homomorfismo de anéis** se $f(a+b) = f(a) \oplus f(b)$ e $f(a \cdot b) = f(a) \odot f(b)$, para todo $a, b \in A$. Se A e B admitem unidades 1_A e 1_B, respectivamente, então exige-se também $f(1_A) = 1_B$.

(v) Dado $f : A \to B$ homomorfismo de anéis, define-se o **núcleo** e a **imagem** de f por $\operatorname{Ker} f = \{a \in A : f(a) = 0\}$ e $\operatorname{Im} f = \{f(a) : a \in A\}$.

Observação. 1. Daqui em diante, abusando de notação, não faremos distinção das operações e elementos neutros da soma e a unidade entre os anéis. Por exemplo, diremos que $f : A \to B$ é homomorfismo se satisfazer $f(a + b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$ e $f(1) = 1$ (se A e B admitem unidades).

2. O termo "ideal", caso não mencionarmos "bilateral", "à direita" ou "à esquerda", entenderemos como "ideal bilateral".

As propriedades seguintes são fáceis de demonstrar e podem ser encontradas em qualquer livro (das referências).

Lema 1.2.4. *Sejam* A *e* B *anéis e* $f : A \to B$ *homomorfismo de anéis.*

(i) $f(0) = 0$,

(ii) $f(-a) = -f(a), \forall a \in A$,

(iii) *se* $a \in A$ *é invertível, então* $f(a^{-1}) = f(a)^{-1}$,

(iv) $\operatorname{Im} f \subset B$ *é subanel e* $\operatorname{Ker} f$ *é ideal de* A.

Exemplo:

1. *Seja $\{A_\alpha\}_{\alpha\in I}$ uma família de anéis. O* ***produto direto*** *dessa família é o anel*

$$\prod_{\alpha\in I} A_\alpha = \left\{ f : I \to \bigcup_{\alpha\in I} A_\alpha \text{ com } f(\alpha) \in A_\alpha, \forall \alpha \in I \right\}.$$

A ***soma direta*** *externa é o seguinte subconjunto do produto direto:*

$$\bigoplus_{\alpha\in I} A_\alpha = \left\{ f \in \prod_{\alpha\in I} A_\alpha : f(\alpha) \neq 0 \text{ para uma quantidade finita de } \alpha \in I \right\}.$$

Para cada $\alpha \in I$, denota-se por π_α a projeção canônica:

$$\pi_\alpha : f \in \prod_{\alpha\in I} A_\alpha \mapsto f(\alpha) \in A_\alpha$$

e utiliza-se a mesma notação $\pi_\alpha : \bigoplus_{\alpha\in I} A_\alpha \to A_\alpha$ a restrição da projeção canônica sobre a soma direta.

2. *Seja $\{A_\alpha\}_{\alpha\in I}$ uma família de subanéis de um anel A. Então $\cap_{\alpha\in I} A_\alpha$ é um subanel de A. Define-se a soma interna da família por*

$$\sum_{\alpha\in I} A_\alpha := \left\{ \sum_{\alpha\in I} a_\alpha : \text{soma é finita}, a_\alpha \in A_\alpha, \forall \alpha \in I \right\}.$$

Caso I for finito, $I = \{1, \cdots, n\}$, denota-se simplesmente a soma

$$\sum_{i\in I} A_i = \sum_{i=1}^{n} A_i = A_1 + \cdots + A_n.$$

Se, em particular, (voltando ao caso de I arbitrário) $A_\alpha \cap (\sum_{\beta\in I, \beta\neq\alpha} A_\beta) = 0, \forall \alpha \in I$, denomina-se também a soma por ***soma direta*** *interna, e denota-se por $\bigoplus_{\alpha\in I} A_\alpha$, ou, no caso de I ser finito, denota-se por $\bigoplus_{i=1}^{n} A_i$ ou $A_1 \oplus \cdots \oplus A_n$.*

3. *Seja $\{I_\alpha\}_{\alpha\in I}$ família de ideais bilaterais (à direita, à esquerda, respectivamente) de um anel A. Então $\bigcap_{\alpha\in I} I_\alpha$ e $\sum_{\alpha\in I} I_\alpha$ são ideais bilaterais (à direita, à esquerda, respectivamente).*

4. *Seja A um anel. Então podemos construir o anel de polinômios em uma variável $A[x]$ (mais detalhes em Cameron [7] ou no livro de Garcia e Lequain [14]). Por indução, construímos o anel de polinômios em n variáveis $A[x_1, \cdots, x_n]$.*

5. *Seja A um anel. Então construímos o anel de matrizes $n \times n$ com entradas em A, denotado por $M_n(A)$ (mais detalhes no livro de Cameron [7]).*

6. *Sejam A um anel e $S \subset A$ um subconjunto não vazio. Então, o subanel gerado por S é definido pelo menor subanel de A que contém S.*

   Casos particulares: sejam K corpo, D anel de divisão, com $K \subset D$, e $S \subset D$ um subconjunto. Denotaremos por $K[S]$ o menor subanel de D contendo K e S, e denotaremos por $K(S)$ o menor anel de divisão de D contendo K e S.

7. *Se $S \subset A$ é tal que $\langle S \rangle = A$, então, dizemos que S é um conjunto gerador de A. Se A admite um conjunto gerador finito, então, dizemos que A é* ***finitamente gerado****. Se $I \subset A$ é um ideal gerado por um único elemento, denomina-se I de principal.*

8. *Seja A um anel. Dizemos que A é domínio de integridade se $xy \neq 0$, para todos $x, y \in A$ não nulos. Dizemos que A é um domínio de ideais principais se A for um domínio e todo ideal de A for principal.*

9. *Sejam A, B anéis e $f : A \to B$ homomorfismo de anéis. Dado $J \subset B$ ideal (bilateral, à direita ou à esquerda, respectivamente), temos que $f^{-1}(J) \subset A$ será ideal (bilateral, à direita ou à esquerda, respectivamente). Mas, dado $I \subset A$ ideal (bilateral, à direita, à esquerda, respectivamente), nem sempre $f(I) \subset B$ será ideal. Caso f seja sobrejetora, então sempre $f(I) \subset B$ será ideal (bilateral, à direita, à esquerda, respectivamente).*

□

Sejam A anel e $a \in A$. Nesta dissertação, utilizaremos as seguintes notações:

(i) Dado $n \in \mathbb{Z}$, define-se

$$na := \begin{cases} \underbrace{a + \cdots + a}_{n \text{ vezes}}, & \text{se } n > 0 \\ 0, & \text{se } n = 0 \\ (-n)(-a), & \text{se } n < 0 \end{cases}$$

(ii) $Aa = \{ra : r \in A\}, aA = \{ar : r \in A\}, AaA = \{ras : r, s \in A\}$.

(iii) $(A + \mathbb{Z})a = \{ra + na : r \in A, n \in \mathbb{Z}\}, a(A + \mathbb{Z}) = \{ar + na : r \in A, n \in \mathbb{Z}\}, (A + \mathbb{Z})a(A + \mathbb{Z}) = \{ras + na : r, s, \in A, n \in \mathbb{Z}\}$.

Temos Aa e $(A+\mathbb{Z})a$ ideais à esquerda; aA e $a(A+\mathbb{Z})$ ideais à direita, e $(A+\mathbb{Z})a(A+\mathbb{Z})$ e AaA ideais bilaterais. Se A admitir unidade 1, então $Aa = (A+\mathbb{Z})a$, $aA = a(A+\mathbb{Z})$ e $AaA = (A+\mathbb{Z})a(A+\mathbb{Z})$. Mas, em geral, se A não admitir unidade, as igualdades não valem (por exemplo, considere $A = 2\mathbb{Z} =$ (inteiros pares) e $a = 2$). Temos $(A + \mathbb{Z})a$, $a(A + \mathbb{Z})$ e $(A + \mathbb{Z})a(A + \mathbb{Z})$ os menores ideais à esquerda, à direita e bilateral, respectivamente, contendo o elemento a.

Existe uma construção clássica para adicionar uma unidade a um anel: seja A um anel (com ou sem unidade). Define-se

$$A^* = \mathbb{Z} \times A$$

com as operações $(n_1, a_1)+(n_2, a_2) = (n_1+n_2, a_1+a_2)$ e $(n_1, a_1)(n_2, a_2) = (n_1n_2, n_1a_2+n_2a_1+a_1a_2)$. Temos que A^* é um anel com unidade $(1, 0)$ e $A \subset A^*$ é um ideal bilateral. Se A admitir unidade $1 \in A$, então esse elemento não será mais unidade em A^*. Denota-se os elementos deste anel por $n + a := (n, a) \in A^*$. Note que, nesta notação, o produto é simplesmente a distributiva $(n_1 + a_1)(n_2 + a_2)$, em que n_1 e n_2 "agem" naturalmente sobre os elementos de A.

Neste trabalho, utilizaremos a seguinte terminologia:

Definição 1.2.5. Seja A um anel:

(i) A é dito **simples** se os únicos ideais bilaterais de A são 0 e A e $A^2 := \{ab : a, b \in A\} \neq 0$.

(ii) Um ideal bilateral $I \subset A$ (à direita, à esquerda, respectivamente) é dito ser **próprio** se $I \neq 0$ e $I \subsetneq A$.

(iii) Um ideal bilateral (à direita, à esquerda, respectivamente) $I \subset A$ é dito ser **maximal** se for diferente de A e não estiver contido propriamente em um ideal próprio bilateral (à direita, à esquerda, respectivamente).

(iv) Um ideal bilateral (à direita, à esquerda, respectivamente) $I \subset A$ é dito ser **minimal** se for não nulo e não conter propriamente um ideal próprio bilateral (à direita, à esquerda, respectivamente).

(v) Um elemento $a \in A$ é dito ser **nilpotente** se existe $n \in \mathbb{N}$ tal que $a^n = 0$ (em que definimos por indução $a^n := a^{n-1}a$ e $a^2 = aa$).

(vi) Um ideal bilateral (à direita, à esquerda, respectivamente) $I \subset A$ é dito ser **nil** se todo $a \in I$ for nilpotente. Dizemos que I é nil de índice n se todo $a \in I$ satisfazer $a^n = 0$ e se existir $b \in I$ tal que $b^{n-1} \neq 0$.

(vii) Um ideal bilateral (à direita, à esquerda, respectivamente) $I \subset A$ é dito ser **nilpotente** se existe $n \in \mathbb{N}$ tal que $I^n = 0$.

(viii) Um elemento $a \in A$ é dito ser **idempotente** se $a^2 = a$.

Sejam A um anel e $I \triangleleft A$ um ideal bilateral. Então, podemos construir o anel quociente A/I (mais detalhes nos livros [14] ou [7]). Para cada $a \in A$, definimos os conjuntos $a + I = \{a + i : i \in I\} \subset A$ (às vezes, denotamos simplesmente por $\bar{a} = a+I$). Denominam-se esses elementos de classes laterais, e o elemento a de representante da classe e denota-se por $A/I = \{a + I : a \in A\}$.

Definiremos soma e produto por $(a + I) + (b + I) = (a + b) + I, (a + I)(b + I) = ab + I$, para $a, b \in A$. Podemos provar que:

(i) $a + I = b + I$ ou $(a + I) \cap (b + I) = \emptyset, \forall a, b \in A$,

(ii) $a + I = b + I$ se e só se $a - b \in I$,

(iii) a soma e o produto definidos acima estão bem definidos, isto é, não dependem da escolha do representante, em outras palavras, se $a + I = a' + I$ e $b + I = b' + I$, então

- $(a + I) + (b + I) = (a' + I) + (b' + I)$,
- $(a + I)(b + I) = (a' + I)(b' + I)$.

(iv) com essas operações, A/I é um anel.

Exemplo: *Sejam A anel com unidade 1 e $I \subset A$ ideal bilateral. Então I é maximal se e só se A/I é simples (não necessariamente A/I será corpo ou anel de divisão; essas condições são garantidas se A for comutativo).* □

O próximo exemplo será muito importante, por ser um objeto que trabalharemos constantemente nesta dissertação:

Exemplo: *Seja D um anel de divisão. Então $M_n(D)$ é anel simples. De fato, denote por e_{ij} a matriz que tem entrada 1 na linha i e coluna j e 0 nas demais entradas, e note que $e_{ij}e_{kl} = \delta_{jk}e_{il}$, em que $\delta_{jk} = 1$, se $j = k$ e $\delta_{jk} = 0$, se $j \neq k$. Seja $I \subset M_n(D)$ um ideal bilateral não nulo e $a = \sum_{i=1}^{n} a_{ij}e_{ij} \in I$ não nulo. Então, existe (pelo menos um) $a_{ij} \neq 0$. Daí, sendo I bilateral, temos $e_{lk} = a_{ij}^{-1}e_{li}ae_{jk} \in I$, para todo $l, k = 1, \cdots, n$, e então, $I = M_n(D)$.* □

Por fim, apresentarei algumas terminologias clássicas de extensões de corpos. Para um estudo mais detalhado, consultar o livro de Endler [13].

Definição 1.2.6. Seja K um corpo. Define-se a característica de K, denotado por car K como o menor inteiro positivo n tal que $n \cdot 1 = 0$. Se não existir um tal inteiro positivo, define-se car $K = 0$.

Observação. 1. A característica de um corpo é sempre zero ou um número primo.

2. Dados um corpo K, $x, y \in K$ e $n \in \mathbb{N}$, vale a fórmula:

$$(x+y)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) x^i y^{n-i}.$$

3. Um caso particular do caso anterior, se car $K = p > 0$, então, dados $x, y \in K$, temos

$$(x+y)^p = x^p + y^p$$

Por indução, conclui-se que

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

Definição 1.2.7. Sejam K e L corpos.

1. Dizemos que L é uma **extensão** (de corpos) de K se $K \subset L$. Denota-se por $L|K$.
2. Seja $L|K$ extensão de corpos e $a \in L$. Dizemos que a é **algébrico** sobre K se existe $f \in K[x]$ não nulo tal que $f(a) = 0$. Caso contrário, dizemos que a é **transcendente**. Dizemos que $L|K$ é **extensão algébrica** se todo $a \in L$ for algébrico sobre K.
3. Uma extensão $L|K$ é dita ser **extensão finita** se L, visto como espaço vetorial sobre K, satisfazer $\dim_K L < \infty$.
4. Define-se o **grau da extensão** de $L|K$ por $[L : K] := \dim_K L$.

Os próximos resultados não são difíceis e encontram-se no livro citado:

Lema 1.2.8. *Seja $L|K$ extensão de corpos.*

1. *Se $a \in L$ é transcendente, então $K[a] \simeq K[x]$ (o subanel de L gerado por K e o elemento a é isomorfo ao anel de polinômios em uma variável com coeficientes em K).*
2. *São equivalentes, para $a \in L$:*
   - *(i) a é algébrico sobre K,*
   - *(ii) existe $n \in \mathbb{N}$ tal que $1, a, a^2, \cdots, a^n$ são linearmente dependentes sobre K (no espaço vetorial L sobre K),*
   - *(iii) o subanel $K[a]$ é corpo,*
   - *(iv) $K[a] = K(a)$ (o subanel de divisão gerado por K e a).*
3. *Seja $F|L$ outra extensão de corpos. Então*
   - *(i) Se $\{a_i\}_{i \in I}$ é base do espaço vetorial F sobre o corpo L e $\{b_j\}_{j \in J}$ é base do espaço vetorial L sobre K, então $\{a_i b_j\}_{(i,j) \in I \times J}$ é base do espaço vetorial F sobre K.*

(ii) $F|K$ *é finito se e só se* $F|L$ *e* $L|K$ *são finitos.*

(iii) $[F : L][L : K] = [F : K]$.

(iv) $F|K$ *é algébrico se e só se* $F|L$ *e* $L|K$ *são algébricos.*

4. Se $L|K$ *é finito, então* $L|K$ *é algébrico.*

Sejam $L|K$ extensão de corpos e $a \in L$ algébrico sobre K. Então, $\{f \in K[x] : f(a) = 0\}$ é um ideal de $K[x]$, como pode ser facilmente verificado. Como $K[x]$ é um domínio de ideais principais (vide livro [14], por exemplo), temos que existe um único polinômio mônico gerador deste ideal. Denomina-se este polinômio de **polinômio mínimo** de a sobre K, e denota-se por $p_K^a(x)$.

Pode-se provar a seguinte afirmação:

Lema 1.2.9. *Seja* $a \in L$ *algébrico sobre* K. *Então* $[K(a) : K] = gr(p_K^a(x))$.

§1.3 Módulos

Nesta seção, serão apresentadas definições e terminologia básica de módulos. A exposição será baseada no livro de Herstein [20], principalmente. Tentarei ser detalhista quanto a exemplos e intuição.

Daqui em diante, em geral, utilizaremos a letra "R" para designar anel e reservaremos "A" para álgebras (a menos que se diga o contrário), e essa regra não será seguida rigorosamente, havendo diversas repetições como "seja R um anel".

Definição 1.3.1. Sejam R um anel e $(M, +)$ um grupo abeliano. Dizemos que M é um **módulo** pela direita sobre R (denomina-se R-módulo à direita) se existe uma operação (denominada produto, ou multiplicação por escalar) $\cdot : (m, r) \in M \times R \mapsto m \cdot r \in M$ tal que:

(i) $(m_1 + m_2) \cdot r = m_1 \cdot r + m_2 \cdot r, \forall m_1, m_2 \in M, \forall r \in R$,

(ii) $(m \cdot r_1) \cdot r_2 = m \cdot (r_1 r_2), \forall m \in M, \forall r_1, r_2 \in R$,

(iii) $m \cdot (r_1 + r_2) = m \cdot r_1 + m \cdot r_2, \forall m \in M, \forall r_1, r_2 \in R$,

Se R admitir unidade 1, dizemos que $(M, +)$ é um R-módulo unitário (à direita) se:

(iv) $m \cdot 1 = m, \forall m \in M$.

Quando não houver ambiguidades, omitiremos a operação $+$ e diremos apenas "o R-módulo M", e omitiremos o produto, denotando por justaposição, isto é, para $m \in M$ e $r \in R$, denotamos por $mr := m \cdot r$.

Da mesma forma, define-se R-módulo à esquerda, em que a ação é dada pela esquerda, isto é, consideramos uma multiplicação por escalar $(r, m) \in R \times M \to r \cdot m \in M$, e, ao invés de (ii), um R-módulo à esquerda satisfaz:

(ii') $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m, \forall m \in M, \forall r_1, r_2 \in R$.

Quando omitirmos os termos "à direita" ou "à esquerda", a menos que seja adotada outra convenção em alguma seção, será entendido como "R-módulo à direita".

As seguintes observações indicarão uma primeira afirmação com relação a estrutura dos R-módulos pela definição (os elementos de $r \in R$ agem como homomorfismos de grupos), e mostraremos que, essencialmente, módulos à direita e à esquerda são a mesma coisa.

Observação. 1. O objetivo deste exemplo pode não ser tão claro num primeiro contato com módulos: sejam R um anel e M um R-módulo à direita. Defina uma operação $* : (r, m) \in R \times M \mapsto r * m := mr \in M$. Então, M é um R-módulo à esquerda, com relação a esta operação?

A resposta é não, e o axioma que falha (em geral - nem sempre) é o (ii') da definição 1.3.1, pois se $r, s \in R$, então, dado $m \in M$,

- $r * (s * m) = r * (ms) = (ms)r = m(sr)$,
- $(rs) * m = m(rs)$

e daí, necessariamente $m(rs) = m(sr), \forall r, s \in R, \forall m \in M$. Essa condição vale, por exemplo, se R é anel comutativo.

2. Para mostrarmos que a escolha de R-módulos "à esquerda" ou "à direita" é praticamente a mesma coisa, precisamos de uma construção mais elaborada que a anterior.

Dado um anel R, define-se o anel $(R^{op}, +, *)$ da seguinte maneira: tomamos o mesmo conjunto, $R^{op} = R$, e a mesma operação soma, e o produto é definido invertendo-se a ordem: $r * s := sr, \forall r, s \in R$. Temos $(R^{op}, +, *)$ anel, e denotamos simplesmente por R^{op}, quando nos referirmos ao anel R com o produto invertido. Ainda, os anéis R^{op} e R são muito parecidos, e mais precisamente, são denominados **anti-isomorfos**, isto é, dois anéis R e S são denominados anti-isomorfos se existe $f : R \to S$ tal que:

(i) f é 1-1 e sobrejetora,

(ii) $f(r_1 + r_2) = f(r_1) + f(r_2), \forall r_1, r_2 \in R$,

(iii) $f(r_1 r_2) = f(r_2)f(r_1), \forall r_1, r_2 \in R$,

(iv) Se R e S admitirem unidade, então $f(1) = 1$.

Denomina-se a aplicação f de **anti-isomorfismo**.

No nosso caso, a aplicação identidade $x \in R \mapsto x \in R^{op}$ é um anti-isomorfismo. Daí, dado um R-módulo à direita M, definindo a ação de R à esquerda de M por $rm := mr$, temos que M é um R^{op}-módulo à esquerda.

O anel R^{op} tem fins formais apenas e, em geral, simplifica muito a notação.

3. Sejam $(M, +)$ um grupo abeliano e considere $E = \mathrm{End}(M) =$(homomorfismos de grupos de M em M). Denotaremos a ação de E em M pela direita, isto é, escrevemos $a\phi$, com $a \in M$ e $\phi \in E$, ao invés de $\phi(a)$ - a vantagem desta notação é que, ao fazermos a composição de dois endomorfismos, $a(\phi\varphi)$, com $a \in M$, $\phi, \varphi \in E$, temos que valerá $a(\phi\varphi) = (a\phi)\varphi$, isto é, ao vermos a composição $\phi\varphi$, vemos a ordem da ação dos endomorfismos pela ordem natural de leitura. Podemos definir uma soma natural em E e considerar a composição usual de aplicações como produto, e com essas operações, segue que E é um anel e M é um E-módulo.

Agora, sejam R um anel e M um R-módulo à direita. Considere novamente $E = \mathrm{End}(M)$ (lembre-se que, por definição, M é um grupo abeliano). O primeiro axioma de R-módulo diz que os elementos de R agem em M como homomorfismos de grupos. Os axiomas seguintes dizem que a ação se comporta bem com relação às operações de R, e isso equivale a, formalmente, que existe um homomorfismo de anéis $R \to E$. Reciprocamente, todo subanel $R \subset E$ induz uma estrutura natural de R-módulo à direita em M, e então, os módulos obtidos à partir de um grupo abeliano M são ações de subanéis $R \subset E$. Essa caracterização é interessante

(principalmente para lembrar dos axiomas de módulos), mas não é intuitivamente boa. Em particular, as propriedades básicas de homomorfismos de grupos valem para as ações de R sobre M.

Exemplo: *Considere R um anel e $M_n(R)$ o anel de matrizes $n \times n$ com entradas em R. Então, a transposição (a clássica transposta de matrizes) é um anti-isomorfismo de $M_n(R)$ sobre ele mesmo. Esse exemplo mostra um anti-isomorfismo natural e que um anel pode ser anti-isomorfo a ele mesmo.* □

A seguir, apresentarei alguns exemplos de módulos:
Exemplo:

1. *Seja V um espaço vetorial sobre K. Então V é um K-módulo à direita (e à esquerda também). Sabe-se que espaços vetoriais sobre corpos (ou sobre anel de divisão) são soma direta de cópias do corpo. Em geral, não é um bom ter "soma de corpos" como modelo de intuição para módulos, pois muitos módulos não estão nem perto dessa situação.*

2. *Sejam V espaço vetorial sobre K e $E = End_K(V)$ o espaço das aplicações lineares de V em V. Então V é um E-módulo (à esquerda ou à direita, depende da notação).*

3. *Seja V um espaço vetorial sobre K e fixe $T \in End_K(V)$ (assuma que a ação das aplicações lineares se dá pela direita). Considere o anel de polinômios em uma variável $K[x]$. Para cada $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, defina $f(T) = a_0I + a_1T + \cdots + a_nT^n \in E$, em que $I \in E$ é a aplicação identidade. Então V é um $K[x]$-módulo à direita com a ação $vf(x) := vf(T), \forall v \in V, \forall f(x) \in K[x]$.*

4. *Sejam R um anel e $I \lhd_r R$ um ideal à direita. Então I admite naturalmente uma estrutura de R-módulo à direita. Em particular, R é um R-módulo à direita.*

□

Alguns elementos que acompanham módulos:

Definição 1.3.2. 1. Sejam M um R-módulo e $N \subset M$ um subconjunto não vazio. Dizemos que N é um **R-submódulo** se N for subgrupo e $nr \in N, \forall n \in N, \forall r \in R$.

2. Sejam M e N R-módulos e $f : M \to N$ função. Dizemos que f é **homomorfismo de R-módulos** se

   (a) $f(m_1 + m_2) = f(m_1) + f(m_2), \forall m_1, m_2 \in M$,
   (b) $f(mr) = f(m)r, \forall m \in M, \forall r \in R$.

3. Sejam M, N R-módulos e $f : M \to N$ homomorfismo de R-módulos. Define-se o **núcleo** e a **imagem** de f por $\operatorname{Ker} f := \{m \in M : f(m) = 0\}$ e $\operatorname{Im} f := \{f(m) : m \in M\}$ (denotado também por $f(M)$). Denota-se por $\operatorname{Hom}_R(M, N)$ ao conjunto de todos os homomorfismos de R-módulos entre M e N. Denota-se simplesmente $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$.

4. Sejam R, S anéis e M um grupo abeliano, que é um R-módulo à direita e um S-módulo à esquerda. Dizemos que M é um **bimódulo** à direita por R e à esquerda por S (ou simplesmente um (S, R)-bimódulo ou denota-se simplesmente por ${}_SM_R$) se $(sm)r = s(mr), \forall m \in M, \forall s \in S, \forall r \in R$.

5. Um homomorfismo de R-módulos $f : M \to N$ é denominado:
   (a) **monomorfismo** se for 1-1,
   (b) **epimorfismo** se for sobrejetora,
   (c) **isomorfismo** se for 1-1 e sobrejetora. Neste caso, dizemos que M e N são isomorfos e denota-se por $M \simeq N$.

Exemplo: *Seja R um anel. Então, os ideais à direita de R são exatamente os R-submódulos do R-módulo à direita R.* □

Dados M um R-módulo e $N \subset M$ um R-submódulo, temos $(N, +)$ subgrupo normal do grupo $(M, +)$ (todo subgrupo de $(M, +)$ é normal, pois M é abeliano). Então podemos construir o grupo (abeliano) quociente M/N. Ainda, podemos definir uma ação de R sobre M/N natural, dado por

$$(m + N)r := (mr) + N, m \in M, r \in R,$$

e com isso, podemos facilmente demonstrar que essa ação é bem definida e M/N é naturalmente um R-módulo.

Observação. Utilizaremos as seguintes notações e fatos neste trabalho:

1. Seja $\{M_\alpha\}_{\alpha \in I}$ uma família de R-módulos.
   (i) O **produto direto** dessa família é definido por

   $$\prod_{\alpha \in I} M_\alpha := \left\{ f : I \to \bigcup_{\alpha \in I} M_\alpha : f(\alpha) \in M_\alpha, \forall \alpha \in I \right\},$$

   e definindo naturalmente soma e multiplicação por escalar, temos que $\prod_{\alpha \in I} M_\alpha$ é um R-módulo.
   (ii) Define-se a soma direta externa dessa família como

   $$\bigoplus_{\alpha \in I} M_\alpha := \left\{ f \in \prod_{\alpha \in I} M_\alpha : f(\alpha) \neq 0 \text{ apenas para um número finito de } \alpha \in I \right\}$$

   tem-se que $\bigoplus_{\alpha \in I} M_\alpha$ é um R-módulo.
2. Sejam M um R-módulo e $\{N_\alpha\}_{\alpha \in I}$ uma família de R-submódulos de M.
   (i) $\bigcap_{\alpha \in I} N_\alpha$ é um R-submódulo de M,
   (ii) $\sum_{\alpha \in I} N_\alpha := \left\{ \sum_{\alpha \in I} a_\alpha : \text{soma finita e } a_\alpha \in N_\alpha, \forall \alpha \in I \right\}$ é R-submódulo de M, denominada de soma de $\{N_\alpha\}_{\alpha \in I}$. No caso da família ser finita, diga-se $\{N_1, \cdots, N_l\}$, denota-se também por

   $$\sum_{i=1}^{l} N_i \text{ ou } N_1 + \cdots + N_l$$

   Se ainda ocorrer $N_\alpha \cap (\sum_{\beta \in I \setminus \{\alpha\}} N_\beta) = 0, \forall \alpha \in I$, diz-se que a soma é direta e denota-se por $\bigoplus_{\alpha \in I} N_\alpha$ (ou, no caso da família ser finita, denota-se por $\bigoplus_{i=1}^{l} N_i$ ou $N_1 \oplus \cdots \oplus N_l$).

3. Seja $a \in M$. Denota-se por:

   (i) para $n \in \mathbb{Z}$, define-se
   $$an := \begin{cases} 0, & \text{se } n = 0 \\ \underbrace{a + \cdots + a}_{n \text{ vezes}}, & \text{se } n > 0 \\ (-n)(-a), & \text{se } n < 0 \end{cases},$$

   (ii) $aR := \{ar : r \in R\}$ (é R-submódulo de M),

   (iii) $a(R + \mathbb{Z}) := \{ar + an : r \in R, n \in \mathbb{Z}\}$ (é R-submódulo de M).

4. Sejam M um R-módulo e $S \subset M$ um conjunto não vazio.

   (a) Definimos o R-submódulo gerado por S como sendo o menor R-submódulo de M contendo S, e denotamos por $\langle S \rangle$. Se $S = \{x_1, \cdots, x_n\}$ for finito, denotamos simplesmente (aproveitando as notações introduzidas anteriormente) por $\langle S \rangle := x_1R + \cdots + x_nR$. Caso $\langle S \rangle = M$, dizemos que S é um conjunto gerador de M. Se S for finito e for um conjunto gerador de M, dizemos que M é **finitamente gerado**.

   (b) Escreva $S = \{a_\alpha\}_{\alpha \in I}$ e assuma que todo $m \in M$ admite uma única representação na forma (soma finita) $m = \sum_{\alpha \in I} a_\alpha r_\alpha$, com $r_\alpha \in R$. Então, M é dito **livre**, e S é denominado de **base livre** de M.

5. Seja M um R-módulo.

   (a) Dado $S \subset M$ um subconjunto não vazio, definimos o **anulador de S em R** por $\mathrm{Ann}_R(S) := \{x \in R : sx = 0, \forall s \in S\}$.

   (b) Dado $G \subset R$ um subconjunto não vazio, definimos o **anulador de G em M** por $\mathrm{Ann}_M(G) := \{m \in M : mx = 0, \forall x \in G\}$.

Enunciamos os teoremas clássicos de isomorfismo:

Lema 1.3.3. *Seja $f : M \to N$ epimorfismo de R-módulos. Então:*

(i) $M/Ker\, f \simeq N$,

(ii) existe bijeção entre os submódulos de M contendo $Ker\, f$ e os submódulos de N, ainda, denomine $\sum_M$ = (submódulos de M contendo $Ker\, f$) e $\sum_N$ = (submódulos de N). Então $A \in \sum_M \mapsto f(A) \in \sum_N$ é a bijeção e sua inversa é $B \in \sum_N \mapsto f^{-1}(B) \in \sum_M$.

(iii) Sejam N_1 e N_2 submódulos de M. Então $(N_1 + N_2)/N_2 \simeq N_1/(N_1 \cap N_2)$.

Observação. A importância do isomorfismo do item (iii) fica mais evidente quando nos deparamos com a seguinte necessidade: dados N_1 e N_2 R-submódulos, queremos considerar o quociente N_1/N_2. O primeiro problema que encontramos é que se N_2 não está contido em N_1, então não faz sentido o quociente. Então, podemos pensar em duas soluções naturais:

1. tomarmos um espaço um pouco maior do que N_1 de modo que este espaço contenha N_2, formalmente, considerar o quociente $(N_1 + N_2)/N_2$;

2. tomarmos um espaço menor do que N_2, de modo que este espaço esteja em N_1, formalmente, considerar o quociente $N_1/(N_1 \cap N_2)$.

Por sorte, esses dois espaços são bons, no sentido de ambos ter propriedades intuitivas que gostaríamos ("N_1 quocientado por N_2"). Ainda, o isomorfismo indicado mostra que esses dois espaços coincidem.

A seguinte terminologia será utilizada ao longo deste trabalho:

Definição 1.3.4. Seja M um R-módulo.

(i) M é dito **irredutível** se os únicos submódulos de M são 0 e M e $MR \neq 0$.

(ii) Um submódulo $N \subset M$ é dito maximal se $N \neq M$ e não estiver contido propriamente em um submódulo próprio.

(iii) Um submódulo $N \subset M$ é dito minimal se $N \neq 0$ e não conter propriamente um submódulo não nulo.

(iv) Uma cadeia ascendente de submódulos é uma família de submódulos $\{N_\alpha\}_{\alpha \in \mathscr{I}}$, indexado por um conjunto bem ordenado $\mathscr{I}$, tal que $N_\alpha \subset N_\beta$ sempre que $\alpha \leq \beta$.

Uma cadeia descendente é uma família de submódulos $\{N_\alpha\}_{\alpha \in \mathscr{I}}$, com $\mathscr{I}$ bem ordenado, tal que $N_\alpha \supset N_\beta$, se $\alpha \leq \beta$.

(v) M é dito **Noetheriano** (ou, que satisfaz a condição de cadeia ascendente) se para toda cadeia ascendente $\{N_\alpha\}_{\alpha \in \mathscr{I}}$ de submódulos, existe $\beta \in \mathscr{I}$ tal que $N_\gamma = N_\beta$, sempre que $\beta \leq \gamma$.

M é dito **Artiniano** (ou, que satisfaz a condição de cadeia descendente) se para toda cadeia descendente de submódulos $\{N_\alpha\}_{\alpha \in \mathscr{I}}$, existe $\beta \in \mathscr{I}$ tal que $N_\gamma = N_\beta$, sempre que $\beta \leq \gamma$.

(vi) Um anel R é dito Noetheriano (respectivamente, Artiniano) se o for como um R-módulo à direita.

Observação.

1. Um R-submódulo $N \subset M$ é dito ser irredutível se for minimal e $NR \neq 0$. Caso R tenha unidade e M for R-módulo unitário (isto é, $1 \in R$ age como identidade), então "irredutibilidade" e "minimalidade" são equivalentes.

2. Se $N \subset M$ é R-submódulo maximal, então M/N é irredutível se e só se $(M/N)R \neq 0$. No caso de M ser unitária (e R admitir unidade), temos N maximal se e só se M/N é irredutível.

3. Sejam N irredutível e $a \in N$ não nulo (temos $N \neq 0$, pela condição $NR \neq 0$). Então $aR = N$. De fato, temos aR um R-submódulo de N, e N sendo irredutível, implica $aR = 0$ ou $aR = N$. A primeira opção não ocorre, pois definindo $N' = \{b \in N : bR = 0\}$, temos N' um R-submódulo de N, e N sendo irredutível, temos $N' = 0$ ou $N' = N$. A segunda é impossível por definição, pois se não, teríamos $NR = 0$. Daí vale a primeira, que é equivalente à afirmação: se $b \in N$ é tal que $bR = 0$, então $b = 0$. Daí, se $a \in N$ é não nulo, então $N = aR$.

4. Seja $N \subset M$ R-submódulo irredutível e $A \subset M$ R-submódulo qualquer. Então $A \cap N = 0$ ou $A \cap N = N$. De fato, essa observação segue direto de $A \cap N$ ser um R-submódulo de N, e N sendo irredutível, segue que $A \cap N = 0$ ou $A \cap N = N$.

5. As condições "Noetheriano" e "Artiniano" parecem simétricas, mas, pode-se mostrar que, para anéis, a condição "Artiniano" é mais forte. Em geral, para módulos, pode-se construir exemplos de módulos Artinianos não Noetherianos.

   Exemplos de módulos Noetherianos e não Artinianos são mais comuns: o anel de inteiros $\mathbb{Z}$, o anel de polinômios em n variáveis, etc.

Proposição 1.3.5. *(i) Um R-módulo M é Noetheriano (respectivamente Artiniano) se e só se toda família não vazia de R-submódulos de M admite um elemento maximal (respectivamente minimal) com respeito a inclusão.*

(ii) Sejam M R-módulo e $N \subset M$ R-submódulo. Então M é Noetheriano (respectivamente Artiniano) se e só se N e M/N são Noetherianos (respectivamente Artinianos).

(iii) M é Noetheriano se e só se todo submódulo $N \subset M$ é finitamente gerado.

(iv) Seja $M = N_1 \oplus N_2$, com M, N_1, N_2 R-módulos. Então M é Noetheriano se e só se N_1 e N_2 são Noetherianos.

A demonstração pode ser encontrada no livro de Lambek [25] ou no livro de Atiyah e Macdonald [4] (no primeiro, assume-se R com unidade; e no segundo, assume-se R comutativo com unidade. Ambos os casos, e no caso geral de R não necessariamente com unidade e não necessariamente comutativo, possuem demonstrações idênticas, sem necessidades dessas hipóteses adicionais).

Uma das ideias ao definir os conceitos de Noetheriano e Artiniano é uma tentativa de obter o que seriam os módulos mais simples. Por exemplo, no caso de espaços vetoriais, os espaços mais simples são os de dimensão finita. Infelizmente, alguns exemplos mostram que não é possível ter um conceito de dimensão bem definido para todos os módulos (um bom exercício é pensar em o que seria uma boa definição para dimensão e após isso, pensar em um exemplo para mostrar que essa definição não é aplicável a todos os módulos, não é boa ou é inconsistente).

A ideia de módulo Noetheriano admite uma certa finitude, uma vez que M será finitamente gerado. Um módulo Artiniano admite finitude no sentido de: iniciando em um submódulo A_1, considere um submódulo A_2 contido propriamente em A_2, e continue tomando submódulos, um propriamente contido no anterior. Seguindo esse processo, em algum passo finito, chegaremos no módulo 0 sempre. Pode-se definir uma noção (relacionado com os conceitos Artiniano e Noetheriano) nos módulos (noções de série de composição e comprimento de série de composição) que é algo bem definido, nos fornece um número que pode servir para medir "simplicidade" de módulo e coincide com a noção de "dimensão" quando calculados em espaços vetoriais. O problema é que, podemos ter espaços não isomorfos que retornam as mesmas informações com respeito a essa medida.

Poderíamos tentar considerar os módulos livres com base livre finita. Mas, o problema estaria no fato de que a estrutura do anel pode não ser simples. Atualmente, o conceito de "módulo mais simples" que mais deu certo foi o estudo de anéis "mais simples possíveis" (anéis completamente redutíveis e Teorema de Wedderburn-Artin).

§1.4 Álgebras

Nesta seção, apresentarei a estrutura sobre a qual trabalharei na maior parte nesta dissertação.

Começaremos com a definição de álgebra:

Definição 1.4.1. Sejam A um espaço vetorial sobre um corpo K e $* : (a, b) \in A \times A \mapsto a * b \in A$ uma operação em A (denominada de produto). Dizemos que $(A, *)$ é uma **álgebra** sobre um corpo K, ou simplesmente uma K-álgebra, se satisfaz:

(i) $(a_1 + \alpha a_2) * b = a_1 * b + \alpha(a_2 * b), \forall a_1, a_2, b \in A, \forall \alpha \in K$,

(ii) $a * (b_1 + \alpha b_2) = a * b_1 + \alpha(a * b_2), \forall a, b_1, b_2 \in A, \forall \alpha \in K$.

Ainda, dizemos que:

1. A é dito ser álgebra com unidade se existir $1 \in A$ tal que $1 * a = a * 1 = a, \forall a \in A$,
2. A é **álgebra associativa** se satisfaz $(a * b) * c = a * (b * c), \forall a, b, c \in A$,
3. A é **álgebra comutativa** se satisfaz $a * b = b * a, \forall a, b \in A$,
4. A é **álgebra de Lie** se satisfaz $a * a = 0, \forall a \in A$ e $a * (b * c) = (a * b) * c + b * (a * c), \forall a, b, c \in A$.

Como de costume, quando não houver ambiguidades com relação ao produto considerado, diremos simplesmente "álgebra A" ao invés de "álgebra $(A, *)$". Ao trabalharmos com álgebras associativas e não houver ambiguidades com relação ao produto considerado, denota-se o produto por justaposição $ab := a * b$. Ao trabalharmos com álgebras de Lie, costuma-se denotar o produto pelo colchete $[a, b] := a * b$.

Observação.

1. Fixaremos a notação que, a menos que se diga o contrário, ao mencionar álgebra, entenderemos como **álgebra associativa, não necessariamente comutativa e não necessariamente com unidade** (essa convenção é adotada pela maioria das pessoas).
2. Fixaremos a notação de, quando trabalharmos com um produto não associativo $*$, um produto de n elementos será "normado à esquerda", isto é, definiremos

$$a_1 * a_2 * \cdots * a_n := (a_1 * \cdots * a_{n-1}) * a_n$$

em particular, para o colchete, denotaremos

$$[a_1, \cdots, a_n] := [[a_1, \cdots, a_{n-1}], a_n]$$

3. Alguns autores trabalham com álgebra sobre um anel comutativo com unidade K. Uma das vantagens de assumir essa generalidade é que incluímos anéis como álgebras (todo anel é uma $\mathbb{Z}$-álgebra). Não assumiremos essa generalidade (mesmo muitos resultados podendo ser provados para esse caso mais geral), e com isso, teremos a rica estrutura de espaço vetorial.
4. Note que toda álgebra (associativa) é um anel (associativo). Dada uma álgebra associativa A, e definindo um colchete em A por $[a, b] := ab - ba$, temos que $(A, [\,])$ será uma álgebra de Lie, como pode ser verificado diretamente.

Exemplo:

1. *As matrizes $M_n(K)$ sobre um corpo (ou anel de divisão) é uma álgebra, com o produto usual de matrizes. Temos também que $M_n(K)$ é uma álgebra de Lie, com respeito ao comutador.*
2. *As matrizes de traço zero, $\mathfrak{sl}(n, K) := \{g \in M_n(K) : tr(g) = 0\}$ é uma álgebra de Lie com respeito ao comutador (mas não é uma álgebra associativa).*
3. *O espaço vetorial $\mathbb{R}^3$ com o produto vetorial $\times$ é uma álgebra de Lie.*

□

Todas as estruturas envolvendo álgebras (subálgebras, ideias, homomorfismos...) são definidas de forma igual ao caso de anéis, com a exigência extra de que a estrutura seja compatível com a ação dos elementos do corpo (isto é, que trabalhemos sobre espaços vetoriais). Iremos indicar a definição exata e rápida dessas estruturas:

Definição 1.4.2. Seja $(A, *)$ uma álgebra não necessariamente associativa sobre K.

1. Um subespaço vetorial $S \subset A$ é dito ser uma subálgebra se $s_1 * s_2 \in S, \forall s_1, s_2 \in S$.

2. Um subespaço vetorial $I \subset A$ é dito ser um ideal bilateral, denotado por $I \lhd A$, se $i * a, a * i \in I, \forall a \in A, \forall i \in S$. Dizemos que I é um ideal à direita, e denotamos por $I \lhd_r A$ se $i * a \in I, \forall a \in A, \forall i \in I$. Da mesma forma, define-se ideal à esquerda, denotado por $I \lhd_l I$. Ao mencionarmos apenas "ideal", entendemos por "ideal bilateral".

3. Sejam $(B, \circ)$ uma álgebra e $f : A \to B$ uma função. Dizemos que f é homomorfismo de álgebras se f é uma transformação K-linear e $f(a * b) = f(a) \odot f(b), \forall a, b \in A$. Denota-se por $\mathrm{Hom}_K(A, B)$ o conjunto dos homomorfismos de álgebras de A em B, e denota-se simplesmente $\mathrm{End}_K(A) := \mathrm{Hom}_K(A, A)$.

4. Sejam A uma álgebra e $I \subset A$ um ideal bilateral. Então a álgebra quociente A/I é um espaço vetorial sobre K, e também é naturalmente uma álgebra.

5. A é dito ser irredutível se os únicos ideais de A forem 0 e A.

6. Um ideal bilateral (à direita, à esquerda, respectivamente) $I \subset A$ é dito ser maximal se não for A e não estiver propriamente contido num ideal bilateral (à direita, à esquerda, respectivamente) diferente de A.

7. Um ideal bilateral (à direita, à esquerda, respectivamente) $I \subset A$ é dito ser minimal se não for nulo e não conter propriamente um ideal bilateral (à direita, à esquerda, respectivamente) não nulo.

8. Define-se o centro da álgebra por $Z(A) = \{z \in A : xz = zx, \forall x \in A\}$, o conjunto de todos os elementos que comutam com todos os elementos da álgebra.

9. Seja M um espaço vetorial sobre K e considere uma função $(m, a) \in M \times A \mapsto ma \in M$. Dizemos que M é um A-módulo (à direita) se essa operação satisfaz:

   (a) $\alpha(ma) = (\alpha m)a = m(\alpha a), \forall m \in M, \forall m \in M, \forall a \in A$,

   (b) $(m_1 + m_2)a = m_1 a + m_2 a, \forall m_1, m_2 \in M, \forall a \in A$,

   (c) $m(a_1 + a_2) = ma_1 + ma_2, \forall m \in M, \forall a_1, a_2 \in A$,

   (d) $m(a_1 * a_2) = (ma_1)a_2, \forall m \in M, \forall a_1, a_2 \in A$.

   Da mesma forma, definimos A-módulo à esquerda. Quando omitirmos o termo que indica o lado, entenderemos como "à direita".

10. Seja M um A-módulo. Dizemos que $S \subset M$ é um A-submódulo se S for subespaço vetorial e $sa \in S, \forall s \in S, \forall a \in A$.

11. Um A-módulo M é dito ser Noetheriano (Artiniano, respectivamente) se toda cadeia ascendente (descendente, respectivamente) de A-submódulos de M admite um elemento máximo (mínimo, respectivamente).

12. A é dito ser Noetheriano (Artiniano, respectivamente) se o for como um A-módulo à direita.

Vale ressaltar que, dada uma álgebra (associativa) A, um subconjunto $I \subset A$ que é ideal de A como anel, não necessariamente será ideal como álgebra. Isso não ocorre se A conter uma unidade 1, pois, neste caso, podemos ver o corpo K como subconjunto de A, e então, todos os ideais necessariamente serão subespaços vetoriais.

Definiremos um objeto muito importante nesta dissertação:

Definição 1.4.3. Seja $\mathscr{B}$ uma classe de álgebras (não necessariamente associativas) e seja F uma álgebra gerada por um conjunto X. Dizemos que F é uma **álgebra livre em** $\mathscr{B}$ se, para cada $A \in \mathscr{B}$ e cada função $f : X \to A$, existe um homomorfismo de álgebras $F \to A$ que extende f. Define-se o **posto** de F como sendo a cardinalidade do conjunto X.

Em particular, a álgebra de polinômios não comutativos é uma álgebra livre:

Teorema 1.4.4. *Para cada conjunto X, a álgebra $K\langle X\rangle$, espaço vetorial com base todas as palavras (associativas)*

$$x_{i_1} \cdots x_{i_n}, n \in \mathbb{N}, x_{i_1}, \cdots, x_{i_n} \in X$$

e multiplicação definido por justaposição:

$$(x_{i_1} \cdots x_{i_n})(x_{j_1} \cdots x_{j_m}) := x_{i_1} \cdots x_{i_n} x_{j_1} \cdots x_{j_m}$$

é uma álgebra livre na classe de todas as álgebras associativas unitárias sobre o corpo K. Define-se os múltiplos escalares das palavras como monômios. Se considerarmos o subespaço de $K\langle X\rangle$ gerado por todas as palavras de tamanho maior ou igual a 1, então obteremos a álgebra não-comutativa livre associativa, que será livre na classe de todas as álgebras associativas.

Definição 1.4.5. Dado um monômio $g = x_{i_1} \cdots x_{i_n} \in K\langle X\rangle$, definimos:

1. Para cada $x_i \in X$, define-se o grau de g em x_i por $\text{grau}_{x_i} g := \#\{j \in \{1, \cdots, n\} : x_i = x_{i_j}\}$, em que $\#$ representa a cardinalidade de um conjunto.

2. Define-se o grau de g, denotado por grau g, como a soma de todos os $\text{grau}_{x_i} g, x_i \in X$, não nulos.

3. Dado um polinômio $f \in K\langle X\rangle$, escreva $f = \sum_{i=1}^{l} g_i$ soma de monômios. Define-se o **grau** de f por:

$$\text{grau}_{x_i} f := \max\{\text{grau}_{x_i} g_1, \cdots, \text{grau}_{x_i} g_l\}, x_i \in X, \qquad \text{grau } f := \max\{\text{grau } g_1, \cdots, \text{grau } g_l\}.$$

4. Se $f = f(x_1, \cdots, x_m)$, define-se o **multigrau** de f pela sequência $(\text{grau}_{x_1} f, \cdots, \text{grau}_{x_m} f)$.

5. Se $f(x_1, \cdots, x_m) = \sum_{i=1}^{l} g_i$ é a decomposição de f como soma de monômios e se acontece de grau f = grau $g_i, \forall i = 1, \cdots, l$, então dizemos que f é homogêneo de grau d = grau f. Se ocorre ainda de $\text{grau}_{x_j} f = \text{grau}_{x_j} g_i, \forall i = 1, \cdots, l, \forall j = 1, \cdots, m$, então dizemos que f é multi-homogêneo de multigrau $(\text{grau}_{x_1} f, \cdots, \text{grau}_{x_m} f)$.

Daqui a diante, a menos que se diga o contrário, adotaremos as seguintes convenções:

1. Fixaremos o conjunto $X = \{x_1, x_2, \cdots\}$ com infinitos (enumerável) elementos, e $K\langle X\rangle$ será a álgebra não-comutativa livre associativa não-unitária gerada por X.

2. Denotaremos por $K\langle X_n\rangle$ ou $K\langle x_1, \cdots, x_n\rangle$ a álgebra livre não-comutativa associativa não-unitária de posto $n \in \mathbb{N}$.

3. Denominaremos $K\langle X\rangle$ de simplesmente "polinômios não-comutativos em infinitas variáveis" e $K\langle X_n\rangle$ de "polinômios não-comutativos em n variáveis", e denominaremos seus elementos por polinômios. Denotaremos por $f(x_1, \cdots, x_n) \in K\langle X\rangle$ um polinômio que aparece apenas os elementos $x_1, \cdots, x_n$. Em geral, usaremos outras letras inclusive para denominar elementos de X, como por exemplo, x, y, z, w...

4. A álgebra de Lie livre de posto infinito será denotado por $L(X)$, e a álgebra de Lie livre de posto finito n será denotado por $L(X_n)$ ou $L(x_1, \cdots, x_n)$, e denominaremos seus elementos de polinômios de Lie.

Por fim, enunciaremos o famoso teorema de Poincaré–Birkhoff–Witt, que diz que toda álgebra de Lie pode ser mergulhada numa álgebra associativa, e esse mergulho preserva representações.

Definição 1.4.6. Seja L uma álgebra de Lie. Dizemos que uma álgebra associativa $U \supset L$ é a **álgebra universal envelopante** se satisfaz a seguinte propriedade universal: Para toda álgebra associativa B e para todo homomorfismo de álgebras de Lie $\psi : L \to (B, [,])$ (considerando B como uma álgebra de Lie com respeito ao comutador $[a, b] := ab - ba$), existe um único homomorfismo de álgebras associativas $\phi : U \to B$ que estende ψ.

Teorema 1.4.7 (Poincaré–Birkhoff–Witt)**.** *Cada álgebra de Lie possui uma única (a menos de isomorfismo) álgebra universal envelopante $U(L)$. Se L admite uma base $\{x_i : i \in I\}$, assumindo uma ordenação total no conjunto I, temos que $U(L)$ terá como base os elementos*

$$e_{i_1} \cdots e_{i_n}, \quad n \in \mathbb{N}, i_1 \leq i_2 \leq \cdots \leq i_n$$

A demonstração desse teorema pode ser encontrado no livro [9] ou no livro [33] (e em vários outros).

Pode-se demonstrar que a álgebra universal envelopante da álgebra de Lie livre $L(X)$ é $K\langle X\rangle$:

Teorema 1.4.8 (Witt)**.** *A álgebra de Lie livre $L(X)$ é isomorfo a subálgebra de Lie de $(K\langle X\rangle, [,])$ gerada por X com respeito ao comutador, e $U(L(X)) = K\langle X\rangle$.*

A demonstração pode ser encontrada em [9].

Finalizaremos a subseção citando algumas propriedades de álgebras de Lie (em [33]):

1. Seja L uma álgebra de Lie. Então define-se a **álgebra derivada** de L, denotado por L' ou $[L, L]$ como o ideal de L gerado pelos elementos $\{[x, y] : x, y \in L\}$.

2. Seja $n \in \mathbb{N}$. Então, como álgebras de Lie, temos

   $$M_2(K) = \mathfrak{sl}(2, K) \oplus K$$

   em que identificamos K com as matrizes múltiplas (por escalar) da identidade. Ainda, pode-se facilmente verificar que:

   $$[M_2(K), M_2(K)] = \mathfrak{sl}(2, K)$$
   $$[\mathfrak{sl}(2, K), \mathfrak{sl}(2, K)] = \mathfrak{sl}(2, K)$$

1.4.1 PI-álgebras

Definiremos o objeto principal de estudo nesta dissertação: álgebras com identidade polinomial, ou simplesmente, PI-álgebras.

Definição 1.4.9. Seja A uma álgebra associativa. Dizemos que A é uma **álgebra com identidade polinomial**, ou simplesmente PI-álgebra, se existe um polinômio $f(x_1, \cdots, x_m) \in K\langle X\rangle$ tal que $f(a_1, \cdots, a_m) = 0$, para todo $a_1, \cdots, a_m \in A$. Neste caso, dizemos que $f(x_1, \cdots, x_m)$ é uma **identidade polinomial** de A, ou simplesmente f é uma identidade, e às vezes será conveniente dizer "a relação $f = 0$ é uma identidade de A".

Uma caracterização que muitas vezes é útil é a seguinte:

Lema 1.4.10. *Um polinômio $f \in K\langle X\rangle$ é uma identidade de uma álgebra A se e só se para todo homomorfismo de álgebras $\psi : K\langle X\rangle \to A$, tem-se $\psi(f) = 0$.*

A demonstração segue direto da propriedade universal de álgebras livres (da possibilidade de estender funções).

Exemplo:

1. *Uma álgebra A é comutativa se e só se satisfaz a identidade $[x_1, x_2] = 0$.*

2. *Define-se o polinômio **standard** por*

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

3. *Define-se o **polinômio de Capelli** por*

$$d_n(x_1, \cdots, x_n, y_1, \cdots, y_{n+1}) = \sum_{\sigma \in S_n} (-1)^\sigma y_1 x_{\sigma(1)} y_2 x_{\sigma(2)} \cdots y_n x_{\sigma(n)} y_{n+1}$$

4. *Qualquer álgebra de dimensão finita satisfaz alguma identidade standard e alguma identidade de Capelli. De fato, ambas são antissimétricas nas variáveis $x_1, \cdots, x_n$, e então, sendo a dimensão da álgebra finita m, temos que A satisfaz toda identidade standard s_n e toda identidade de Capelli d_n, com $n > m$.*

5. *Podemos escrever a identidade standard de grau 4 na forma:*

$$s_4(x_1, x_2, x_3, x_4) = \frac{1}{2} \sum_{\sigma \in S_3} -(-1)^\sigma [x_4, x_{\sigma(1)}] \circ [x_{\sigma(2)}, x_{\sigma(3)}]$$

   como pode ser verificado diretamente, em que $a \circ b := ab + ba$ é o produto simétrico, definido em qualquer álgebra associativa.

   Nessa representação, vemos que $M_2(K)$ satisfaz a identidade standard de grau 4, pois $\{e_{11} + e_{22}, e_{12}, e_{21}, e_{22}\}$ é uma base de $M_2(K)$, sendo e_{ij} a matriz que possui 1 na entrada de linha i e coluna j, e 0 nas demais entradas. Mas $e_{11} + e_{22}$ é a matriz identidade, ela comuta com toda matriz, e portanto anula os comutadores. Logo sobram somente três matrizes para substituir numa soma alternada de 4 elementos. Mas então a soma vai zerar.

6. *O* ***polinômio de Hall*** *é definido por*

$$[[x_1, x_2]^2, x_3]$$

e temos que $M_2(K)$ satisfaz essa identidade também. De fato, dada qualquer matriz $A \in M_2(K)$, utilizando o Teorema de Cayley–Hamilton, sabemos que o polinômio característico p de A anula a matriz A. Sabemos também que o polinômio característico é dado por $p(x) = x^2 - tr(A)x + det(A)$. Ainda, por propriedades do traço, temos que

$$tr([A, B]) = tr(AB) - tr(BA) = 0$$

e então, para quaisquer $A, B \in M_2(K)$, segue que $tr([A, B]) = 0$. Daí, por Cayley–Hamilton e pela forma do polinômio característico, $[A, B]^2 = -det([A, B])I$, sendo $I \in M_2(K)$ a matriz identidade, e em particular, $[A, B]^2$ é uma matriz escalar e comuta com qualquer outra matriz, o que implica $[[A, B]^2, C] = 0$, ou seja, $M_2(K)$ satisfaz a identidade $[[x_1, x_2]^2, x_3] = 0$.

7. *Algumas características de álgebras podem ser postas por meio de identidades polinomiais, por exemplo:*

   (a) *Uma álgebra A é nil de índice finito menor ou igual a n ($n \in \mathbb{N}$) se e só se A satisfaz a identidade polinomial $x^n = 0$.*

   (b) *Uma álgebra é nilpotente de índice menor ou igual a n ($n \in \mathbb{N}$) se e só se A satisfaz a identidade polinomial $x_1 \cdots x_n = 0$.*

□

A seguir, iremos discutir as principais ideias para se estudar as identidades de uma álgebra:

Definição 1.4.11. Seja $T \subset K\langle X\rangle$ um subconjunto não vazio, com X sendo finito, ou infinito. Dizemos que T é um **T-ideal**, se for um ideal bilateral de $K\langle X\rangle$, e se, para todo homomorfismo de álgebras $f : K\langle X\rangle \to K\langle X\rangle$, tivermos $f(T) \subset T$.

Exemplo: *Dizer que um subconjunto $T \subset K\langle X\rangle$ é um ideal é o mesmo que dizer que ele é fechado por multiplicações à direita e à esquerda. O conceito intuitivo de T-ideal é que, além disso, dado qualquer polinômio $f(x_1, x_2, \cdots, x_m) \in T$ e quaisquer polinômios $g_1, g_2, \cdots, g_m \in K\langle X\rangle$, temos $f(g_1, g_2, \cdots, g_m) \in T$, ou seja, os polinômios de T continuam em T se trocarmos suas entradas por polinômios.* □

Definição 1.4.12. Seja $F \subset K\langle X\rangle$ não vazio. Definimos o T-ideal de $K\langle X\rangle$, gerado por F, como sendo o menor T-ideal contendo F, e denota-se por $T(F)$ ou $\langle F\rangle$. Se $F = \{f_1, \cdots, f_n\}$, denota-se também por $T(f_1, \cdots, f_n)$ ou $\langle f_1, \cdots, f_n\rangle^T$. Dados $f, g \in K\langle X\rangle$, dizemos que o polinômio g é **consequência** de f (ou "segue de f", ou "f implica g") se $f \in \langle g\rangle^T$. Dizemos que f e g são **equivalentes** se f é consequência de g e g é consequência de f.

Na prática, um polinômio g será consequência de f se podemos obter g a partir de combinação linear de substituição de variáveis de f por polinômios e multiplicações por polinômios à direita e à esquerda.

Exemplo: *A identidade standard s_{n+1} é consequência de s_n. De fato, temos*

$$s_{n+1}(x_1, \cdots, x_{n+1}) = \sum_{i=1}^{n+1} (-1)^{1+i} x_i s_n(x_1, \cdots, \hat{x}_i, \cdots, x_{n+1})$$

em que $\hat{x}_i$ indica omissão de variável, ou seja, estamos considerando a identidade standard s_n nas variáveis $x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n$. □

Definição 1.4.13. Seja $\mathscr{B}$ uma classe de álgebras (não necessariamente associativas). Dizemos que $\mathscr{B}$ é uma **variedade** se existe um subconjunto $\mathscr{F} \subset K\langle X\rangle$ tal que vale a seguinte propriedade: uma álgebra A está em $\mathscr{B}$ se e só se A satisfaz todas as identidades de $\mathscr{F}$.

Um subconjunto $\mathscr{N} \subset \mathscr{B}$ é dito ser subvariedade se for não vazio e se for uma variedade.

Definição 1.4.14. Dado $\mathscr{F} \subset K\langle X\rangle$ um subconjunto, define-se a **variedade gerada** por $\mathscr{F}$ como sendo a classe de todas as álgebras que satisfazem todos os polinômios em $\mathscr{F}$, e dizemos que $\mathscr{M}$ é gerada por $\mathscr{F}$.

Dada uma variedade $\mathscr{M}$, dizemos que $\mathscr{M}$ admite base finita se existir $\mathscr{F} \subset K\langle X\rangle$ finito tal que $\mathscr{F}$ gera a variedade $\mathscr{M}$.

Dizemos que uma variedade $\mathscr{M}$ satisfaz a **propriedade de Specht** se toda subvariedade de $\mathscr{M}$ (incluindo o próprio $\mathscr{M}$) admite base finita.

Observação.

1. As noções de identidades polinomiais, T-ideal, variedades, e propriedade de Specht podem ser definidas de forma análoga para álgebras de Lie.

2. O problema de verificar se toda variedade admite base finita foi proposto por Specht em 1950 (vide [43]) (antes disso, B. H. Neumann havia feito a mesma pergunta para grupos em sua tese em 1935). Então, esse problema e propriedade ficaram conhecidos com o nome de Specht.

3. Em 1987, em uma série de publicações profundas e de grande impacto, Kemer respondeu positivamente o problema de Specht para o caso de álgebras associativas sobre corpos de característica zero.

4. Para o caso de variedades de Lie, o primeiro contra-exemplo para a propriedade de Specht foi dado por Vaughan-Lee em 1970 (vide [44]), para o caso de característica $p = 2$. Para o caso de característica $p > 0$ qualquer, um contra-exemplo foi dado por Drensky em 1974 (vide para a construção detalhada [9]). O caso de característica 0 foi considerado por Iltyakov, ele demonstrou que toda variedade gerada por uma álgebra de Lie de dimensão finita, satisfaz a propriedade de Specht. O resultado de Iltyakov é bem mais abrangente que o enunciado aqui, referimos os leitores para [16]. Ressaltamos que uma resposta positiva (ou negativa) para o problema de Specht para álgebras de Lie em característica 0 ainda não é conhecida.

O próximo resultado é fácil de ser demonstrado, e segue direto da propriedade universal de $K\langle X\rangle$:

Proposição 1.4.15. *Seja $\mathscr{M}$ uma variedade e considere o conjunto $T(\mathscr{M})$ constituído de todas as identidades que são satisfeitas por todas as álgebras de $\mathscr{M}$. Então $T(\mathscr{M})$ é um T-ideal.*

Daqui em diante, utilizaremos a seguinte notação: dado $\mathscr{M}$ uma variedade, definimos $T(\mathscr{M})$ como sendo o T-ideal de todas as identidades satisfeitas por todas as álgebras em $\mathscr{M}$. Dada uma PI-álgebra A, denotamos por $T(A)$ o T-ideal de todas as identidades satisfeitas por A.

Foi demonstrado que, dada uma variedade, o conjunto das identidades satisfeitas pelos elementos dessa álgebra é um T-ideal. A volta dessa afirmação vale, isto é, dado um T-ideal T, existe pelo menos uma álgebra F tal que $T(F) = T$.

Definição 1.4.16. Seja $\mathscr{M}$ uma variedade. Uma álgebra F é dita ser **relativamente livre em $\mathscr{M}$** se F for livre na classe $\mathscr{M}$.

Teorema 1.4.17. *Seja T um T-ideal. Então, existe uma álgebra livre F de posto infinito tal que $T(F) = T$.*

Demonstração. A construção é fácil e é feita da seguinte maneira: basta considerarmos a álgebra $F = K\langle X\rangle/T$, com X infinito. □

Observação. Considere F_n e F as álgebras relativamente livres contruídas nessa última demonstração. Então, é fácil ver que toda álgebra A que é imagem homomorfica dessas álgebras (isto é, existe $f : F \to A$ homomorfismo de álgebras sobre) é uma PI-álgebra, e $T(A) \supset T$ (sendo T o conjunto sobre o qual F e F_n foram construídos). Reciprocamente, se A é uma PI-álgebra com $T(A) \supset T$, então existem uma álgebra relativamente livre F, com $T(F) = T$, e $f : F \to A$ homomorfismo de álgebras sobre.

Daqui para frente, adotaremos a seguinte notação: para cada $n \in \mathbb{N}$ e dada uma variedade $\mathscr{M}$, denotaremos por $T_n(\mathscr{M}) := T(\mathscr{M}) \cap K\langle x_1, \cdots, x_n\rangle$. Da mesma forma, definimos $T_n(A) := T(A) \cap K\langle x_1, \cdots, x_n\rangle$, para A uma PI-álgebra.

Exemplo:

1. *A classe de todas as álgebras associativas comutativas é denominada de* ***variedade abeliana*** *e denotada por $\mathscr{A}$.*
2. *A classe de todas as álgebras associativas que são nilpotentes de um índice fixo $n \in \mathbb{N}$ é denominada de* ***variedade nilpotente de índice*** *n e é denotada por $\mathscr{N}_n$.*

□

Uma construção muito útil envolvendo variedades é o denominado produto de variedades:

Definição 1.4.18. Sejam $\mathscr{M}$ e $\mathscr{N}$ duas variedades. Definimos a variedade produto $\mathscr{M}\mathscr{N}$ por: uma álgebra A está na variedade produto $\mathscr{M}\mathscr{N}$ se e só se existe um ideal bilateral $I \subset A$ tal que $I \in \mathscr{M}$ e $A/I \in \mathscr{N}$.

Não iremos discutir aqui mais detalhes sobre essa construção, e para mais detalhes, indicamos o livro de Bahturin [5].

Por fim, finalizaremos enunciando algumas relações entre álgebras de Lie e suas identidades (nem todas são triviais de serem demonstradas, e outras podem servir como definição dos termos apresentados):

1. Uma álgebra de Lie é dita ser nilpotente se existe $n \in \mathbb{N}$ tal que L satisfaz a identidade $[x_0, x_1, \cdots, x_n] = 0$.
2. Para cada $n \in \mathbb{N}$, defina indutivamente o polinômio seguinte:

   $$\delta_n(x_1, \cdots, x_{2^n}) := [\delta_{n-1}(x_1, \cdots, x_{2^{n-1}}), \delta_{n-1}(x_{2^{n-1}+1}, \cdots, x_{2^n})]$$
   $$\delta_1(x_1, x_2) := [x_1, x_2]$$

   Uma álgebra de Lie é solúvel se existe $n \in \mathbb{N}$ tal que L satisfaz a identidade δ_n.

   Em linguagem não de identidades, defina a n-ésima derivada de L indutivamente por:

   $$L^{(1)} := [L, L]$$
   $$L^{(n)} := [L^{(n-1)}, L^{(n-1)}]$$

   então L é solúvel se e só se existe $n \in \mathbb{N}$ tal que $L^{(n)} = 0$.

3. Pode se mostrar que uma álgebra de Lie L é solúvel se e só se existe um ideal nilpotente $I \subset L$ tal que L/I é abeliano (essa afirmação é equivalente a álgebra derivada L' ser nilpotente). Então, L é solúvel se e só se L está no produto de uma variedade nilpotente com uma variedade abeliana.

§1.5 Produto Tensorial

Nesta seção, apresentaremos a definição de produto tensorial. Para mais detalhes, consultar os livros de Northcott [27] ou Rotman [32].

O conceito de produto tensorial pode ser apresentado com uma abordagem muito formal e, a princípio, pouco intuitiva, mas, pode ser encarado informalmente como uma "multiplicação" entre dois espaços (ou módulos). No caso dos módulos admitirem base livre, fica fácil manipular os elementos do produto tensorial entre eles.

Definiremos produto tensorial para R-módulos, e obteremos, como casos particulares, produto tensorial entre espaços vetoriais (módulos sobre corpos), produto tensorial entre anéis (todo anel é um $\mathbb{Z}$-módulo), e produto tensorial entre álgebras.

Definição 1.5.1. Sejam M um R-módulo à direita, N um R-módulo à esquerda, $(G, +)$ um grupo abeliano e $f : M \times N \to G$ uma função. Dizemos que f é R-bilinear se:

(i) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n), \forall m_1, m_2 \in M, \forall n \in N$,

(ii) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2), \forall m \in M, \forall n_1, n_2 \in N$,

(iii) $f(mr, n) = f(m, rn), \forall m \in M, \forall n \in N, \forall r \in R$.

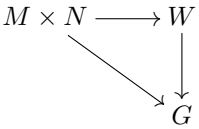
Citamos dois exemplos importantes:
Exemplo:

1. *A aplicação $(A, B) \in M_n(K) \times M_n(K) \mapsto tr(AB) \in K$ é K-bilinear.*
2. *Seja R um anel. Então, a aplicação $(r, s) \in R \times R \mapsto rs \in R$ é R-bilinear.*

□

O próximo resultado caracteriza o produto tensorial por meio de uma propriedade Universal. A demonstração pode ser encontrada nos livros referenciados.

Teorema 1.5.2. *Sejam M um R-módulo à direita, N um R-módulo à esquerda e $(G, +)$ um grupo abeliano. Então, existe um único par (a menos de isomorfismo) (W, i), com W grupo abeliano e $i : M \times N \to W$ R-bilinear tal que, para toda aplicação R-bilinear $f : M \times N \to G$, existe um único homomorfismo de grupos $\bar{f} : W \to G$ tal que $\bar{f} \circ i = f$, em diagrama:*



Definição 1.5.3. Denominamos o par (W, i) de produto tensorial entre M e N. Denotamos $W = M \otimes_R N$ e para cada $m \in M, n \in N$, denotamos $m \otimes n := i(m, n)$.

Observação. 1. Nem sempre $M \otimes_R N = \{m \otimes n : m \in M, n \in N\}$, mas, esse conjunto gera $M \otimes_R N$.

2. No caso geral, dado $m \neq 0$ e $n \neq 0$, podemos ter $m \otimes n = 0$. De fato, um exemplo é considerar os $\mathbb{Z}$-módulos $\mathbb{Z}_2$ e $\mathbb{Z}_3$. Temos $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0$ (escreva $1 = 2 \cdot 2 + 3 \cdot (-1)$ e utilize a bilinearidade para concluir que $m \otimes n = 0, \forall m \in \mathbb{Z}_2, \forall n \in \mathbb{Z}_3$. Uma outra forma de concluir isso é utilizar a propriedade universal: mostre que toda $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \to G$ $\mathbb{Z}$-bilinear é nula (com mesmo argumento do caso anterior) e daí, 0 é um produto tensorial entre $\mathbb{Z}_2$ e $\mathbb{Z}_3$, e segue pois o produto tensorial é único).

A patologia citada na observação 2 não ocorre se os módulos são livres e R é comutativo, mas, antes, mostraremos que podemos obter módulos como produto tensorial:

Teorema 1.5.4. *Sejam M um (S, R)-bimódulo e N um R-módulo à esquerda. Então, $M \otimes_R N$ é um S-módulo à esquerda, com a ação*

$$s(m \otimes n) := (sm) \otimes n, s \in S, m \in M, n \in N.$$

Se M é um R-módulo à direita e N é um (R, S)-bimódulo, então $M \otimes_R N$ é um S-módulo à direita, com a ação

$$(m \otimes n)s := m \otimes (ns), s \in S, m \in M, n \in N.$$

A demonstração desse último teorema não é difícil. Como consequência obtemos:

Corolário 1.5.5. *(i) Se M é um (S, R)-bimódulo e N um (R, T)-bimódulo, com R, S, T anéis, então $M \otimes_R N$ é um (S, T)-bimódulo.*

(ii) Se R é comutativo, então todo R-módulo é um R-bimódulo. Em particular, se M e N forem R-módulos, então $M \otimes_R N$ será R-módulo.

(iii) Sejam R anel comutativo e M, N R-módulos. Então, $M \otimes_R N \simeq N \otimes_R M$ como R-módulos.

(iv) Sejam R anel comutativo e M_1, M_2, M_3 R-módulos. Então

$$(M_1 \otimes_R M_2) \otimes_R M_3 \simeq M_1 \otimes_R (M_2 \otimes_R M_3)$$

como R-módulos.

Teorema 1.5.6. *Sejam R anel comutativo, M um R-módulo livre com base livre $\{m_\alpha\}_{\alpha \in I}$ e N um R-módulo livre com base livre $\{n_\beta\}_{\beta \in J}$. Então $M \otimes_R N$ é R-módulo livre com base livre $\{m_\alpha \otimes n_\beta\}_{(\alpha,\beta) \in I \times J}$.*

A demonstração desse último teorema pode ser encontrada em [27].

Por fim, podemos obter anéis como produto tensorial:

Teorema 1.5.7. *Sejam R e S anéis. Então $R \otimes_{\mathbb{Z}} S$ é anel, com o produto:*

$$(r_1 \otimes s_1)(r_2 \otimes s_2) = (r_1 r_2) \otimes (s_1 s_2)$$

A demonstração desse resultado por ser obtido diretamente (com auxílio dos resultados anteriores). De forma análoga, obtemos:

Teorema 1.5.8. *Sejam A e B K-álgebras. Então $A \otimes_K B$ é K-álgebra.*

Uma construção muito importante é a extensão do corpo base de espaços vetoriais (ou álgebras), que pode ser formalizado por meio de produto tensorial:

Teorema 1.5.9. *Sejam $L|K$ uma extensão de corpos e A um espaço vetorial (ou álgebra) sobre K. Então $A \otimes_K L$ á um espaço vetorial (ou álgebra) sobre L. Ainda, $dim_L A = dim_K A$ e se $\{v_\alpha\}_{\alpha \in I}$ é base de A sobre K, então $\{v_\alpha \times 1\}_{\alpha \in I}$ é base de $A \otimes_K L$ sobre L.*

Esse último teorema formaliza a ideia de, quando estamos trabalhando num espaço vetorial, muitas vezes é útil considerar o mesmo espaço sobre um corpo maior (no caso trabalharmos com espaços vetoriais reais, e considerarmos o espaço sobre os complexos, denomina-se também de complexificação). Essa técnica é muito útil quando nos deparamos com problemas de diagonalização, e é muito conveniente utilizá-la em álgebras, uma vez que muitas propriedades envolvendo o produto da álgebra é preservada (ainda, por ambas álgebras admitirem "a mesma base", o produto é praticamente preservado).

Exemplo: *Seja $L|K$ extensão de corpos. Então, como pode ser verificado diretamente, $M_n(K) \otimes_K L \simeq M_n(L)$.* □

§1.6 Teoria de Representações

Nesta seção, apresentaremos definições básicas de representações de grupos e o importantíssimo Teorema de Maschke. A exposição será baseada no livro de Serre [35].

A ideia de teoria de representações é estudar objetos abstratos (grupos, no caso) por meio de objetos mais conhecidos e palpáveis (matrizes). Para o resto desta seção, fixe G um grupo finito. Dado V um espaço vetorial, denote por $\mathrm{Gl}(V) = (\text{automorfismos de } V) = \{T : V \to V \text{ transformação linear 1-1 e sobre}\}$.

Definição 1.6.1. Uma **representação** de G em V é um homomorfismo de grupos $\rho : G \to \mathrm{Gl}(V)$. O grau da representação é definido como $\dim V$, e denomina-se representação finita se o grau for finito. Utilizaremos a notação $\rho_s := \rho(s)$, para cada $s \in G$, e diremos simplesmente "representação V" ao invés de "representação $\rho : G \to \mathrm{Gl}(V)$". Denomina-se também V de o **espaço de representação** de G.

Exemplo:

1. *Considere $\rho : G \to Gl(V)$, com V qualquer espaço vetorial não nulo, dado por $\rho(s) = I$, para todo $s \in G$, sendo I a matriz identidade. Essa representação é denominada* ***representação trivial****.*

2. *Seja θ um ângulo racional (isto é, $\frac{2\pi}{\theta} \in \mathbb{Q}$). Então, a associação de θ à rotação do plano pelo ângulo θ é uma representação do grupo $\mathbb{Z}_n$ ($\simeq \{0, \theta, 2\theta, \cdots, n\theta(= 2k\pi)\}$) dos ângulos módulo 2π. Mais precisamente, a representação é dada por*

$$m\theta \mapsto \begin{pmatrix} cos\, m\theta & -sen\, m\theta \\ sen\, m\theta & cos\, m\theta \end{pmatrix} \in Gl(V)$$

em que V é espaço vetorial de dimensão 2 sobre um corpo K.

3. *Seja* $V = K^n$ *e, para cada* $i = 1, \cdots, n$, *defina* $e_i = (0, \cdots, 0, \underbrace{1}_{i\text{-ésima entrada}}, 0, \cdots, 0)$ *os vetores canônicos. Considere* $G = S_n$ *o grupo de permutações de* n *elementos. Então, existe uma ação natural de* G *sobre* V *dado, nos elementos da base, por*

$$\sigma(e_i) = e_{\sigma(i)}, i = 1, \cdots, n, \sigma \in S_n$$

e estendemos a ação para V *por linearidade, isto é,* $\sigma(a_1e_1 + \cdots + a_ne_n) = a_1e_{\sigma(1)} + \cdots + a_ne_{\sigma(n)}$, $a_1, \cdots, a_n \in K$. *Temos* σ *invertível, com inversa* $\sigma^{-1} \in S_n$. *Então, isso gera naturalmente uma representação* $S_n \to Gl(K^n)$.

4. *Mais geralmente, assuma* X *um conjunto finito e* G *um grupo que age sobre* X, *isto é, todo* $\sigma \in G$ *é uma aplicação* $\sigma : X \to X$ *tal que:*

   (a) $\sigma(\tau(x)) = (\sigma\tau)(x), \forall \sigma, \tau \in G, \forall x \in X$,

   (b) $1(x) = x, \forall x \in X$, *sendo* $1 \in G$ *o elemento neutro.*

   Note que cada $g \in G$ *age como permutação dos elementos de* X, *pois* $gg^{-1}x = g^{-1}gx = x, \forall x \in X$, *e então,* $g : X \to X$ *é invertível. Considere o espaço vetorial formal sobre* K *com base* X, *isto é, considere elementos* $\{e_x\}_{x \in X}$ *e tome o espaço* $V_X = \{a_1e_{x_1} + \cdots + a_ne_{x_n} : a_1, \cdots, a_n \in K\}$, *em que denotamos por* $X = \{x_1, \cdots, x_n\}$. *Temos* $V_X \simeq K^n$, *e cada* $g \in G$ *admite uma ação em* V_X, *dada pelos elementos da base por* $g(e_x) = e_{g(x)}, g \in G, x \in X$. *Daí, obtemos representação* $G \to Gl(V_X)$.

5. *Um caso particular e muito importante do exemplo anterior é o conhecido como* ***representação regular***. *Seja* G *um grupo. Então, os elementos de* G *agem sobre o próprio grupo* G *pelo produto.*

   Seja V_G *o espaço vetorial formal com base* $\{e_g\}_{g \in G}$ *e considere a ação de* G *sobre* V_G *dado por* $ge_h = e_{gh}, g, h \in G$. *Então, temos naturalmente uma representação* $G \to Gl(V_G)$.

6. *Sejam* $\rho_1 : G \to GL(V_1)$ *e* $\rho_2 : G \to GL(V_2)$ *duas representações. Então, define-se o* ***produto tensorial de representações*** ρ_1 *e* ρ_2 *por* $\rho_1 \otimes \rho_2 : G \to GL(V_1 \otimes V_2)$ *em que, dados* $v_1 \otimes v_2 \in V_1 \otimes V_2$ *e* $g \in G$,

$$(\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2) := (\rho_1(g)(v_1)) \otimes (\rho_2(g)(v_2))$$

□

O espaço V_G construído no exemplo anterior é muito importante e tem um nome e notação própria:

Definição 1.6.2. Seja G um grupo. A **álgebra de grupo de** G **sobre** K, denotada por KG, é o espaço vetorial formal sobre K com base $\{e_g\}_{g \in G}$, com o produto definido na base por $e_ge_h = e_{gh}, g, h \in G$. Muitas vezes, denotaremos os elementos da base pelos elementos do grupo, ou seja, usamos $g := e_g \in KG$.

Representações de um grupo G e KG-módulos estão ligados, e, antes de mostrarmos a conexão, apresentaremos mais alguns conceitos:

Definição 1.6.3. Seja $\rho : G \to \mathrm{Gl}(V)$ uma representação. Um subespaço $W \subset V$ é dito ser uma subrepresentação se $\rho_s(W) \subset W, \forall s \in G$, ou seja, se $\rho_s(w) \in W, \forall s \in G, \forall w \in W$.

Note que dados uma representação $\rho : G \to \mathrm{Gl}(V)$ e $W \subset V$ uma subrepresentação, temos $\rho_s|_W \in \mathrm{Gl}(W), \forall s \in G$, e daí, $\rho : G \to \mathrm{Gl}(W)$ é uma representação.

Exemplo: *Seja G um grupo e considere a representação regular $\rho : G \to Gl(KG)$. Considere $W = \langle e \rangle$, o subespaço gerado por $e = \sum_{g \in G} e_g$. Temos que W é uma subrepresentação de KG, e se comporta como a representação trivial, pois $\rho_s(e) = e, \forall s \in G$.* □

Como não estamos interessados em considerar como diferentes duas representações que se comportam da mesma forma, mudando apenas a natureza dos objetos e o modo de definir as ações, vamos definir formalmente um conceito de equivalência entre representações:

Definição 1.6.4. Sejam G grupo e $\rho_1 : G \to \mathrm{Gl}(V_1)$ e $\rho_2 : G \to \mathrm{Gl}(V_2)$ duas representações. Dizemos que ρ_1 e ρ_2 são equivalentes (ou isomorfas) se existe $T : V_1 \to V_2$ isomorfismo tal que $T \circ \rho_1(s) = \rho_2(s) \circ T, \forall s \in G$. Isso equivale ao seguinte diagrama ser comutativo para todo $s \in G$:

$$\begin{array}{ccc} V_1 & \longrightarrow & V_1 \\ \downarrow & & \downarrow \\ V_2 & \longrightarrow & V_2 \end{array}$$

Informalmente, a transformação linear $T : V_1 \to V_2$ associa os elementos de tal forma que a ação da representação ρ_1 sobre $x \in V_1$ age da mesma forma que ρ_2 age sobre $T(x) \in V_2$. Podemos "transitar" entre os espaços V_1 e V_2 (através de T), e a ação de ρ_1 ou ρ_2 (dependendo do espaço que estivermos), terá o mesmo efeito.

Exemplo: *A representação trivial é isomorfa à representação W, do último exemplo.* □

Um importantíssimo teorema é o conhecido como Teorema de Maschke.

Teorema 1.6.5. *Sejam G um grupo finito e K um corpo de característica zero ou $p > 0$ tal que p não divide $|G|$. Sejam $\rho : G \to Gl(V)$ uma representação finita e $W \subset V$ uma subrepresentação. Então, existe $W_0 \subset V$ uma subrepresentação tal que $V = W \oplus W_0$.*

Demonstração. Seja W' um subespaço qualquer de V tal que $V = W \oplus W'$, e considere a projeção $\pi : W \oplus W' \to W$. Defina $\pi_0 = \frac{1}{g} \sum_{s \in G} \rho_s^{-1} \pi \rho_s$, em que g é a quantidade de elementos no grupo G. Temos π_0 projeção, pois $\pi_0(V) \subset W$ e se $w \in W$, então $\rho_s(w) \in W, \forall s \in G$, e

$$\pi_0(w) = \frac{1}{g} \sum_{s \in G} \rho_s^{-1}(\underbrace{\pi(\rho_s(w))}_{\rho_s(w)}) = \frac{1}{g} \sum_{s \in G} w = w$$

e daí $\pi_0^2 = \pi_0$. Ainda, $\pi_0(V) = W$. Segue que $V = W \oplus \operatorname{Ker} \pi_0$, e mostraremos que $\operatorname{Ker} \pi_0$ é subrepresentação de V.

Claro que $\rho_s^{-1} \pi_0 \rho_s = \pi_0, \forall s \in G$, e daí, em particular, $\pi_0 \rho_s = \rho_s \pi_0, \forall s \in G$. Dado $x \in \operatorname{Ker} \pi_0$, temos $\pi_0(\rho_s(x)) = \rho_s(\pi_0(x)) = 0$, e daí, $\rho_s(x) \in \operatorname{Ker} \pi_0$. Segue que $\rho_s(\operatorname{Ker} \pi_0) \subset \operatorname{Ker} \pi_0, \forall s \in G$, e daí $\operatorname{Ker} \pi_0$ é subrepresentação, o que conclui o resultado. □

Note que $\rho : G \to \mathrm{Gl}(V)$ é totalmente determinado pelas subrepresentações $\rho_W : G \to \mathrm{Gl}(W)$ e $\rho_{W_0} : G \to \mathrm{Gl}(W_0)$, isto é, existe uma base de V tal que $\forall s \in G$, tem-se as matrizes

$$[\rho_s] = \begin{pmatrix} [\rho_W(s)] & 0 \\ 0 & [\rho_{W_0}(s)] \end{pmatrix}.$$

Isso motiva a definição seguinte:

Definição 1.6.6. Sejam $\rho_1 : G \to \mathrm{Gl}(V_1)$ e $\rho_2 : G \to \mathrm{Gl}(V_2)$ duas representações. A **soma direta** dessas representações é a representação $\rho_1 \oplus \rho_2 : G \to \mathrm{Gl}(V_1 \oplus V_2)$ dado por

$$\rho_1 \oplus \rho_2(s)(v_1 + v_2) = \rho_1(s)(v_1) + \rho_2(s)v_2, s \in G, v_1 \in V_1, v_2 \in V_2.$$

Definição 1.6.7. Dada uma representação $\rho : G \to \mathrm{Gl}(V)$, dizemos que V é **irredutível** se não admite subrepresentações diferentes de 0 e V.

O teorema de Maschke mostra que toda representação que admite uma subrepresentação é a soma direta de duas representações. Podemos dizer ainda mais: dada uma representação $\rho : G \to \mathrm{Gl}(V)$, então V é irredutível ou existe subrepresentação $W \subset V$, com W não nulo e diferente de V. Daí, ou ρ é irredutível ou ρ se escreve como $V = W \oplus W'$ (estamos abusando e facilitando a notação). Podemos repetir o processo para W e W' (o processo terminará, pois a dimensão de V é finita, por hipótese), e concluiremos que V é soma direta de representações irredutíveis, isto é:

Corolário 1.6.8. *Se $|G| < \infty$ e o corpo base tem característica p tal que $p = 0$ ou p não divide $|G|$ então toda representação de grau finito de G é soma direta de representações irredutíveis.*

Estudaremos mais profundamente a decomposição de uma representação com o auxílio do Teorema de Wedderburn-Artin.

Por fim, iremos relacionar KG-módulos com representações de G:

Lema 1.6.9. *Sejam G grupo e V espaço vetorial sobre K.*

(i) Uma representação $\rho : G \to Gl(V)$ induz uma estrutura de KG-módulo em V (V como espaço vetorial, mais precisamente, (KG, K)-módulo), dado por:

$$\left(\sum_{g \in G} \alpha_g g\right) v := \sum_{g \in G} \alpha_g \rho_g(v), v \in V.$$

(ii) Um KG-módulo à esquerda V (mais precisamente um (KG, K)-bimódulo V) induz uma representação $\rho : G \to Gl(V)$, definido por $\rho_g(v) := gv, \forall v \in V, \forall g \in G$.

(iii) Seja $W \subset V$ subespaço vetorial, $\rho : G \to Gl(V)$ representação, e considere V como KG-módulo, de modo que as ações coincidem (no sentido de (i) ou (ii)). Então

(a) W é subrepresentação de ρ se e só se W é (KG)-submódulo de V,

(b) W é subrepresentação irredutível se e só se W é (KG)-submódulo irredutível.

Capítulo 2

Teoria clássica de Álgebras

Neste capítulo, serão apresentados algumas noções da teoria e linguagem clássica da álgebra não comutativa (e algumas poucas coisas da álgebra comutativa e álgebras de Lie) que serão importantes na demonstração de um dos resultados principais deste trabalho. Este capítulo será interessantíssimo, pelo fato de que muito da teoria clássica da álgebra não comutativa casa bem com a teoria de identidades polinomiais.

§2.1 Anéis Primitivos

Nesta seção, apresentarei algumas noções da teoria clássica sobre anéis primitivos. Basicamente, um anel primitivo é um anel de matrizes $M_n(D)$ sobre um anel de divisão D, ou pode ser um "subconjunto grande" de "matrizes infinitas" sobre um anel de divisão; os conceitos formais serão apresentados adiante. Usando-se a linguagem das transformações lineares e não a das matrizes, os anéis primitivos são anéis de operadores lineares em espaços vetoriais (sobre anel de divisão), que contêm muitos operadores. A exposição seguirá o livro de I. Herstein (vide [20]).

Apresentarei essencialmente 3 definições sobre anéis primitivos:

i. Uma definição intrínseca e abstrata, mas será de grande importância, por ser uma caracterização indireta.

ii. Definição de como um anel primitivo pode agir sobre um grupo abeliano: será importante para interligar as outras duas noções.

iii. Uma definição de estrutura (anel de matrizes ou "subconjunto grande" de "anel de matrizes infinito").

Esta caracterização indireta, unida com a noção de produto subdireto será de grande importância no estudo e entendimento de PI-álgebras.

Começaremos com uma definição e caracterização de ideal primitivo. Mas antes, vale relembrar a noção de ideal modular:

Definição 2.1.1. Seja R um anel. Um ideal $I \lhd_r R$ é dito **modular** se existe $x \in R$ tal que $xa - a \in I$ para todo $a \in R$.

Observação. Vale ressaltar que, se R admite unidade 1, então todo ideal é modular, pois neste caso, $1 \in R$ é tal que $1a - a = 0 \in I$, para todo $a \in R$.

Definição 2.1.2. Sejam R um anel e $I \lhd R$ um ideal bilateral. Dizemos que I é **primitivo** se existe $M \lhd_r R$ ideal maximal modular tal que $I \subset M$ e I é o maior ideal bilateral contido em M.

Lema 2.1.3. *$I \lhd R$ é primitivo se e somente se existe $M \lhd_r R$ maximal modular tal que vale $I = (M : R) := \{x \in R : Rx \subset M\}$.*

Demonstração. Assuma I primitivo e $M \lhd_r R$ maximal modular com $I \subset M$, segundo a definição de ideal primitivo, e considere $J = \{x \in R : Rx \subset M\}$. Claro que J é um ideal bilateral de R, ainda, seja $e \in R$ tal que $ea - a \in M$, para todo $a \in R$. Então, para todo $x \in J$, temos $ax - x \in M$, e como $ax \in M$ por definição de J, segue que $x \in M$, ou seja, $J \subset M$, e daí, pela definição de I, segue que $J \subset I$. Dado $x \in I$, temos $Rx \subset I \subset M$, e daí $x \in J$, ou seja, $I = J$.

Reciprocamente, se $M \lhd_r R$ é maximal modular e $I = \{x \in R : Rx \subset M\}$ e $J \lhd R$ é tal que $J \subset M$, então todo $x \in J$ é tal que $Rx \subset J \subset M$, ou seja, $J \subset I$. Segue que I é o maior ideal bilateral contido em M, e então, I é primitivo. □

Essa definição tem a vantagem de ser intrínseca do próprio anel.

Exemplo:

1. *Se R é comutativo, então as noções de ideal à direita e bilateral coincidem, e então $I \lhd R$ é primitivo se e só se é maximal e modular. Em particular, se R é comutativo e $0 \lhd R$ é primitivo*

(comutatividade e $0 \lhd R$ primitivo implicam que R admite unidade, pois 0 será ideal modular (será o maior ideal bilateral contido num ideal maximal modular à direita — mas como R é comutativo, necessariamente esse ideal maximal modular será 0), e deve existir $1 \in R$ tal que $a1 - a \in \{0\}, \forall a \in R$, ou seja, R admite unidade 1), então R é corpo.

2. *Se R admite unidade e $I \lhd R$ é maximal, então I é primitivo. Em particular, se R admite unidade e é simples, então R é primitivo. Em especial, $M_n(D)$, o anel das matrizes $n \times n$ com entradas em um anel de divisão D, é primitivo.*

□

Definição 2.1.4. Seja M um R-módulo. M é dito **fiel** se para todo $r \in R$, $r \neq 0$, existe $m \in M$ tal que $mr \neq 0$

A seguir, uma definição alternativa para ideal primitivo:

Lema 2.1.5. *Sejam R um anel e $P \lhd R$ um ideal. Então P é primitivo se e só se existe um (R/P)-módulo M fiel e irredutível*

Demonstração. Assuma que M é um (R/P)-módulo fiel e irredutível. Temos que M tem estrutura de R-módulo irredutível. Seja $m \in M$, $m \neq 0$. Então, sendo M irredutível, $m(R/P) = M$. Seja $N = \{x \in R : mx = 0\}$. Temos $P \subset N$ e $N \lhd_r R$, e ainda, N é maximal, pois o quociente $R/N \simeq M$ é simples, e N é modular, pois chame $\varphi : x \in R \mapsto mx \in M$ o homomorfismo de R-módulos e tome $e \in R$ tal que $\varphi(e) = m$. Daí, para todo $r \in R$, temos $\varphi(er - r) = \varphi(e)r - \varphi(r) = mr - mr = 0$, e daí $er - r \in N = \text{Ker}\varphi$, ou seja, N é modular. Ainda, dado $I \lhd R$ com $I \subset N$, temos $MI = mRI \subset mI \subset mN = 0$, e daí $I \subset P$, ou seja, P é primitivo.

Reciprocamente, seja $N \lhd_r R$ maximal tal que $P = (N : R)$ e considere o R-módulo $M := R/N$. Como N é maximal, M é irredutível, e além disso, $MP = 0$, e daí M é um (R/P)-módulo. Ainda, por escolha de P, M é um (R/P)-módulo fiel, pois se $\bar{x} \in R/P$ é tal que $M\bar{x} = 0$, então $Rx \subset N$, ou seja, $x \in (N : R) = P$. □

A noção de ideal primitivo pode ser definida de forma totalmente análoga trocando "direita" por "esquerda". Existem exemplos de ideal que é primitivo à direita, mas não à esquerda. O primeiro tal exemplo foi encontrado por G. Bergman, vide [6].

Definição 2.1.6. Seja R um anel. R é dito **primitivo** se $0 \lhd R$ for um ideal primitivo.

Exemplo: *Se $I \subset R$ é um ideal primitivo, então R/I é um anel primitivo.* □

Teorema 2.1.7. *Um anel R é primitivo se e só se existe um R-módulo M fiel e irredutível.*

Vale ressaltar que se M é um R-módulo irredutível, para um anel R qualquer, então $\text{Hom}_R(M, M)$ é um anel de divisão. De fato, dado $f \in \text{Hom}_R(M, M)$, tanto $\text{Ker}f$ quanto $f(M)$ são R-submódulos de M, e sendo M irredutível, necessariamente $f = 0$ ou f é isomorfismo (ou seja, invertível). Esta afirmação é bem conhecida com *Lema de Schur*, e é um dos fatos fundamentais na teoria das representações de grupos, bem como em outras áreas da matemática.

Seja $D = \text{Hom}_R(M, M)$. Então, podemos considerar M como um D-módulo à esquerda (podemos fazer isso, independente de M ser irredutível ou não como R-módulo). No caso de D ser anel de

divisão, M é nada mais nada menos que um D-espaço vetorial, e boa parte da teoria da álgebra linear sobre corpos é válida aqui (para mais detalhes, ver o livro de Van der Waerden [36]). Ainda, por definição de $\mathrm{Hom}_R(M,M)$, temos que M tem estrutura de (D,R)-bimódulo, pois $(dm)r = d(mr)$, para todo $d \in D, m \in M, r \in R$, e segue disso que cada $r \in R$ age como transformação linear do D-espaço vetorial M. Segue que existe $R \to \mathrm{Hom}_D(M,M)$ natural. No caso específico em que M é R-módulo fiel, temos inclusão 1-1, isto é $R \subset \mathrm{Hom}_R(M,M)$.

O próximo teorema será uma caracterização de grande importância de anéis primitivos:

Teorema 2.1.8 (Densidade)**.** *Sejam R um anel primitivo, M um R-módulo fiel e irredutível e $D = Hom_R(M,M)$. Considere M como um D-módulo à esquerda e seja $E = Hom_D(M,M)$. Então, para cada $G \subset M$ D-submódulo finitamente gerado e para todo $e \in E$, existe $r \in R$ tal que $G(e-r) = 0$.*

Demonstração. Fixe $e \in E$. Provaremos por indução em $n = \dim_D G$ que:

1. existe $r \in R$ tal que $G(e-r) = 0$
2. $\mathrm{Ann}_M(\mathrm{Ann}_R(G)) = G$

Se $n = 0$ então o resultado vale trivialmente. Assuma então que o resultado vale para um D-subespaço G, ou seja, existe $r \in R$ tal que $G(e-r) = 0$, e seja $a \in M \setminus G$.

Assuma que existe $r' \in R$ que satisfaz $(G + Da)(r' - e) = 0$. Então, escrevendo $r' = r + s$, para algum $s \in R$ (mais precisamente $s = r' - r$), isso equivale a

$$\underbrace{(G + Da)(r-e)}_{Da(r-e)} = (G + Da)s = Gs + Das$$

daí, basta encontrar $s \in \mathrm{Ann}_R(G)$ tal que $as = a(r-e)$. Para isso, basta mostrar que $a\mathrm{Ann}_R(G) = M$. Se $a\mathrm{Ann}_R(G) \neq 0$, então, sendo $a\mathrm{Ann}_R(G)$ R-submódulo do R-módulo irredutível M, segue que $a\mathrm{Ann}_R(G) = M$ e vale. Se $a\mathrm{Ann}_R(G) = 0$, então $a \in \mathrm{Ann}_M(\mathrm{Ann}_R(G)) = G$ (por hipótese de indução 2), absurdo. Isso prova que $G + Da$ satisfaz 1.

Temos $\mathrm{Ann}_R(G+Da) = \mathrm{Ann}_R(G) \cap \mathrm{Ann}_R(a)$. Sejam $V = G + Da$ e $W = \mathrm{Ann}_M(\mathrm{Ann}_R(G+Da))$. Claro que $V \subset W$. Dado $b \in W$ considere o homomorfismo de R-módulos $\varphi : ax \in a\mathrm{Ann}_R(G) \mapsto bx \in b\mathrm{Ann}_R(G)$. Se $b\mathrm{Ann}_R(G) = 0$, então $b \in G \subset V$ e vale. Se não, temos $b\mathrm{Ann}_R(G) \simeq a\mathrm{Ann}_R(G) \simeq M$, e daí, $\varphi \in D$, e então, existe $d \in D$ tal que $\varphi(x) = dx, \forall x \in M$. Como para todo $s \in \mathrm{Ann}_R(G)$ temos $bs = \varphi(as) = das$, segue que $(b - da)s = 0$, ou seja, $da - b \in \mathrm{Ann}_M(\mathrm{Ann}_R(G)) = G$, e daí, $b \in G + Da = V$, e isso prova 2. □

Corolário 2.1.9. *Seja R um anel primitivo. Então existe D anel de divisão tal que uma, e somente uma, ocorre:*

1. *Existe $n \in \mathbb{N}$ tal que $R \simeq M_n(D)$.*
2. *Para todo $k \in \mathbb{N}$, existe subanel $S \subset R$ tal que $S \simeq M_k(D)$.*

Demonstração. Utilizando a mesma notação: M o R-módulo fiel e irredutível e $D = \mathrm{Hom}_R(M,M)$ (anel de divisão), seja $n = \dim_D M$. Se $n < \infty$, então $\mathrm{Hom}_D(M,M) \simeq M_n(D)$. Daí, pelo Teorema da Densidade, necessariamente $R = \mathrm{Hom}_D(M,M) \simeq M_n(D)$.

Se $n = \infty$, para cada $k \in \mathbb{N}$, considere $e_1, \cdots, e_k$ D-linearmente independentes e seja $G = De_1 + \cdots + De_k$. Então, considerando $R \subset \mathrm{Hom}_D(M,M)$ e tomando as aplicações $r \in R$ tal que $Gr \subset G$, ou seja, $S := \{r \in R : r\text{“} \in \text{”}\mathrm{Hom}_D(G,G)\}$, temos S subanel de R e, pelo Teorema da Densidade, $S = \mathrm{Hom}_D(G,G) \simeq M_k(D)$. □

Nota. A volta desse último teorema vale, isto é, sejam M um espaço vetorial sobre um anel de divisão D, $E = \mathrm{Hom}_D(M, M)$ o anel de endomorfismos de M e $R \subset E$ um anel que satisfaz a seguinte propriedade: para todo D-subespaço de dimensão finita $G \subset M$ e para cada $e \in E$, existe $r \in R$ tal que $G(e - d) = 0$ (um tal anel é dito ser "**denso** sobre um anel de endomorfismos de um espaço vetorial"). Então R é primitivo. De fato, para demonstrar isso, basta mostrar que M é um R-módulo fiel e irredutível. Como $R \subset E$, segue direto que M é um R-módulo e é fiel. Ainda, fixando $m \in M$, e para cada $x \in M$, existe $e \in E$ tal que $me = x$, e daí, tomando o subespaço $G = Dm + Dx$, temos que existe $r \in R$ tal que $mr = x$. Segue que $mR = M$, ou seja, M é R-módulo irredutível, e portanto, R é primitivo.

Este último corolário mostra que anéis primitivos são anéis de matrizes, ou contém todos os anéis de matrizes, e esta caracterização será de grande importância nos estudos de PI-álgebras.

A razão do nome "Teorema da densidade" se deve ao fato de poder definir uma topologia em E ($E = \mathrm{Hom}_D(M, M)$), em que R será denso em E, e não será apresentado em detalhes aqui (brevemente: considere o conjunto $M^M = \{f : M \to M \text{ função}\}$, e tome a topologia discreta em M, a topologia produto em M^M e a topologia induzida em $E \subset M^M$. Neste caso, dado $e \in E$, uma vizinhança básica de e é da forma $V(a_1, \cdots, a_m) = \{f \in E : a_1 f = a_1 e, \cdots, a_m f = a_m e\}$, com $m \in \mathbb{N}$ e $a_1, \cdots, a_m \in M$. O Teorema da densidade diz que R será denso em E com esta topologia, pois toda vizinhança básica contém pelo menos um elemento de R.)

§2.2 Radical de Jacobson e Produto Subdireto

Nesta seção apresentaremos duas ferramentas muito úteis na álgebra não-comutativa e que, unidas ao Teorema da Densidade, obtemos uma técnica muito forte no estudo de PI-álgebras.

Definição 2.2.1. Seja R um anel. Define-se o **radical de Jacobson** de R por

$$J(R) := \bigcap_{P \lhd R \text{ primitivo}} P.$$

Definição 2.2.2. Denomina-se R **semiprimitivo** se $J(R) = 0$.

Lema 2.2.3. *Seja R anel. Então $R/J(R)$ é semiprimitivo. Ainda, se $I \lhd R$ é tal que R/I é semiprimitivo, então $J(R) \subset I$.*

Para tornar o texto completo e para refinar a intuição algébrica por trás desta definição, apresentarei várias equivalências para o Radical de Jacobson (que serão úteis em algumas caracterizações mais precisas do radical). Em alguns casos específicos, uma caracterização pode ser mais fácil de calcular que as demais, mas, em geral, é difícil obter explicitamente o radical.

Diferente da noção de ideal e anel primitivo, a noção de semiprimitividade e o conceito de radical de Jacobson não dependem do lado, isto é, se invertermos a noção de ideal primitivo à direita (trocando direita para esquerda) para "ideal primitivo à esquerda", e redefinirmos o radical de Jacobson como a intersecção dos ideais primitivos à esquerda, então, concluiremos que em ambos os casos o radical coincide, e esse fato será obtido a partir das caracterizações do $J(R)$.

Lema 2.2.4. $J(R) = \bigcap\{M \lhd_r R \text{ maximal modular}\}$ *(cf. Definição 2.1.1).*

Demonstração. Seja $J' = \bigcap\{M \lhd_r R \text{ maximal modular}\}$. Como todo ideal primitivo está contido em um ideal maximal modular, segue que $J(R) \subset J'$.

Reciprocamente, seja $P \triangleleft R$ primitivo e $M \triangleleft_r R$ o ideal maximal modular tal que $P = (M : R)$. Temos

$$P = \bigcap_{\bar{m} \in R/M} \{x \in R : \bar{m}x = \bar{0}\}$$

de fato, sendo $P' = \bigcap_{\bar{m} \in R/M} \{x \in R : \bar{m}x = \bar{0}\}$, é claro que $P \subset P'$. Dado $r \in P'$, temos que $Rr \subset M$, ou seja, $r \in (M : R) = P$. Ainda, $N_m := \{x \in R : \bar{m}x = \bar{0}\}$ é todo o anel R ou é modular maximal (mesmo argumento na demonstração do Lema 2.1.5), e daí, P é intersecção de ideais modulares maximais à direita, e o resultado segue. □

A seguir, apresentarei algumas caracterizações do radical envolvendo mais explicitamente os elementos do anel:

Lema 2.2.5. *Seja R um anel com unidade 1. Então*

$$J(R) = \{r \in R : 1 - rs \text{ é invertível à direita, para todo } s \in R\}.$$

Demonstração. Provarei que valem as seguintes equivalências (lembre-se que, como R admite unidade, as noções de ideal e ideal modular coincidem):

(i) $r \in J(R)$,

(ii) $rs \in M$, para todo $M \triangleleft_r R$ maximal e para todo $s \in R$,

(iii) $1 - rs \notin M$, para todo $M \triangleleft_r R$ maximal e para todo $s \in R$,

(iv) $1 - rs$ é invertível pela direita.

$(i) \Rightarrow (ii)$: Por $J(R)$ ser ideal.
$(ii) \Rightarrow (i)$: Pois $1 \in R$, e daí, em particular, $r1 = r \in M$, para todo $M \triangleleft_r R$ maximal.
$(ii) \Rightarrow (iii)$: Se $1 - rs \in M$, para algum $M \triangleleft_r R$ maximal, então $1 \in M$, absurdo.
$(iii) \Rightarrow (ii)$: Assuma que $rs \notin M$ para algum $M \triangleleft_r R$ maximal. Então, $rsR + M = R$, ou seja, $1 \in rsR + M$, e daí, $1 - rs \in M$.
$(iii) \iff (iv)$: $(1 - rs)R$ não está contido em nenhum ideal maximal se e só se $(1 - rs)R = R$, logo, vale a equivalência. □

Lema 2.2.6. *Seja R um anel com unidade 1. Então $J(R)$ é o maior ideal tal que todo $r \in J(R)$ é tal que $1 - r$ é invertível.*

Demonstração. Seja $r \in J(R)$ e $1 - s$ a inversa pela direita de $1 - r$. Basta mostrar que $1 - s$ é invertível pela direita, pois, sendo x sua inversa pela direita, temos

$$(1 - s)(1 - r) = (1 - s)(1 - r)(1 - s)x = (1 - s)x = 1$$

e então, a inversa pela direita de $1 - s$ é $1 - r$ e valerá a afirmação.

Note que temos $1 = (1 - r)(1 - s) = 1 - r - s + rs$, e daí, $s = rs - r \in J(R)$, e então $1 - s$ é invertível pela direita.

Agora, seja $I \triangleleft R$ um ideal tal que todo $x \in I$ satisfaz $1 - x$ invertível. Dado $x \in I$, temos $xr \in I$, para todo $r \in R$, e $1 - xr$ é invertível pela direita, e então, $x \in I$. Segue que $I \subset J(R)$, e $J(R)$ é o maior ideal com essa propriedade. □

Exatamente o mesmo argumento prova que:

Corolário 2.2.7. *Seja R um anel com unidade 1. Então $J(R)$ é o maior ideal à direita tal que todo $r \in J(R)$ é tal que $1 - r$ é invertível.*

Corolário 2.2.8. $J(R) = \bigcap\{M \lhd_l R \text{ maximal}\} = \bigcap\{P \lhd R : P \text{ primitivo à esquerda}\}$

O último corolário segue pelo fato do lema 2.2.6 caracterizar o radical de forma simétrica, independente do lado.

Podemos repetir essas caracterizações para anéis sem unidade da seguinte maneira: se $1 \in R$ e $r, s \in R$ são tais que $(1-r)(1-s) = 1$, então $1 = 1 - r - s + rs$, ou seja, $r + s - rs = 0$. Definindo o produto $\odot$ em R dado por $r \odot s := r + s - rs$, temos que $\odot$ satisfaz:

i. $(r \odot s) \odot t = r \odot (s \odot t), \forall r, s, t \in R$

ii. $r \odot 0 = 0 \odot r = r, \forall r \in R$

e daí, $(R, \odot)$ é um semigrupo, com $0 \in R$ sendo a identidade. Dado $r \in R$, se existir $s \in R$ tal que $r \odot s = 0$, então s é um inverso à direita de r em $(R, \odot)$. Assim, obtemos a seguinte caracterização de $J(R)$:

Lema 2.2.9. *Seja R um anel (com ou sem unidade). Então*

(i) $J(R) = \{r \in R$: rs *tem inversa à direita em* $(R, \odot), \forall s \in R\}$

(ii) $J(R)$ *é o maior ideal à direita tal que todos os elementos de* $J(R)$ *são inversíveis em* $(R, \odot)$

Demonstração. Para cada $r \in R$, e considerando o ideal (com notação sugestiva, mesmo R não necessariamente tendo unidade) $(1-r)R := \{x - rx : x \in R\}$, as demonstrações seguem de forma análoga no caso de R ter unidade. □

A seguir, apresentarei a definição de produto subdireto:

Definição 2.2.10. Seja R um anel. Dizemos que R é o **produto subdireto** de uma família de anéis $\{R_\alpha\}_{\alpha \in I}$ se existe subanel $S \subset \prod_{\alpha \in I} R_\alpha$, com $R \simeq S$ e $\pi_\alpha(S) = R_\alpha, \forall \alpha \in I$, sendo $\pi_\alpha : \prod_{\beta \in I} R_\beta \to R_\alpha$ a projeção canônica. Denota-se por $R = \prod_{\alpha \in I}{}^S R_\alpha$.

Uma caracterização muito útil para produto subdireto é a seguinte:

Teorema 2.2.11. *Sejam R anel e $\{R_\alpha\}_{\alpha \in I}$ família de anéis. Então $R = \prod_{\alpha \in I}{}^S R_\alpha$ se e só se existe família $\{I_\alpha\}_{\alpha \in I}$ de ideais bilaterais de R tal que $\bigcap_{\alpha \in I} I_\alpha = 0$ e $R/I_\alpha \simeq R_\alpha, \forall \alpha \in I$.*

Demonstração. Se $R = \prod_{\alpha \in I}{}^S R_\alpha$, considere $I_\alpha = \text{Ker}(\pi_\alpha|_R)$ (realizando as devidas identificações para termos $R \subset \prod_{\alpha \in I} R_\alpha$). Temos $\cap I_\alpha = 0$ e $R_\alpha \simeq R/I_\alpha, \forall \alpha \in I$: o primeiro pelo fato da inclusão $R \hookrightarrow \prod_{\alpha \in I} R_\alpha$ ser 1-1 e o segundo pelo Teorema do Isomorfismo.

Reciprocamente, considere $R'_\alpha = R/I_\alpha (\simeq R_\alpha)$ e tome a aplicação canônica $\varphi : R \to \prod_{\alpha \in I} R'_\alpha$. Por construção, $\pi_\alpha(\varphi(R)) = R_\alpha$ e dado $x \in R$, $\varphi(x) = 0$ se e só se $\pi_\alpha(\varphi(x)) = 0, \forall \alpha \in I$, ou seja, se e só se $x \in I_\alpha, \forall \alpha \in I$, ou seja, se e só se $x \in \cap I_\alpha = 0$. Daí $R \to \prod_{\alpha \in I} R'_\alpha$ é 1-1 e $R = \prod_{\alpha \in I}{}^S R_\alpha$. □

Esta definição, à primeira vista, parece não depender muito da estrutura do anel R, e aparenta ser algo distante do anel, carregando poucas informações. Isso de fato ocorre, e podemos ter diferentes anéis, em que ambos são produto subdireto da mesma família de anéis.

Exemplo:

1. *Seja* $\{R_\alpha\}_{\alpha\in I}$ *família de anéis. Então* $\prod_{\alpha\in I} R_\alpha$ *e* $\bigoplus_{\alpha\in I} R_\alpha$ *são produtos subdiretos de* $\{R_\alpha\}_{\alpha\in I}$*, e se* $S \subset \prod_{\alpha\in I} R_\alpha$ *é produto subdireto dessa família, então, para um subconjunto* $J \subset I$*, temos que* $S + \sum_{\beta\in J} R_\beta$ *e* $S + \prod_{\beta\in J} R_\beta$ *são produtos subdiretos de* $\{R_\alpha\}_{\alpha\in I}$*.*

2. *Em particular, se* $A = \{f : \mathbb{R} \to \mathbb{R}$ *função*$\}$ *e* $B = \mathbb{R}$*, então* A *e* B *são o produto subdireto de* $\{\mathbb{R}_x\}_{x\in\mathbb{R}}$*, em que* $\mathbb{R}_x = \mathbb{R}$*.*

3. *Em* $\mathbb{Z}$*, temos* $0 = \bigcap_{p\ primo} p\mathbb{Z}$*, e daí,* $\mathbb{Z} = \prod_{p\ primo}{}^{S}\mathbb{Z}/p\mathbb{Z}$ *é o produto subdireto de corpos.*

4. *Seja* R *um anel semiprimitivo. Então* $\bigcap_{P\ primitivo} P = 0$*, e daí,* R *é produto subdireto de anéis primitivos. Reciprocamente, se* R *é produto subdireto de anéis primitivos, então* R *é semiprimitivo.*

□

Um dos fatos que torna produto subdireto importantíssimo na teoria de PI-álgebras é o fato de preservar identidades, isto é, a seguinte observação:

Teorema 2.2.12. *Sejam* A *álgebra sobre um corpo* K*,* $\{A_\alpha\}_{\alpha\in I}$ *família de álgebras sobre o mesmo corpo* K*, de modo que* $A = \prod_{\alpha\in I}{}^{S} A_\alpha$ *e* $f(x_1, \cdots, x_m) \in K\langle X\rangle$*. Então* f *é identidade polinomial de* A *se e só se* f *é identidade polinomial de* A_α*, para todo* $\alpha \in I$*.*

Demonstração. Assuma f identidade de A. Então, dados $\alpha \in I$ e $a_1, \cdots, a_m \in A_\alpha$, existem $b_1, \cdots, b_m \in A$ tais que $\pi_\alpha(b_i) = a_i, i = 1, \cdots, m$, e daí

$$f(a_1, \cdots, a_m) = f(\pi_\alpha(b_1), \cdots, \pi_\alpha(b_m)) = \pi_\alpha f(b_1, \ldots, b_m) = 0.$$

Reciprocamente, dados $a_1, \cdots, a_m \in A$, temos que $\pi_\alpha f(a_1, \ldots, a_m) = f(\pi_\alpha(a_1), \cdots, \pi_\alpha(a_m)) = 0$, para todo $\alpha \in I$, e isso é o mesmo que $f(a_1, \cdots, a_m) = 0$. □

Exemplo: *Seja* A *uma álgebra sobre um corpo* K *que satisfaz uma identidade polinomial não satisfeita por* $M_2(K)$*, e assuma que* A *é produto subdireto de álgebras matriciais sobre* K*. Então* A *é comutativa. De fato, as álgebras matriciais* $M_n(K)$ *devem necessariamente satisfazer* $n = 1$*, e então, serão corpos. Logo todos serão comutativos, o que implicará em* A *comutativo (em outras palavras, todos satisfazem* $[x, y] = 0$ *e então,* A *deve satisfazer essa identidade). De fato, se existir uma álgebra matricial* $M_n(K)$*, com* $n > 1$*, então, em particular,* $M_2(K) \subset M_n(K)$*, o que é contradição, pois implicará que* $M_2(K)$ *satisfaz todas as identidades de* A*.* □

Como veremos adiante, a mesma afirmação vale para um caso mais geral.

Finalizaremos com algumas considerações sobre o Radical de Jacobson: todas as definições e resultados apresentados nesta seção e na anterior foram feitos para anéis, mas poderíamos construir

os análogos para álgebras (exigindo que todas as estruturas envolvidas nas definições sejam subespaços vetoriais). Toda essa teoria poderia ser feita, sem maiores problemas, para álgebras sobre anéis comutativos com unidade, e isso incluiria os casos de anéis e álgebras sobre corpos. Como já foi discutido, dada uma álgebra A, nem todo ideal de A, com A considerada como anel, será ideal de A como álgebra. Isso implica, em particular, que não necessariamente o radical de A, vista como anel, irá coincidir com o radical de A, vista como álgebra. Para o caso de trabalharmos com álgebras sobre corpos, os radicais coincidem:

Lema 2.2.13. *Sejam A uma álgebra sobre um corpo K e $I \subset A$ um ideal modular maximal de A, com A vista como anel. Então I é um ideal modular maximal de A, com A vista como álgebra.*

Demonstração. Basta mostrar que $\alpha I \subset I$, para cada $\alpha \in K$, e então, seguirá que I é ideal de A como álgebra, e como trivialmente cada ideal de A como álgebra necessariamente é ideal de A como anel, segue que I automaticamente será ideal maximal de A (como álgebra), e I já é suposto modular (e continuará sendo modular).

Seja $e \in A$ tal que $e - ea \in I, \forall a \in A$. Note que, para cada $\alpha \in K$, temos αI um ideal à direita de A (como anel). Se existir $\alpha \in K$ tal que $\alpha I \nsubseteq I$, então, em particular, $\alpha I + I = A$, uma vez que I é maximal em A. Daí, existem $a, b \in I$ tais que $e = \alpha a + b$.

Por um lado, temos $e^2 = \alpha ae + be = a(\alpha e) + be \in I$, e por outro lado, por propriedade de e, temos $e - e^2 \in I$, o que implica $e \in I$, e então $I = A$, contradição. Segue que $\alpha I \subset I$ para todo $\alpha \in K$, e então, pelos comentários iniciais, segue que I é ideal maximal modular de A, com A vista como álgebra. □

Com isso, obtemos imediatamente o seguinte resultado:

Teorema 2.2.14. *Sejam A uma álgebra sobre um corpo K e $I \subset A$ um subconjunto não vazio. Então I é um ideal maximal modular de A como anel se e só se I é ideal maximal modular de A como álgebra.*

Demonstração. O lema 2.2.13 anterior mostra que se I é maximal modular como anel, então I é ideal maximal modular como álgebra. Reciprocamente, se I é ideal maximal modular como álgebra, então, pelo lema de Zorn, existe um ideal de A (como anel) maximal modular I' com $I \subset I'$, e, novamente pelo lema 2.2.13, temos I' ideal de A como álgebra, e então, por maximalidade de I, segue que $I = I'$, e em particular, I é ideal maximal modular de A como anel. □

Como consequência, obtemos que, se A é uma álgebra sobre um corpo K, então o radical $J(A)$ é independente se considerarmos A como anel ou como álgebra. Ainda mais, temos que $J(A)$ é necessariamente subespaço vetorial, e valem todas as relações envolvendo elementos do anel ($J(A)$ é o maior ideal de A (ideal como anel ou como subespaço vetorial) tal que todo elemento em $J(A)$ admite inversa à direita em $(A, \odot)$).

§2.3 Anéis de Divisão

Nesta seção, serão apresentados alguns resultados sobre anéis de divisão que serão úteis para estudar identidades polinomiais. Neste trabalho, não será apresentado um estudo aprofundado sobre o assunto. Um exemplo de aplicação: dada uma PI-álgebra semiprimitiva, ela é um produto subdireto de álgebras primitivas e de matrizes $M_n(D)$, com D anel de divisão. Mas, em que condições, podemos dizer que D é um corpo?

Começaremos com um teorema, para fins de motivação, mas antes vale notar que, dado um anel de divisão D, seu centro $Z = Z(D) = \{x \in D : xd = dx, \forall d \in D\}$ é um corpo, e dado qualquer $d \in D$, a extensão de anéis de divisão $Z(d)$ também é um corpo.

Teorema 2.3.1. *Sejam K um corpo algebricamente fechado e D um anel de divisão com $K \subset Z(D)$ e $dim_K D < \infty$. Então $D = K$.*

Demonstração. Seja $d \in D$. Então, existe $n \in \mathbb{N}$ tal que $\{1, d, d^2, \cdots, d^n\}$ forma um conjunto linearmente dependente, e então, existem $\alpha_0, \alpha_1, \cdots, \alpha_n \in K$ não todos nulos tais que $\alpha_0 + \alpha_1 d + \cdots + \alpha_n d^n = 0$. Seja $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$. Temos $K(d)$ um corpo e $p(d) = 0$, ou seja, d é algébrico sobre K, e sendo K algebricamente fechado, segue que $d \in K$. Daí $D = K$. □

Uma questão interessante é: dado um anel de divisão que não é corpo D, $Z = Z(D)$ e um fecho algébrico $\bar{Z}$ de Z, qual a estrutura de $\bar{D} := D \otimes_Z \bar{Z}$? Como $\bar{D} \neq \bar{Z}$ (pois $\dim_{\bar{Z}} \bar{D} = \dim_Z D > 1$) e $\bar{Z} \subset Z(\bar{D})$, segue que $\bar{D}$ deixa de ser um anel de divisão. Como será mostrado adiante, em alguns casos, $\bar{D} = M_n(\bar{Z})$; e no caso mais geral, existe um corpo K, com $Z \subset K \subset D$, tal que $D \otimes_Z K$ é primitivo. Mas, antes de demonstrar isso, será necessário introduzir a linguagem básica de álgebras centrais e simples.

Definição 2.3.2. Seja A uma álgebra sobre K.

i. Dizemos que A é **simples** se os únicos ideais bilaterais de A são 0 e A, e $A^2 \neq 0$.

ii. Dizemos que A é **central** se $Z(A) \simeq K$.

Lema 2.3.3. *Sejam A álgebra central e simples e B álgebra simples com $K \subset Z(B)$. Então $A \otimes_K B$ é álgebra simples.*

Demonstração. Seja $I \lhd A \otimes_K B$ ideal não nulo. Para cada $u \in I$, defina

$$l(u) := \min \left\{ n \in \mathbb{N} : \exists a_1 \otimes b_1, \cdots, a_n \otimes b_n \in A \otimes_K B,\ b_1, \cdots, b_n \text{ l.i., com } u = \sum_{i=1}^{n} a_i \otimes b_i \right\}$$

Sejam $m = \min\{l(u) : u \in I, u \neq 0\}$ e $u \in I$ tal que $l(u) = m$. Provaremos que $m = 1$. Para cada $s, t \in A$, temos $I \ni (s \otimes 1)u(t \otimes 1) = (sa_1t) \otimes b_1 + \cdots + (sa_nt) \otimes b_n$. Sejam $s, t \in A$ tais que $sa_1t = 1$ (existem, pois $Aa_1A = A$, pois A é simples). Então, denominando $v = (s \otimes 1)u(t \otimes 1)$, segue que $v = 1 \otimes b_1 + a'_2 \otimes b_2 + \cdots + a'_n \otimes b_n$. Para cada $a \in A$, temos $I \ni [a \otimes 1, v] = (a \otimes 1)v - v(a \otimes 1)$, mas, $l([a \otimes 1, v]) < l(v) \leq l(u) = m$, e então, necessariamente $[a \otimes 1, v] = 0$, e daí, como

$$0 = [a \otimes 1, v] = [a, 1] \otimes b_1 + [a, a'_2] \otimes b_2 + \cdots + [a, a'_n] \otimes b_n$$

e sendo $a \in A$ arbitrário e $b_1, \cdots, b_n$ linearmente independentes, temos $a'_2, \cdots, a'_n \in Z(A) = K$, e então, podemos escrever $v = 1 \otimes b$ (tomando $b = b_1 + a'_2 b_2 + \cdots + a'_n b_n$, mas não é relevante isso). Segue que $m = 1$.

Temos que, para todo $c, d \in B$, $I \ni (1 \otimes c)v(1 \otimes d) = 1 \otimes (cbd)$, e tomando $c, d \in B$ tais que $cbd = 1$ (existem, pois B é simples, e daí $BbB = B$), segue que $I \ni 1 \otimes 1$, e daí $I = A \otimes_K B$. □

Definição 2.3.4. Sejam R anel e $S \subset R$ um subconjunto. Define-se o **centralizador** de S em R por $C_R(S) = \{r \in R : rs = sr, \forall s \in S\}$.

Lema 2.3.5. *$C_R(S)$ é subanel de R. Ainda, se R é anel de divisão, $C_R(S)$ também será anel de divisão.*

Observação. Seja M um R-módulo e considere $E = \mathrm{Hom}(M, +)$ o anel de endomorfismos de grupos do grupo abeliano M. Então $\mathrm{Hom}_R(M, M) = C_E(R)$. De fato, $e \in \mathrm{Hom}_R(M, M)$ se e só se $(em)r = e(mr), \forall m \in M, \forall r \in R$, ou seja, se e só se $e \in C_E(R)$.

Definição 2.3.6. Seja D um anel de divisão e $Z = Z(D)$. Um **subcorpo maximal** de D é um corpo K tal que $Z \subset K \subset D$ e se $L \subset D$ é um corpo com $K \subset L$, então $L = K$.

Observação.

1. Pelo Lema de Zorn, sempre existe subcorpo maximal de um anel de divisão.
2. Se D não é corpo, Z e K nunca coincidem. De fato, isso segue da observação que, para todo $d \in D$, $Z \subsetneq Z(d)$ é um corpo.

Lema 2.3.7. *Sejam D anel de divisão, $Z = Z(D)$ e $K \subset D$ corpo. Então K é subcorpo maximal se e só se $C_D(K) = K$.*

Demonstração. Assuma K subcorpo maximal. Dado $x \in C_D(K)$, temos a extensão $K(x)$ corpo, mas, sendo K maximal, temos $x \in K$, ou seja, $C_D(K) \subset K$. É claro que $K \subset C_D(K)$ e daí, vale a igualdade.

Reciprocamente, assuma $C_D(K) = K$. Dado $L \subset D$ corpo, com $K \subset L$, temos $L \subset C_D(K) = K$, e daí, $L = K$ e então K é subcorpo maximal de D. □

Observação. Note que sempre $Z \subset C_D(K) = K$.

Com isso, podemos demonstrar o resultado principal desta seção:

Teorema 2.3.8. *Sejam D anel de divisão, $Z = Z(D)$ e $K \subset D$ subcorpo maximal. Então $D \otimes_Z K$ é anel denso no anel de transformações lineares do espaço vetorial D sobre K (c.f. nota após Corolário 2.1.9).*

Demonstração. Sejam $E = \mathrm{Hom}(D, +)$, $D_r = \{T_a : x \in D \mapsto xa \in D | a \in D\}$, $K_l = \{L_k : x \in D \mapsto kx \in D | k \in K\}$, $D_l = \{L_a : x \in D \mapsto ax \in D | a \in D\}$ e $\Delta = C_E(D_r K_l)$.

Considere o subanel $D_r K_l \subset E$, gerado pelos produtos $T_a L_k$, com $T_a \in D_r, L_k \in K_l$. Note que, como os elementos de D_r comutam com os elementos de K_l, segue que $D_r K_l = \{\sum T_a L_k : T_a \in D_r, L_k \in K_l\}$.

Passo 1: D é um $D_r K_l$-módulo fiel e irredutível.

Como D é anel de divisão, para todo $d \in D, d \neq 0$, $dD_r = D$, e ainda, para todo $T_a L_k \in D_r K_l \setminus \{0\}$, temos $DT_a L_k \neq 0$ (por exemplo, $1T_a L_k \neq 0$). Daí D é $D_r K_l$-módulo fiel e irredutível. Em particular, $\Delta = C_E(D_r K_l) = \mathrm{Hom}_{D_r K_l}(D)$.

Passo 2: $\Delta = K_l \simeq K$.

É claro que $K_l \subset \Delta$. Ainda, como em particular $\Delta \subset C(D_r)$, temos que $\forall \varphi \in \Delta$, $\varphi T_a = T_a \varphi, \forall a \in D$, e em particular, sendo $b = 1\varphi$, temos $a\varphi = 1a\varphi = 1T_a\varphi = 1\varphi T_a = bT_a = ba$, para todo $a \in D$, ou seja, $\varphi = L_b$, e daí, $\varphi \in D_l$. Em particular, como $\Delta \subset D_l \subset C_E(K_l)$, temos $\Delta \subset K_l$, pelo lema 2.3.7.

Com isso, temos que $D_r K_l$ é subanel do anel de endomorfismos do K-espaço vetorial D.

Por fim, defina $\phi : D \otimes_Z K \to D_r K_l$, tal que $\phi(a \otimes k) = T_a L_k$. Temos ϕ sobrejetor, e, como D é álgebra central e simples sobre Z e K é central com unidade, segue que $D \otimes_Z K$ é simples (pelo lema 2.3.3). Daí ϕ é isomorfismo, pois $\mathrm{Ker}\phi = 0$.

Segue que $D \otimes_Z K$ é anel denso no anel de transformações lineares do K-espaço vetorial D, pelo Teorema da Densidade. □

Corolário 2.3.9. *Sejam $Z \subset K \subset D$, com D anel de divisão, $Z = Z(D)$ e $K \subset D$ subcorpo maximal. Então, se $dim_K D < \infty$, $K \otimes_Z D \simeq M_n(K)$, em que $n^2 = dim_Z D$ (ou, equivalentemente, $n = dim_K D$).*

Como veremos, com auxílio desse importantíssimo teorema e auxílio de alguma técnicas, poderemos "transformar" anéis de divisão em álgebra de matrizes sobre corpos, e em geral, essa técnica será muito conveniente e útil ao se trabalhar com PI-álgebras.

§2.4 Radical de Jacobson (2)

Seja A uma álgebra sobre um corpo K e considere a álgebra $A^* = K \cdot 1 \oplus A$, obtida adicionando uma unidade a A. O objetivo desta seção será unicamente mostrar um resultado muito útil: os radicais de Jacobson das duas álgebras coincidem, ou seja, $J(A^*) = J(A)$.

Para isso, vale relembrar a operação $\odot$ definida em um anel (ou em uma álgebra) dada por $x \odot y := x + y - xy$, com $x, y \in A$, e $\odot$ é uma operação associativa com identidade 0. Utilizaremos a teoria desenvolvida para o Radical de Jacobson, considerando anéis não necessariamente com unidade, mais especificamente, a seguinte caracterização: $J(A)$ é o maior ideal tal que todo $x \in J(A)$ possui inverso em $(A, \odot)$, ou seja, existe $y \in A$ (na verdade $y \in J(A)$) tal que $x \odot y = 0$. Em particular, se I é um ideal tal que todo $x \in I$ possui inverso em $(A, \odot)$, então $I \subset J(A)$ (c.f. Teorema 2.3.7).

Lema 2.4.1. *Sejam A uma álgebra e $I \subset A$ um ideal nil. Então $I \subset J(A)$.*

Demonstração. Seja $x \in I$. Então $x^n = 0$, para algum $n \in \mathbb{N}$, e daí, tomando $y = -x - x^2 - \cdots - x^{n-1}$, obtemos

$$x \odot y = x + (-x - x^2 - \cdots - x^{n-1}) - x(-x - x^2 - \cdots - x^{n-1}) = 0$$

e daí, todo $x \in I$ tem inverso em $(A, \odot)$, e então, $I \subset J(A)$. □

Um resultado muito útil que será utilizado ao explorar as propriedades do radical é o seguinte:

Lema 2.4.2. *Sejam A, B álgebras e $f : A \to B$ epimorfismo de álgebras. Então $f(J(A)) \subset J(B)$. Em particular, se B é semiprimitivo, então $J(A) \subset Kerf$.*

Demonstração. Nestas hipóteses, $f(J(A))$ é um ideal em B, e todo $y \in f(J(A))$ tem inverso em $(B, \odot)$. De fato, escreva $y = f(x)$. Então, como $x \in J(A)$, existe $z \in A$ tal que $x \odot z = 0$, e daí, $f(x) \odot f(z) = f(x) + f(z) - f(x)f(z) = f(x \odot z) = 0$. Segue que $f(J(A)) \subset J(B)$. □

Exemplo:

1. *Nem sempre um epimorfismo de anéis $f : R \to S$ satisfaz $f(J(A)) = J(S)$. Um exemplo simples é o seguinte: sejam $R = \mathbb{Z}$ (semiprimitivo, pois a intersecção dos ideais maximais, que coincidem com os ideais gerados por números primos, é 0) e $S = \mathbb{Z}/p^n\mathbb{Z}$, sendo $p \in \mathbb{Z}$ primo e $n \in \mathbb{Z}$. Então, o ideal $pS \subset S$ é nilpotente, e então, $pS \subset J(S)$, e daí $J(S) \neq 0$. A projeção canônica $\pi : R \to S$ é sobre, mas, certamente $\pi(J(R)) = 0 \neq J(S)$.*

2. *Se $f : R \to S$ é um isomorfismo, então $f(J(R)) = J(S)$, devido a esse lema. De fato, $f(J(R)) \subset J(S)$, e por outro lado, $f^{-1}(J(S)) \subset J(R)$, o que implica $J(S) \subset f(J(R))$. Daí $f(J(R)) = J(S)$.*

□

Lema 2.4.3. *Sejam A álgebra semiprimitiva e $I \lhd_r A$. Então $J(I) = \{x \in I : xI = 0\}$.*

Demonstração. Chame $J' = \{x \in I : xI = 0\}$. Temos $J(I)I$ ideal em A, e todo elemento de $J(I)I \subset J(I)$ tem inverso em $(A, \odot)$, e daí $J(I)I \subset J(A) = 0$. Segue que $J(I) \subset J'$.

Reciprocamente, $J'^2 \subset J'I = 0$, e daí J' é nil como ideal de I, e então, $J' \subset J(I)$ e vale a igualdade. □

Teorema 2.4.4. *Sejam A álgebra e $I \lhd A$. Então $J(I) = J(A) \cap I$.*

Demonstração. Assuma A semiprimitivo. Então $J(I) = \{x \in I : xI = 0\}$ é um ideal bilateral de A, e todo $x \in J(I)$ tem inverso em $(A, \odot)$, ou seja, $J(I) \subset J(A) = 0$, e então, vale o resultado.

Para o caso geral, considere $I' := (I + J(A))/J(A)$. Temos I' ideal de $A/J(A)$, e $A/J(A)$ é semiprimitivo, o que implica $J(I') = 0$. Mas daí, $I/(I \cap J(A)) \simeq I'$ é semiprimitivo, e considerando a projeção canônica $\pi : I \to I/(I \cap J(A))$, pelo lema 2.4.2, $J(I) \subset \text{Ker}\pi = I \cap J(A)$.

Reciprocamente, $I \cap J(A)$ é um ideal em I tal que todo elemento admite inverso em $(A, \odot)$ (e então, seu inverso está em $I \cap J(A)$, ou seja, admite inverso em $(I, \odot)$), e segue que $I \cap J(A) \subset J(I)$, e isso prova a igualdade. □

Este teorema diz que o radical de Jacobson é *hereditário*. Na teoria geral de radicais em álgebras tal condição assume-se como parte da definição de radical (no sentido geral).

Exemplo: *Esse último resultado não vale se considerarmos subálgebra, ao invés de ideal. De fato, seja $R = M_n(D)$, anel de matrizes sobre um anel de divisão D. Como R é primitivo, temos $J(R) = 0$. Mas, $S = UT_n(D) =$ (matrizes triangulares superiores) $\subset R$ é uma subálgebra, e*

$$I := \left\{ \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \right\} \subset S$$

é um ideal de S e é nil, e portanto, $I \subset J(S)$. Daí $J(S) \neq 0$, e $J(S) \neq S \cap J(R) = 0$. □

Corolário 2.4.5. *Seja A uma álgebra. Então $J(A^*) = J(A)$, sendo $A^* = K \cdot 1 \oplus A$ a álgebra obtida adicionando 1 a A.*

Demonstração. Temos A um ideal de A^*. Daí $J(A) = A \cap J(A^*)$, ou seja, $J(A) \subset J(A^*)$. Reciprocamente, como $A^*/A \simeq K$ é semiprimitivo, considerando a projeção canônica $\pi : A^* \to A^*/A$, temos $J(A^*) \subset \text{Ker}\pi = A$, pelo lema 2.4.2. Sendo $J(A^*)$ ideal de A^*, e como $J(A^*) \subset A$, segue que $J(A^*)$ é ideal de A, e todo $x \in J(A^*)$ admite inverso em $(A^*, \odot)$, e seu inverso está em $J(A^*) \subset A$. Daí $J(A^*) \subset J(A)$, e isso prova a igualdade. □

§2.5 Notas em Álgebra Comutativa

Nesta seção, serão apresentadas noções básicas de alguns tópicos da álgebra comutativa: grau de transcendência e especialização.

Começaremos com uma definição básica:

Definição 2.5.1. Sejam K e L anéis com $K \subset L$ e $a_1, \cdots, a_n \in L$. Dizemos que $a_1, \cdots, a_n$ são **algebricamente independentes** em K se para todo polinômio $f \in K[x_1, \cdots, x_n]$, $f \neq 0$, tem-se $f(a_1, \cdots, a_n) \neq 0$.

Observação. (i) $a_1, \cdots, a_n \in L$ são algebricamente independentes em K se e só se (ver notação abaixo) $K[a_1, \cdots, a_n] \simeq K[x_1, \cdots, x_n]$, o anel de polinômios em n variáveis com coeficientes em K.

(ii) Se $n = 1$, dizemos simplesmente que a_1 é **transcendente** em K (comparar com a definição 3.1.1).

Notação: Dados K e L corpos, com $K \subset L$, e $a_1, \cdots, a_n \in L$, denota-se por:

(i) $K[a_1, \cdots, a_n]$ o menor subanel de L que contém K e $a_1, \cdots, a_n$.

(ii) $K(a_1, \cdots, a_n)$ o menor subcorpo de L que contém K e $a_1, \cdots, a_n$. Note que $K(a_1, \cdots, a_n)$ é o corpo de frações de $K[a_1, \cdots, a_n]$.

Definição 2.5.2. Sejam K e L corpos, com $K \subset L$ e L finitamente gerado (como álgebra) sobre K. Um subconjunto $\{y_1, \cdots, y_n\} \subset L$ é dito ser **base de transcendência** de L sobre K se

(i) $y_1, \cdots, y_n$ são algebricamente independentes,

(ii) $L|K(y_1, \cdots, y_n)$ é extensão algébrica.

Provaremos que sempre existe uma base de transcendência, para uma extensão finita de corpos:

Lema 2.5.3. *Sejam $L|K$ extensão de corpos, $y_1, \cdots, y_n \in L$ algebricamente independentes sobre K e $w \in L$. Então, w é algébrico sobre $K(y_1, \cdots, y_n)$ se e só se $\{y_1, \cdots, y_n, w\}$ não é algebricamente independente.*

Demonstração. Assuma w algébrico sobre $K(y_1, \cdots, y_n)$. Então, existem

$$\frac{f_0(y_1, \cdots, y_n)}{g_0(y_1, \cdots, y_n)}, \cdots, \frac{f_m(y_1, \cdots, y_n)}{g_m(y_1, \cdots, y_n)} \in K(y_1, \cdots, y_n)$$

com $f_m(y_1, \cdots, y_n) \neq 0$, tais que

$$w^m \left(\frac{f_m(y_1, \cdots, y_n)}{g_m(y_1, \cdots, y_n)} \right) + \cdots + w \left(\frac{f_1(y_1, \cdots, y_n)}{g_1(y_1, \cdots, y_n)} \right) + \frac{f_0(y_1, \cdots, y_n)}{g_0(y_1, \cdots, y_n)} = 0$$

daí, multiplicando por $g_0(y_1, \cdots, y_n) \cdots g_m(y_1, \cdots, y_n)$, obtemos que $\{y_1, \cdots, y_n, w\}$ é algebricamente dependente.

Reciprocamente, existe um polinômio $F(x_1, \cdots, x_n, z) \in K[x_1, \cdots, x_n, z]$, $F \neq 0$, tal que $F(y_1, \cdots, y_n, w) = 0$. A variável z efetivamente ocorre, pois se não, teríamos $F(y_1, \cdots, y_n, w) = F(y_1, \cdots, y_n) = 0$, contradição, por $y_1, \cdots, y_n$ serem algebricamente independentes. Daí, escrevendo

$$F(y_1, \cdots, y_n, w) = w^m f_m(y_1, \cdots, y_n) + \cdots + w f_1(y_1, \cdots, y_n) + f_0(y_1, \cdots, y_n) = 0$$

temos que w é algébrico sobre $K(y_1, \cdots, y_n)$. □

Teorema 2.5.4. *Sejam $L|K$ extensão de corpos e $a_1, \cdots, a_n \in L$ tais que $L = K(a_1, \cdots, a_n)$. Então $\{a_1, \cdots, a_n\}$ contém uma base de transcendência.*

Demonstração. Se $L|K$ é algébrico, então o conjunto vazio é uma base de transcendência. Se não, considere $\{a_{i_1}, \cdots, a_{i_m}\} \subset \{a_1, \cdots, a_n\}$ um subconjunto maximal algebricamente independente, e seja $\{a_{j_1}, \cdots, a_{j_l}\}$ o complementar de $\{a_{i_1}, \cdots, a_{i_m}\}$ em $\{a_1, \cdots, a_n\}$.

Pelo lema 2.5.3, temos que $a_{j_1}, \cdots, a_{j_l}$ são algébricos sobre $K(a_{i_1}, \cdots, a_{i_m})$ (pois $\{a_{i_1}, \cdots, a_{i_m}, a_{j_p}\}$ não é algebricamente independente, por escolha de $a_{i_1}, \cdots, a_{i_m}$, para $p = 1, \cdots, l$). Daí, $L = K(a_1, \cdots, a_n) = K(a_{i_1}, \cdots, a_{i_m})(a_{j_1}, \cdots, a_{j_l})$ é algébrico sobre $K(a_{i_1}, \cdots, a_{i_m})$, e daí $\{a_{i_1}, \cdots, a_{i_m}\}$ é base de transcedência de L sobre K. □

Provaremos a seguir que o conjunto de elementos numa base de transcendência é constante.

Lema 2.5.5. *Sejam $L|K$ extensão de corpos, $\{y_1, \cdots, y_m\} \subset L$ base de transcendência de L sobre K e $\{w_1, \cdots, w_s\} \subset L$ algebricamente independente sobre K. Então $s \leq m$.*

Demonstração. Assuma $m \geq 1$. A demonstração será por indução em s. Se $s = 1$, então $s = 1 \leq m$ e o resultado vale. Então, assuma $s > 1$. Temos $\{y_1, \cdots, y_m, w_1\}$ não algebricamente independente, e daí, existe um polinômio não nulo $G(x_1, \ldots, x_m, z) \in K[x_1, \cdots, x_m, z]$ tal que $G(y_1, \cdots, y_m, w_1) = 0$. A variável z efetivamente ocorre em G, pois $\{y_1, \cdots, y_m\}$ é algebricamente independente, e como w_1 não é algébrico sobre K, pelo menos uma das variáveis x_i efetivamente ocorre em G. Assuma, sem perda de generalidade, que x_1 ocorre em G. Então, y_1 é algébrico sobre $K(w_1, y_2, \cdots, y_n)$, e daí, considerando $K_1 = K(w_1)$, temos:

(i) L é algébrico sobre $K_1(y_2, \cdots, y_m)$, pois L é algébrico sobre $K(y_1, \cdots, y_m, w_1)$ e $K(y_1, \cdots, y_m, w_1)$ é algébrico sobre $K(y_2, \cdots, y_m, w_1)$.

(ii) $\{y_2, \cdots, y_m\}$ é algebricamente independente em K_1, pela suposição de que x_1 ocorre efetivamente em G.

Daí $\{y_2, \cdots, y_m\}$ é base de transcendência de L sobre K_1. Claro que $\{w_2, \cdots, w_s\}$ é algebricamente independente sobre K_1, e por hipótese de indução, segue que $s - 1 \leq m - 1$, ou seja, $s \leq m$. □

Corolário 2.5.6. *Seja $L|K$ extensão de corpos, com $L = K(a_1, \cdots, a_n)$. Então, duas bases de transcendência de L sobre K possuem o mesmo número de elementos.*

Definição 2.5.7. Seja $L|K$ extensão de corpos. Define-se o **grau de transcendência** de L sobre K, denotado por $\operatorname{gr\,tr}_K L$, como o número de elementos de uma base de transcendência de L sobre K. Se D é uma álgebra sobre K que é um domínio de integridade, define-se

$$\operatorname{gr\,tr}_K D := \operatorname{gr\,tr}_K (\operatorname{cf}(D))$$

em que $\operatorname{cf}(D)$ é o corpo de frações de D.

Exemplo:

1. *Seja $L|K$ extensão de corpos com L finitamente gerado sobre K (isto é, $L = K(a_1, \cdots, a_n)$, com $a_1, \cdots, a_n \in L$). Então, existem $y_1, \cdots, y_m, z_1, \cdots, z_l \in L$ tais que*

$$L = K(y_1, \cdots, y_m)[z_1, \cdots, z_l]$$

com $\{y_1, \cdots, y_m\}$ algebricamente independente sobre K e $z_1, \cdots, z_l$ algébricos sobre $K(y_1, \cdots, y_m)$ ($\{y_1, \cdots, y_m\}$ será base de transcendência de L sobre K). Isso segue direto do Teorema 2.5.4.

2. *Nas mesmas condições, se K é algebricamente fechado, então $L = K(y_1, \cdots, y_m)$, com $\{y_1, \cdots, y_m\}$ algebricamente independente sobre K. De fato, sendo K algebricamente fechado, temos $K(y_1, \cdots, y_m)$ algebricamente fechado, e se z é algébrico sobre $K(y_1, \cdots, y_m)$, então $z \in K(y_1, \cdots, y_m)$. Daí, na notação do exemplo 1, temos*

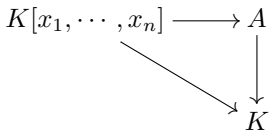
$$L = K(y_1, \cdots, y_m)[z_1, \cdots, z_l] = K(y_1, \cdots, y_m).$$

□

A seguir, apresentarei uma técnica muito útil (principalmente na geometria algébrica) que será utilizada para demonstrar um dos teoremas de Amitsur: especializações.

Definição 2.5.8. Sejam $A = K[a_1, \cdots, a_n]$ álgebra finitamente gerada sobre K. Uma **especialização** de A em K é um homomorfismo de anéis $\varphi : A \to K$.

Observação. Sejam $A = K[a_1, \cdots, a_n]$ álgebra finitamente gerada sobre K, considere o anel de polinômios $K[x_1, \cdots, x_n]$ e o homomorfismo $\pi : K[x_1, \cdots, x_n] \to A$ tal que $\pi(x_i) = a_i, i = 1, \cdots, n$. Equivalentemente, $\varphi : A \to K$ é uma especialização se e só se existe $\bar{\varphi} : K[x_1, \cdots, x_n] \to K$ tal que o seguinte diagrama é comutativo:



Uma especialização é sempre uma extensão de uma substituição $a_i \mapsto b_i \in K, i = 1, \cdots, n$. Mas, nem toda substituição $a_i \mapsto b_i \in K, i = 1, \cdots, n$, é uma especialização, pois nem sempre está bem definida.

Exemplo:

(i) Sejam $K = \mathbb{Q}$ e considere $A = \mathbb{Q}[\sqrt{2}]$. Então, a substituição $\sqrt{2} \mapsto 1$ não se estende a uma especialização. De fato, se existir um homomorfismo de álgebras $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}$ tal que $\varphi(\sqrt{2}) = 1$, então, teríamos

$$0 = \varphi(0) = \varphi(\sqrt{2}^2 - 2) = \varphi(\sqrt{2})^2 - \varphi(2) = 1 - 2 = -1$$

contradição.

(ii) Seja $A = k[x]/I$, em que $I = (x^4 - 16)$ o ideal gerado por $x^4 - 16$, e denote $A = K[a]$, em que $a = x + I \in A$. Então, a substituição $a \mapsto 2$ se estende a uma especialização $A \to K$.

□

Note que, no caso de $\{y_1, \cdots, y_n\}$ ser algebricamente independente sobre K, qualquer substituição $y_i \mapsto b_i \in K, i = 1, \cdots, n$, se estende a uma especialização $\varphi : K[y_1, \cdots, y_n] \to K$. Tendo isso em mente, podemos estender o conceito de especialização para corpos. Utilizaremos um símbolo extra ∞ em conjunto com o corpo K, e assumiremos as seguintes relações no conjunto $K \cup \{\infty\}$:

1. $\infty + \alpha = \alpha + \infty = \infty, \forall \alpha \in K$,

2. $\infty \cdot \alpha = \alpha \cdot \infty = \infty, \forall \alpha \in K, \alpha \neq 0$,

3. $\infty \cdot 0 = 0 \cdot \infty = 0$.

A inclusão desse símbolo ∞ ficará clara após a seguinte definição:

Definição 2.5.9. Sejam $L|K$ extensão de corpos, com $L = K(y_1, \cdots, y_n)$, $\{y_1, \cdots, y_n\}$ algebricamente independente sobre K, e $\varphi : K[y_1, \cdots, y_n] \to K$ uma especialização. Uma **especialização de corpos** $\psi : L \to K \cup \{\infty\}$ é uma aplicação tal que, dados $\frac{f}{g} \in L$,

$$\psi\left(\frac{f}{g}\right) = \begin{cases} \infty & , \text{ se } \varphi(g_1) = 0, \text{ para todo } g_1 \in K[y_1, \cdots, y_n], \text{ tal que } \frac{f}{g} = \frac{f_1}{g_1}, \\ \frac{\varphi(f_1)}{\varphi(g_1)} & , \text{ para algum } \frac{f_1}{g_1} = \frac{f}{g}, \text{ com } \varphi(g_1) \neq 0. \end{cases}$$

Exemplo: *Existe uma especialização $\psi : L \to K$, em que $\psi(a) \neq 0, \forall a \in L$ com $a \neq 0$ e $\psi(a) \neq \infty, \forall a \in L$, se e só se $L \simeq K$.* □

Quando não houver ambiguidades, omitiremos o termo "de corpos" e o símbolo ∞, e diremos simplesmente "especialização $\psi : K(y_1, \cdots, y_n) \to K$". A especialização, assim definido, possui propriedades boas com relação a soma e produto no anel:

Proposição 2.5.10. *Segundo a notação da definição 2.5.9, temos*

(i) ψ está bem definida,

(ii) $\psi\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) = \psi\left(\frac{f_1}{g_1}\right) + \psi\left(\frac{f_2}{g_2}\right)$, *se* $\psi\left(\frac{f_1}{g_1}\right) \neq \infty$ *e* $\psi\left(\frac{f_2}{g_2}\right) \neq \infty$,

(iii) $\psi\left(\frac{f_1}{g_1} \cdot \frac{f_2}{g_2}\right) = \psi\left(\frac{f_1}{g_1}\right) \cdot \psi\left(\frac{f_2}{g_2}\right)$, *se* $\psi\left(\frac{f_1}{g_1}\right) \neq \infty$ *e* $\psi\left(\frac{f_2}{g_2}\right) \neq \infty$,

Demonstração. (i) Se todo $g_1 \in K[y_1, \cdots, y_n]$ tal que $\frac{f}{g} = \frac{f_1}{g_1}$ é tal que $\varphi(g_1) = 0$, então $\psi(f/g) = \infty$ e está bem definido. Então, assuma $\frac{f_1}{g_1} = \frac{f_2}{g_2}$, ou seja, $f_1 g_2 = f_2 g_1$, com $\varphi(g_1) \neq 0$ e $\varphi(g_2) \neq 0$. Daí $\psi\left(\frac{f_1}{g_1}\right) = \psi\left(\frac{f_2}{g_2}\right)$ se e só se $\varphi(f_1)\varphi(g_2) = \varphi(f_2)\varphi(g_1)$, e a segunda ocorre, pois φ é homomorfismo de anéis.

(ii) Assumindo $\varphi(g_1) \neq 0$ e $\varphi(g_2) \neq 0$ (o que implica $\varphi(g_1 g_2) \neq 0$), temos

$$\psi\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) = \psi\left(\frac{f_1 g_2 + f_2 g_1}{g_1 g_2}\right) = \frac{\varphi(f_1)\varphi(g_2) + \varphi(f_2)\varphi(g_1)}{\varphi(g_1)\varphi(g_2)} = \psi\left(\frac{f_1}{g_1}\right) + \psi\left(\frac{f_2}{g_2}\right)$$

(iii) Assumindo $\varphi(g_1) \neq 0$ e $\varphi(g_2) \neq 0$ (o que implica $\varphi(g_1 g_2) \neq 0$), temos

$$\psi\left(\frac{f_1}{g_1}\frac{f_2}{g_2}\right) = \frac{\varphi(f_1 f_2)}{\varphi(g_1 g_2)} = \frac{\varphi(f_1)\varphi(f_2)}{\varphi(g_1)\varphi(g_2)} = \psi\left(\frac{f_1}{g_1}\right)\psi\left(\frac{f_2}{g_2}\right)$$

e vale a igualdade.

□

Uma especialização $\psi : L \to K \cup \{\infty\}$ induz uma **especialização no anel de matrizes** $\psi_n : M_n(L) \to M_n(K \cup \{\infty\})$ dada por: se $(a_{ij}) \in M_n(L)$, então $\psi_n(a_{ij})$ é a matriz $(\psi(a_{ij}))$, ou seja, a entrada (i, j) de $\psi_n(a_{ij})$ é $\psi(a_{ij})$.

Proposição 2.5.11. *Sejam $\psi : L \to K \cup \{\infty\}$ especialização, $\psi_n : M_n(L) \to M_n(K \cup \{\infty\})$ a especialização induzida e $a, b \in M_n(L)$. Então, se $\psi_n(a)$ e $\psi_n(b)$ contêm todas as entradas diferentes de ∞, valem:*

(i) $\psi_n(a+b) = \psi_n(a) + \psi_n(b)$,

(ii) $\psi_n(ab) = \psi_n(a)\psi_n(b)$.

Demonstração. Segue pela definição de soma e produto de matrizes e pela proposição 2.5.10. □

§2.6 Teorema de Wedderburn-Artin

Nesta seção, apresentaremos mais noções da álgebra não comutativa, e estudaremos algumas de suas propriedades (anéis primos, anéis completamente redutíveis e semiprimos). No fim, demonstraremos o teorema de Wedderburn-Artin, que caracteriza a estrutura de anéis completamente redutíveis.

A teoria desenvolvida nesta seção é importante pela linguagem, para exemplos e contra-exemplos e pelo importantíssimo teorema de estrutura de Wedderburn e Artin. Os conceitos desenvolvidos serão explorados no estudo de representações do grupo simétrico S_n, principalmente.

Como usual nesta dissertação, consideraremos anéis associativos, não necessariamente comutativos e não necessariamente com unidade, e a teoria será baseada nos livros de Jacobson [24], Herstein [20] e principalmente em Lambek [25].

2.6.1 Anéis Primos

Começaremos com a definição e caracterização básica de ideal primo e um primeiro resultado importante neste sentido:

Definição 2.6.1. Um ideal $P \triangleleft R$ é dito ser **primo** se, para todos $A, B \triangleleft R$ ideais tais que $AB \subset P$, tem-se $A \subset P$ ou $B \subset P$.

Lema 2.6.2. *Seja $P \triangleleft R$ um ideal. São equivalentes:*

(i) P é ideal primo, ou seja, para todos $A, B \triangleleft R$, com $AB \subset P$, tem-se $A \subset P$ ou $B \subset P$,

(ii) Para cada $I \triangleleft R$, $I \nsubseteq P$, tem-se $(I : P) := \{x \in R : xI \subset P\} = P$,

(iii) Para todos $a, b \in R$ tais que $aRb \subset P$, tem-se $a \in P$ ou $b \in P$,

(iv) Para todos $a, b \in R$ tais que $a(\mathbb{Z} + R)b := \{arb + nab : r \in R, n \in \mathbb{Z}\} \subset P$, tem-se $a \in P$ ou $b \in P$.

As mesmas equivalências valem trocando ideais A, B e I por ideais à direita, ou à esquerda.

Demonstração. $(i) \Rightarrow (ii)$: Seja $x \in (I : P)$. Então $((\mathbb{Z} + R)x(\mathbb{Z} + R))I \subset P$, e daí, como $I \nsubseteq P$, temos $(\mathbb{Z} + R)x(\mathbb{Z} + R) \subset P$, e em particular, $x \in P$, o que implica $(I : P) \subset P$. Certamente $P \subset (I : P)$ e vale a igualdade.
$(ii) \Rightarrow (iii)$: Sejam $a, b \in R$ tais que $aRb \subset P$. Assuma $Rb(\mathbb{Z} + R) \nsubseteq P$. Então, $a \in (Rb(\mathbb{Z} + R) : P) = P$ e vale a afirmação. Se $Rb(\mathbb{Z} + R) \subset P$, então, se $b \notin P$, então $(\mathbb{Z} + R)b(\mathbb{Z} + R) \nsubseteq P$, mas $b(\mathbb{Z} + R)b(\mathbb{Z} + R) \subset Rb(\mathbb{Z} + R) \subset P$, absurdo, pois implicaria $b \in ((\mathbb{Z} + R)b(\mathbb{Z} + R) : P)$, mas $b \notin P$. Segue que $b \in P$ e vale a afirmação.
$(iii) \Rightarrow (iv)$: Sejam $a, b \in R$ tais que $a(\mathbb{Z} + R)b \in P$. Então, em particular, $aRb \subset P$, o que implica

$a \in P$ ou $b \in P$ e vale.
$(iv) \Rightarrow (i)$: Assuma $A, B \subset R$ ideais de modo que $A \nsubseteq P$ e $AB \subset P$. Logo, existe $a \in A$ com $a \notin P$. Daí, para cada $b \in B$, tem-se $a(\mathbb{Z}+R)b \subset AB \subset P$, portanto, $a \in P$ ou $b \in P$, e como a primeira não ocorre, segue que $b \in P$, ou seja, $B \subset P$. □

Teorema 2.6.3. *Seja $P \lhd R$ um ideal primitivo. Então P é primo.*

Demonstração. Sejam $M \lhd_r R$ modular maximal tal que $P = (M : R)$ e $a, b \in R$ com $a(\mathbb{Z}+R)b \subset P$. Assuma $a \notin P$. Então, $(\mathbb{Z}+R)a(\mathbb{Z}+R) \nsubseteq P$, e em particular, $(\mathbb{Z}+R)a(\mathbb{Z}+R) \nsubseteq M$, e daí $M + (\mathbb{Z}+R)a(\mathbb{Z}+R) = R$. Segue que

$$R(P + (\mathbb{Z}+R)b(\mathbb{Z}+R)) = (M + (\mathbb{Z}+R)a(\mathbb{Z}+R))(P + (\mathbb{Z}+R)b(\mathbb{Z}+R)) \subset$$
$$\underbrace{M+P}_{\subset M} + (\mathbb{Z}+R)\underbrace{a(\mathbb{Z}+R)b}_{\subset P}(\mathbb{Z}+R) \subset M + P \subset M$$

implica em $P + (\mathbb{Z}+R)b(\mathbb{Z}+R) \subset (M : R) = P$, e segue que, $(\mathbb{Z}+R)b(\mathbb{Z}+R) \subset P$, e em particular, $b \in P$ e vale o resultado. □

Definição 2.6.4. Um anel R é dito ser **primo** se $0 \lhd R$ for um ideal primo.

Exemplo: *Um ideal $P \lhd R$ é primo se e só se R/P é um anel primo.* □

Na álgebra comutativa, um anel é primo se e só se é domínio. Na álgebra não comutativa, o máximo que conseguimos garantir é que, num anel primo, o produto de ideais se comporta como um domínio, isto é, as equivalentes afirmações do lema 2.6.2, para o caso $P = 0$ primo, ficam: R é primo se e só se $AB = 0$ implica $A = 0$ ou $B = 0$, para $A, B \lhd R$, e se e só se $\mathrm{Ann}_R(I) = 0$, para cada $I \lhd R$, $I \neq 0$.

No caso geral, um anel primo quase nunca será domínio:
Exemplo: *Pelo teorema 2.6.3, todo anel primitivo é anel primo. Pelo mencionado na seção 2.1, $M_n(D)$ são anéis primitivos, para D anel de divisão, e então, anéis primos. Mas, se $n > 1$, então $M_n(D)$ não é domínio.* □

Um anel primo não admite ideais não nulos nilpotentes, pois se $I \lhd R$ é tal que $I^n = 0$, então $I^{n-1} \subset \mathrm{Ann}(I)$. Mas, pelo lema 2.6.2, $\mathrm{Ann}(I)$ pode ser 0 (se $I \neq 0$) ou R (se $I = 0$). Daí, se $I \neq 0$, e $n \in \mathbb{N}$ é o menor natural tal que $I^n = 0$, teríamos $I^{n-1} \subset \mathrm{Ann}(I) = 0$, o que é uma contradição.

Uma álgebra prima não possui ideais nilpotentes, pelo comentário acima, e uma classe importante de álgebras são as álgebras que não possuem ideais nilpotentes. Uma teoria foi desenvolvida por Baer em [37] neste sentido. Provaremos posteriormente um resultado, como consequência da teoria desenvolvida, envolvendo PI-álgebras que não possuem ideais nilpotentes.

Definição 2.6.5. Seja R um anel. O **radical de Baer** (ou o radical primo, ou nilradical) é definido por

$$B(R) = \bigcap_{P \lhd R \text{ primo}} P.$$

Se R não admite ideais primos, então define-se $B(R) = R$.

Observação. Como todo ideal primitivo é primo, temos $B(R) \subset J(R)$, o radical de Jacobson.

Na álgebra comutativa, $B(R)$ é exatamente o conjunto de todos os elementos nilpotentes de R. Em geral, temos que criar um conceito mais forte:

Definição 2.6.6. Seja R um anel. Um elemento $a \in R$ é dito ser **fortemente nilpotente** se para toda sequência $a_0, a_1, a_2, \cdots$ de elementos de R satisfazendo:

(i) $a_0 = a$,

(ii) $a_n \in a_{n-1}Ra_{n-1}, \forall n \geq 1$.

implica que existe $m \in \mathbb{N}$ tal que $a_m = 0$.

Observação. (i) Uma sequência $a_0, a_1, a_2, \cdots$, de elementos de R tal que $a_n \in a_{n-1}Ra_{n-1}, \forall n \geq 1$, é denominada **m-sequência**.

(ii) Um elemento fortemente nilpotente é nilpotente. De fato, se $a \in R$ é fortemente nilpotente, então a sequência $a_0 = a, a_1 = a^3, a_2 = a^7, \cdots$, é tal que $a_n \in a_{n-1}Ra_{n-1}, \forall n \geq 1$, portanto, existe $m \in \mathbb{N}$ tal que $0 = a_m = a^n$, para algum $n \in \mathbb{N}$ adequado (não importa muito determinar n em função do subíndice m).

(iii) Na álgebra comutativa, todo elemento nilpotente é fortemente nilpotente. De fato, neste caso, uma m-sequência é da forma $a_0, a_1, a_2, \cdots$, com $a_n = c_n a^{2^n-1}$, para algum $c_n \in R, n \geq 1$. Daí, existir $m \in \mathbb{N}$ com $a^m = 0$ implica que $a_n = 0$, para todo $n \in \mathbb{N}$ tal que $2^n - 1 \geq m$.

Assim, conseguimos uma caracterização mais precisa do radical de Baer:

Proposição 2.6.7. $B(R) = \{a \in R : a \text{ é fortemente nilpotente}\}$

Demonstração. Assuma $a \in B(R)$. Então, existe $P \lhd R$ primo tal que $a \notin P$. Então, existe $r_1 \in R$ tal que $a_1 = ar_1a \notin P$ (lema 2.6.2.(iii)) e em particular, $a_1 \neq 0$. Por indução, tendo $a_1, \cdots, a_n$, com $a_1, \cdots, a_n \notin P$, existe $r_{n+1} \in R$ tal que $a_{n+1} := a_n r_{n+1} a_n \notin P$. Daí, a não é fortemente nilpotente, pois $a_0 = a, a_1, a_2, \cdots$ é uma m-sequência iniciada em a que não se anula.

Se a não é fortemente nilpotente, existe m-sequência $a_0, a_1, a_2, \cdots$ que não se anula. Seja $P \lhd R$ um ideal maximal com a propriedade $a_n \notin P, \forall n \geq 0$ (existe pelo menos um, pois 0 é um ideal que satisfaz isso, e existe um maximal, pelo lema de Zorn). Provaremos que P é primo. Sejam $x, y \in R$ com $x, y \notin P$. Então, como $P \subsetneq P + RxR$ e $P \subsetneq P + RyR$, por maximalidade de P, existem $a_{m_1} \in P + RxR$ e $a_{m_2} \in P + RyR$. Como $a_n \in I$ implica $a_{n+1} \in I$, para qualquer ideal bilateral $I \subset R$ e qualquer $n \geq 0$, temos que existe $m \in \mathbb{N}$ tal que $a_m \in (P + RxR) \cap (P + RyR)$. Daí

$$a_{m+1} \in (P + RxR)(P + RyR) \subset P + RxRyR$$

e então, necessariamente $xRy \nsubseteq P$ (pois se não, teríamos $a_{m+1} \in P$, contradição), o que implica P primo. Logo $a \notin B(R)$. □

Definição 2.6.8. Define-se um anel R por **semiprimo** se $B(R) = 0$.

Lema 2.6.9. *$R/B(R)$ é semiprimo e se $I \lhd R$ é tal que R/I é semiprimo, então $B(R) \subset I$.*

Vale ressaltar que, se $I \lhd R$ é nilpotente, então $I \subset B(R)$. De fato, se $I^n = 0$, segue que toda m-sequência iniciada em a, satisfaz $a_m \in I^{2^m-1}$, e daí, $a_m = 0$, para $2^m - 1 > n$. Mais geralmente, se $I \subset R$ é um ideal (bilateral, à esquerda, ou à direita) tal que existe $n \in \mathbb{N}$ com $I^n \subset B(R)$, então $I \subset B(R)$. De fato, se $I^n \subset B(R)$, implica que para cada ideal primo $P \subset R$, temos $I^n \subset P$, e daí, $I^{n-1} \subset P$ ou $I \subset P$, e ambos implicam $I^{n-1} \subset P$, e segue que $I^{n-1} \subset B(R)$, o que implica a afirmação por indução em $n \in \mathbb{N}$. Para futuras referências, denominaremos esse fato como proposição:

Proposição 2.6.10. *Seja R um anel e $B(R)$ seu radical de Baer. Então, se $I \subset R$ é um ideal (bilateral, à direita, à esquerda) tal que existe $n \in \mathbb{N}$ com $I^n \subset B(R)$, temos que $I \subset B(R)$.*

Com isso, podemos demonstrar uma caracterização de anéis semiprimos:

Proposição 2.6.11. *São equivalentes:*

(i) *R é semiprimo,*

(ii) *$0 \lhd R$ é o único ideal nilpotente de R,*

(iii) *Se $A, B \lhd R$ são tais que $AB = 0$, então $A \cap B = 0$.*

Demonstração. $(i) \Rightarrow (ii)$: Seja $I \lhd R$ um ideal nilpotente. Segue que, pelo comentário acima, $I \subset B(R) = 0$.
$(ii) \Rightarrow (iii)$: Sejam $A, B \lhd R$ com $AB = 0$. Então $(A \cap B)^2 \subset AB = 0$, e daí, $A \cap B$ é nilpotente, o que implica $A \cap B = 0$.
$(iii) \Rightarrow (i)$: Seja $a \in R, a \neq 0$. Se, para todo $r \in R$, tivermos $ara = 0$, então, em particular,

$$RaRRaR \subset R\underbrace{aRa}_{0}R = 0$$

e daí, $RaR = (RaR) \cap (RaR) = 0$. Em particular, sendo $I_a = (\mathbb{Z} + R)a(\mathbb{Z} + R)$, temos $I_a^3 = 0$, o que implica $I_a^2 I_a = 0$, ou seja, $I_a^2 = I_a^2 \cap I_a = 0$, e da mesma forma, $I_a = I_a \cap I_a = 0$, e daí, $a = 0$, absurdo. Segue que todo $a \in R, a \neq 0$, não é fortemente nilpotente, e então, $B(R) = 0$. □

2.6.2 Módulos Completamente Redutíveis

A seguir, desenvolveremos uma teoria de anéis e módulos completamente redutíveis. Originalmente, a teoria foi desenvolvida para anéis semiprimitivos Artinianos. Mas, os resultados dessa teoria podem ser provados com hipóteses mais fracas (primo e semiprimo), e serão feitos assim nesta seção, pois alguns dos lemas serão importantes na teoria de representações.

Começaremos estudando módulos, com uma definição que será útil ao restringir os estudos para anéis:

Definição 2.6.12. Seja A um R-módulo pela direita. Define-se o **radical** de A por

$$J(A) := \bigcap \{M \subset A \text{ submódulo: } A/M \text{ é } R\text{-módulo irredutível}\}$$

Se A não admite tais submódulos, então $J(A) = A$.

Observação. Considerando um anel R como um R-módulo, as noções do radical $J(R)$ definido agora e o radical de Jacobson coincidem (lema 2.2.4).

O conceito mais importante para estudar módulos (ou anéis) completamente redutíveis é o seguinte:

Definição 2.6.13. Seja A um R-módulo. Define-se a **base de** A por

$$S(A) = \sum_{\substack{M \subset A \text{ submódulo} \\ \text{irredutível}}} M.$$

Define-se $S(A) = 0$, se A não admite submódulos irredutíveis.

Definição 2.6.14. Um R-módulo A é denominado **completamente redutível** (ou semissimples, mas evitaremos este termo aqui) se $A = S(A)$.

Proposição 2.6.15. *Seja A um R-módulo. Então:*

(i) Existe uma família de R-submódulos irredutíveis $\{N_\alpha\}_{\alpha\in I}$ tal que

$$S(A) = \bigoplus_{\alpha\in I} N_\alpha.$$

(ii) $S(A)$ é invariante por endomorfismos.

Demonstração. (i) Seja $\mathscr{F} = \{N \subset A \text{ submódulo irredutível}\}$ e denomine um subconjunto $\mathscr{I} \subset \mathscr{F}$ de direto se a soma $\sum_{N\in\mathscr{I}} N$ for direta. Pelo lema de Zorn, existe $\mathscr{T} \subset \mathscr{F}$ maximal. Então, defina

$$B := \bigoplus_{N\in\mathscr{T}} N \subset S(A).$$

Como cada $N \in \mathscr{F}$ é irredutível, temos $N \cap B = 0$ ou $N \cap B = N$. Se $B \neq S(A)$, então existe $N \in \mathscr{F}$ tal que $N \cap B = 0$, contradizendo a maximalidade de $\mathscr{F}$ (pois $\mathscr{T} \cup \{N\}$ será direto). Daí $B = S(A)$.

(ii) Seja N um R-módulo irredutível e $F : A \to A$ um homomorfismo de R-módulos. Então, $\operatorname{Ker} f|_N$ é um R-submódulo de N, e daí, $f|_N$ é tal que $f(N) = 0 \subset S(A)$ ou $f(N) \simeq N$ (e $f(N) \subset S(A)$, pois $f(N)$ será irredutível). O resultado segue.

□

Provaremos algumas propriedades importantes de módulos completamente redutíveis, e para isso, provaremos algumas equivalências envolvendo mais conceitos:

Definição 2.6.16. Um submódulo $B \subset A$ é denominado **grande** se, para todo $C \subset A$ submódulo não nulo, tem-se $B \cap C \neq 0$.

Um módulo A admite submódulos grandes se existe um conjunto não nulo de A que necessariamente deve estar contido em todos os submódulos de A.

Proposição 2.6.17. *Sejam $B \subset A$ submódulo e $C \subset A$ submódulo maximal com a propriedade $B \cap C = 0$. Então $B + C$ é grande.*

Demonstração. Seja $D \subset A$ um submódulo com $(B + C) \cap D = 0$. Então, $B \cap (C + D) = 0$, de fato, se $b = c + d \in B \cap (C + D)$, então, $d = b - c \in (B + C) \cap D = 0$. Como $B \cap C = 0$, temos $b = c \in B \cap C = 0$, e daí $B \cap (C + D) = 0$. Por maximalidade de C, temos necessariamente $C + D = C$, ou seja, $D \subset C$, portanto, $D \subset (B + C) \cap D = 0$, o que implica $D = 0$, e daí $B + C$ é grande. □

Definição 2.6.18. Seja A um R-módulo. Denomina-se A **com complementos** se para todo R-submódulo $B \subset A$, existe R-submódulo $B' \subset A$ tal que $A = B \oplus B'$.

Lema 2.6.19. *Sejam R anel e A um R-módulo com complementos.*

(i) Se $B \subset A$ é submódulo, então B é com complementos,

(ii) Se R admite unidade 1*, então* $J(A) = 0$.

Demonstração. (i) Sejam $B \subset A$ um R-módulo e $C \subset B$ um R-submódulo. Então $C \subset A$ é submódulo, e daí, existe $C' \subset A$ submódulo com $A = C \oplus C'$. Defina $C'' = C' \cap B$. Claro que $C \cap C'' = 0$, e como $A = C + C'$, temos

$$C + C'' = C \cap B + C' \cap B = (C + C') \cap B = A \cap B = B$$

(a segunda igualdade é não trivial e utiliza-se o fato de $C \subset B$) e daí $B = C \oplus C''$.

(ii) Seja $a \in A, a \neq 0$, e considere M_a um submódulo maximal com a propriedade $a \notin M_a$. Assuma $N \subset A$ submódulo com $M_a \subset N$. Então, existe $N' \subset A$ submódulo tal que $A = N \oplus N'$. Mas, como $N' + M_a = N' \oplus M_a$, e $a \in N \supset M_a$, temos necessariamente $a \notin N' + M_a$ (pois se não, $N + N'$ não seria soma direta, por existir duas representações distintas para a) e daí $N' = 0$. Segue que M_a é maximal, e então, A/M_a é irredutível (pois R admite unidade).

□

Com esses lemas provados, podemos relacionar todas as definições:

Teorema 2.6.20. *Sejam R um anel com unidade* 1 *e A um R-módulo. São equivalentes:*

(i) A é completamente redutível,

(ii) A não admite submódulos próprios grandes,

(iii) A admite complementos.

Demonstração. $(i) \Rightarrow (ii)$: Seja $B \subset A$ um submódulo grande. Para cada $N \subset A$ submódulo irredutível, temos $N \cap B = 0$ ou $N \cap B = N$, e como B é grande, o primeiro não ocorre. Daí $N \cap B = N$, e em particular, $N \subset B$. Daí, segue que $A = S(A) \subset B$, e então, $B = A$.
$(ii) \Rightarrow (iii)$: Seja $B \subset A$ um submódulo e considere $C \subset A$ submódulo com a propriedade $C \cap B = 0$. Então $C + B = C \oplus B$, e ainda, pela proposição 2.6.16, $C + B$ é grande, ou seja, $A = B \oplus C$.
$(iii) \Rightarrow (i)$: Seja $B = S(A)$. Então, existe $C \subset A$ submódulo tal que $A = B \oplus C$. Se $C \neq 0$, então existe $c \in C, c \neq 0$. Considere M_c um submódulo maximal com a propriedade $c \notin M_c$ e $B \subset M_c$. Então, por mesmo argumento do lema 2.6.19.(ii), temos M_c maximal, portanto, sendo A com complementos, existe $N_c \subset A$ submódulo tal que $A = M_c \oplus N_c$, mas, $N_c \simeq A/M$ é irredutível, o que implica $N_c \subset S(A) \subset M_c$, donde chega-se a uma contradição. Daí $B = S(A) = A$. □

Seja $E = \mathrm{End}_R(A)$. Temos A um (E, R)-bimódulo. Dado $N \subset A$ R-módulo irredutível, temos EN um (E, R)-subbimódulo de A (argumento da proposição 2.6.15.(ii)).

Definição 2.6.21. EN é denominada uma **componente homogênea** do (E, R)-bimódulo A.

Lema 2.6.22. *Sejam R anel com unidade* 1*, A um R-módulo completamente redutível, com $R = \bigoplus_{i=1}^{m} A_i$ soma finita de R-módulos irredutíveis e $N \subset A$ R-submódulo irredutível. Então $EN = \sum\{A_i \subset A$ R-submódulo:$A_i \simeq N\}$.*

Demonstração. Seja $F = \sum\{A_i \subset A$ R-submódulo: $A_i \simeq N\}$. Para cada $e \in E$, temos $eN \simeq N \subset F$ ou $eN = 0 \subset F$. Reciprocamente, considere $\pi_i : R \to R_i$ as projeções. Seja A_i irredutível com $N \simeq A_i$ e seja $e_0 : N \to A_i$ o isomorfismo. Escreva $A = N \oplus N'$ (possível, pois A é completamente redutível), e chame $\pi : A \to N$ a projeção e defina $e = \pi_i e_o \pi \in E$, temos $EN \supset eN = A_i$, e o resultado segue. □

2.6.3 Anéis Completamente Redutíveis

Definição 2.6.23. Um anel R é dito **completamente redutível** se, visto como um R-módulo pela direita, for completamente redutível.

Como consequência da estrutura de módulos completamente redutíveis, temos

Proposição 2.6.24. *Seja R um anel completamente redutível e M um R-módulo irredutível. Então, existe um ideal minimal $I \lhd_r R$ tal que $M \simeq I$ como R-módulos.*

Demonstração. Sendo M irredutível (por argumentos já utilizados nesta dissertação), para todo $m \in M, m \neq 0$, temos $mR \simeq M$. Considere a aplicação $\psi : r \in R \mapsto mr \in M$. Sendo R completamente redutível, existe $I \subset R$ ideal à direita tal que $\operatorname{Ker}\psi \oplus I = R$, e ainda, $M \simeq R/\operatorname{Ker}\psi \simeq I$, e, sendo M irredutível, temos I minimal, e isso prova o resultado. □

Começaremos exibindo a estrutura de ideais minimais em anéis semiprimos:

Lema 2.6.25. *Seja $K \lhd_r R$ minimal. Então $K^2 = 0$ ou existe $e \in R$ idempotente tal que $K = eR$.*

Demonstração. Assuma $K^2 \neq 0$. Então, como $K^2 \subset K$ é ideal, temos $K^2 = K$, e existe $e \in K$ tal que $Ke = K$ (pois existe $e \in K$ tal que $Ke \neq 0$, mas $Ke \subset K$ é um ideal não nulo pela direita). Daí, $Ke^2 = Ke$, e então, $K(e^2 - e) = 0$. Considere $I = \{r \in R : Kr = 0\}$. Temos I ideal à direita, e $I \cap K \subset K$, e sendo K minimal, temos $I \cap K = 0$ ou $I \cap K = K$ (o que não ocorre, pois $e \notin I \cap K$), portanto, $K \cap I = 0$. Como $e^2 - e \in K \cap I$, temos $e^2 - e = 0$, ou seja, $e^2 = e$, logo e é idempotente. □

Corolário 2.6.26. *Se R é semiprimo e $K \lhd_r R$ é minimal, então existe $e \in R$ idempotente tal que $K = eR$.*

Demonstração. Pela proposição 2.6.11, R não admite ideais nilpotentes, e daí, dado $K \lhd_r R$ minimal, se $K^2 = 0$, então $K = 0$. Segue, pelo lema 2.6.25, que existe idempotente $e \in R$ tal que $K = eR$. □

Lema 2.6.27. *Sejam R anel, $e, f \in R$ com e idempotente. Então $Hom_R(eR, fR) \simeq fRe$ como grupos abelianos aditivos. Se $e = f$, então são isomorfos como anéis.*

Demonstração. Considere a aplicação $\phi : x = fre \in fRe \mapsto \phi_x \in \operatorname{Hom}_R(eR, fR)$, em que $\phi_x(ey) = xey = ferey$. Temos ϕ bem definido, homomorfismo de grupos e ainda, dado $\varphi \in \operatorname{Hom}_R(eR, fR)$, seja $x = \varphi(e) = \varphi(ee) \in fR$. Note que $x \in fRe$, pois $x = \varphi(e) = \varphi(eee) = \varphi(ee)e = xe$. Então, para todo $er \in eR$, temos $\phi_x(er) = xer = \varphi(e)er = \varphi(eer) = \varphi(er)$, e daí $\phi(x) = \varphi$, e isso mostra que ϕ é sobre. Se $\phi(fre) = 0$, então $\phi_{fre}(ez) = freez = 0$, para todo $ez \in eR$, e em particular, tomando $z = e$, temos $fre = 0 \in fRe$, ou seja, ϕ é 1-1.

Se $e = f$, então a aplicação ϕ satisfaz $\phi(exeeye) = \phi_{exe}\phi_{eye}$, pois

$$\phi_{exeeye}(er) = exeeyeer$$
$$\phi_{exe}(\phi_{eye}(er)) = \phi_{exe}(eyeer) = exeeyeer$$

e daí ϕ é isomorfismo de anéis, e isso prova o resultado. □

Como consequência, obtemos:

Corolário 2.6.28. *Sejam R anel semiprimo e $I, J \subset R$ dois ideais minimais à direita e $\varphi : I \to J$ um homomorfismo de anéis. Então, existe $r \in R$ tal que $a \in I \mapsto ra \in J$ coincide com ϕ.*

Demonstração. Segue direto da caracterização de ideais minimais (lema 2.6.26) e da caracterização de $\mathrm{Hom}_R(I, J)$ (lema 2.6.27). □

Vale relembrar que dado um R-módulo irredutível A, $\mathrm{Hom}_R(A, A)$ é um anel de divisão (isso segue olhando os R-submódulos $\mathrm{Ker}\, f, \mathrm{Im}\, f$ de A, para cada $f \in \mathrm{Hom}_R(A, A)$, e pelo fato de A ser irredutível). Ainda, dado $e \in R$ idempotente, temos que eRe é um anel, e admite unidade e, como pode ser facilmente observado.

O próximo resultado apresenta uma caracterização importante para ideais minimais em anéis primos:

Lema 2.6.29. *Seja R semiprimo e $e \in R$ idempotente. São equivalentes:*

(i) $eR \lhd_r R$ *é ideal minimal,*

(ii) eRe *é anel de divisão,*

(iii) $Re \lhd_l R$ *é minimal.*

Demonstração. $(i) \Rightarrow (ii)$: Neste caso, o eR é um R-módulo irredutível, e então, utilizando o lema 2.6.27, temos $eRe \simeq \mathrm{Hom}_R(eR, eR)$, e este último é anel de divisão, pelo comentário acima.
$(ii) \Rightarrow (i)$: Seja $r \in R$ com $er \neq 0$. Então, sendo R semiprimo, temos $erRer \neq 0$ (pois se não, pela proposição 2.6.12.(iii), teríamos $(\mathbb{Z} + R)er(\mathbb{Z} + R)(\mathbb{Z} + R)er(\mathbb{Z} + R) \subset erRer = 0$, logo, $(\mathbb{Z} + R)er(\mathbb{Z} + R) = (\mathbb{Z} + R)er(\mathbb{Z} + R) \cap (\mathbb{Z} + R)er(\mathbb{Z} + R) = 0$, contradição). Segue que existe $t \in R$ com $erter \neq 0$, e em particular, $erte \neq 0$. Portanto, existe $ese \in eRe$ tal que $(erte)(ese) = (ese)(erte) = e$. Segue que $erR = eR$, pois dado $x \in R$, temos $ex = (erte)(ese)x = er(tese)x \in erR$. Daí, dado $I \subset eR$ ideal não nulo e $i \in I$ não nulo, existe $j \in R$ tal que $i = ej$, e como consequência, $ei = e(ej) = ej = i \neq 0$, o que implica $eR = eiR = iR \subset I$, de onde se tem eR minimal.
$(i) \iff (iii)$: Análogo. □

A seguir, apresentaremos alguns resultados técnicos que serão importantes na demonstração do Teorema de Wedderburn-Artin:

Lema 2.6.30. *Sejam $e, f \in R$ idempotentes. Então $eR \simeq fR$ se e só se existem $u, v \in R$ com $vu = e$ e $uv = f$.*

Demonstração. Assuma primeiramente $eR \simeq fR$. Pelo lema 2.6.27, existe $u \in fRe$ tal que $ex \mapsto uex \in fR$ é isomorfismo. Temos $u = fu = ue = fue$. Ainda, existe $v \in eRf$ tal que $fx \in fR \mapsto vfx \in eR$ é isomorfismo, e $v = ev = vf = evf$. Daí $e = vue = vu$ e $f = uvf = uv$.

Reciprocamente, suponha $u, v \in R$ tais que $vu = e$ e $uv = f$. Então $ue = u(vu) = (uv)u = fu$. Da mesma forma, $vf = vuv = ev$. Considere uma aplicação $eR \to fR$ dado por $ex \in eR \mapsto uex \in fR$ (que é facilmente verificado em ser homomorfismo de R-módulos), e defina também $fx \in fR \mapsto vfx \in eR$, que também é um homomorfismo de R-módulos. Compondo as aplicações, obtemos

$$fx \in fR \mapsto vfx \in eR \mapsto uvfx = f^2x = fx \in fR$$
$$ex \in eR \mapsto uex \in fR \mapsto vuex = e^2x = ex \in eR$$

e o resultado segue. □

Corolário 2.6.31. *Nas mesmas hipóteses, $eR \simeq fR$ se e só se $Re \simeq Rf$.*

Lema 2.6.32. *Suponha R semiprimo. Então:*

(i) $S(R_R) = S({}_RR)$*, em que* R_R *é o anel* R *visto como um* R*-módulo pela direita, e* ${}_RR$ *é* R *visto como um* R*-módulo à esquerda,*

(ii) As componentes homogêneas à direita de R *coincidem com as componentes à esquerda de* R*,*

(iii) As componentes homogêneas coincidem com os ideais minimais bilaterais de R*.*

Demonstração. (i) Sejam $S' = \sum eR, S'' = \sum Re$, em que a soma é entre os idempotentes $e \in R$ tal que eRe é anel de divisão (lema 2.6.29). Então, nos somatórios, os elementos idempotentes que aparecem são os mesmos. Para cada $e \in S'$, temos $Re \subset S'$, uma vez que S' é invariante por endomorfismos e R age como endomorfismo pela esquerda. Isso implica, em particular, que $S'' \subset S'$. Da mesma forma, $S'' \subset S'$ e o resultado vale.

(ii) Seja $f \in R$ idempotente com fRf anel de divisão e considere a componente homogênea de f, $H = \sum eR$, em que a soma percorre todos os idempotentes e tais que $eR \simeq fR$. Então, $H' := \sum Re$, com a soma percorrendo todos os elementos idempotentes e com $Re \simeq Rf$, temos, pelo lema 2.6.31, que o somatório contém exatamente os mesmos idempotentes. Daí, basta repetir o argumento em (i) e concluir a igualdade.

(iii) Seja $H = \sum eR \subset R$ uma componente homogênea, com cada $eR \simeq fR$, para algum idempotente $f \in R$, e considere $K \subset R$ um ideal bilateral não nulo com $K \subset H$. Sendo H R-módulo completamente redutível, segue que K será R-módulo completamente redutível, e então, $K = \sum eR$, com alguns idempotentes $e \in R$ (e todos os eR que entram no somatório são isomorfos, pois eles participam da soma que resulta em H). Pelo lema 2.6.30, existem $u, v \in R$ tais que $vu = e$ e $uv = f$. Daí $f = uev$, e então, $fR = uevR = ueR$. Segue que u realiza o isomorfismo $fR \to eR$. Como $K \subset R$ é ideal, temos $uK \subset K$, consequentemente, necessariamente $K = H$, o que conclui que H é minimal.

□

Teorema 2.6.33. *Seja* R *um anel com unidade* 1*. São equivalentes:*

(i) Todo A R*-módulo à direita é completamente redutível,*

(ii) R *é completamente redutível, como* R*-módulo pela direita,*

(iii) Todo A R*-módulo à esquerda é completamente redutível,*

(iv) R *é completamente redutível como* R*-módulo pela esquerda.*

Demonstração. (i)⇒(ii): Em particular, R é um R-módulo pela direita, e então, R é anel completamente redutível.
(ii)⇒(i): Escreva $R = \sum_{i \in I} R_i$ soma de ideais irredutíveis. Então, dado A um R-módulo, para cada $a \in R$, temos aR_i nulo ou irredutível, uma vez que $aR_i = 0$ ou $aR_i \simeq R_i$ como R-módulos. Resulta que $A = \sum_{\substack{a \in A \\ i \in I}} aR_i$.
(ii) $\iff$ (iv): Como R admite unidade e é completamente redutível, segue, por lema 2.6.19.(ii), que R é semiprimitivo, e então, R é semiprimo. Daí, o resultado segue pelo lema 2.6.32.
(iii) $\iff$ (iv): Análogo. □

Exemplo: *Seja D um anel de divisão. Então, como D é completamente redutível (por exemplo, D não admite D-submódulos próprios grandes, pois é irredutível como D-módulo), segue que todo D-módulo (D-espaço vetorial) é completamente redutível.* □

Lema 2.6.34. *Sejam R anel primo e $e \in R$ idempotente, com $eR \lhd_r R$ minimal. Denote por $S_R = S(R_R)$. Então $End_R(S_R) \simeq End_{eRe}(Re)$, em que Re é visto como um (eRe)-módulo à direita.*

Demonstração. Primeiramente, note que se H_1 e H_2 são duas componentes homogêneas distintas de R, então $H_1H_2 \subset H_1 \cap H_2 = 0$, segue que, sendo R primo, necessariamente $H_1 = 0$ ou $H_2 = 0$. Segue que existe uma única componente homogênea de R, e ainda, $S(R) = H$. Escreva $S(R) = \bigoplus e_iR$, com e_i idempotente e $e_iR \simeq eR$, para um idempotente fixo $e \in R$. Pelo lema 2.6.30, existem $u_i, v_i \in R$ tais que $u_iv_i = e_i, v_iu_i = e$, e em particular, $u_iev_i = e_i$.

Dado $\varphi \in \mathrm{End}_R(S(R))$, uma vez que $Re \subset H = S(R)$, existe $\varphi' \in \mathrm{End}_{eRe}(Re)$ tal que $\varphi(re) = \varphi'(re)$.

Seja $s \in S(R)$ e escreva $s = \sum e_ir_i = \sum u_iev_ir_i$. Então, $\varphi(s) = \sum \varphi(u_ie)v_ir_i = \sum \varphi'(u_ie)v_ir_i$, e em particular, φ é totalmente determinado por φ'. Segue que $\varphi \in \mathrm{End}_R(S(R)) \mapsto \varphi' \in \mathrm{End}_{eRe}(Re)$ é isomorfismo, e isso conclui a demonstração. □

Teorema 2.6.35 (Wedderburn-Artin)**.** *Seja R um anel com unidade 1. Então*

(i) R é completamente redutível se e só se $R = \bigoplus_{i=1}^m R_i$, com cada R_i anel completamente redutível e simples,

(ii) R é completamente redutível e simples se e só se $R \simeq M_n(D)$, para algum $n \in \mathbb{N}$ e algum D anel de divisão.

Demonstração. (i) Assuma R completamente redutível e escreva $R = \bigoplus_{i\in I} K_i$, soma direta de ideais à direita irredutíveis. Como R admite unidade $1 \in R$, existem $e_1 \in K_1, \cdots, e_n \in K_n$, com $K_1, \cdots, K_n$ alguns dos ideais dessa soma, tais que $1 = e_1 + \cdots + e_n$, e isso implica necessariamente que $R = \bigoplus_{i=1}^n K_i$.

Sejam $H_1, \cdots, H_m$ as componentes homogêneas de R (c.f. definição 2.6.21 e lema 2.6.22), temos $R = \bigoplus_{i=1}^m H_i$. Ainda, pelo lema 2.6.32, segue que $H_1, \cdots, H_m$ são ideais bilaterais minimais de R, e, sendo cada H_i um R-submódulo de R, pelo lema 2.6.19, temos que cada H_i é um R-módulo completamente redutível.

Por fim, note que, para cada $a_i \in H_i$, temos $a_iH_i = a_iR$, de fato, claro que $a_iH \subset a_iR$, e dado $r \in R$, podemos escrever $r = r_1 + \cdots + r_m$, com $r_i \in H_i, i = 1, \cdots, m$. Sendo R a soma direta dos H_i, temos $H_iH_j = 0$, se $i \neq j$, e então, $a_ir = a_i(r_1 + \cdots + r_m) = a_ir_i \in a_iH_i$. Então, vale $a_iH_i = a_iR$. Isto implica, em particular, que todas as propriedades de H_i como R-módulo são o mesmo que as propriedades de H_i como H_i-módulo, isto é, temos em particular H_i anel completamente redutível (pois vimos que é um R-módulo completamente redutível, e o comentário feito implica em ser H_i-módulo completamente redutível), e, sendo H_i ideal simples, temos H_i anel simples.

Reciprocamente, se $R = \bigoplus_{i=1}^m R_i$ é soma direta de anéis simples e completamente redutíveis, por mesmo argumento do último parágrafo, temos que cada R_i é R-módulo completamente redutível, e então, necessariamente R será R-módulo completamente redutível.

(ii) Assuma R completamente redutível e simples. Seja eR um ideal minimal de R, com e idempotente. Então, sendo $R = S(R_R)$, segue, pelo lema 2.6.27 e pelo lema 2.6.34 que

$$R \simeq \mathrm{Hom}_R(R, R) \simeq \mathrm{End}_{eRe}(Re)$$

Daí, basta mostrar que Re admite dimensão finita sobre o anel de divisão eRe, e para isso, é suficiente mostrar que Re é Noetheriano como eRe-módulo.

Primeiramente, temos que R é Noetheriano como R-módulo à direita. De fato, sendo R anel completamente redutível com unidade, pelo argumento dessa demonstração feita em (i), segue que $R = R_1 \oplus \cdots \oplus R_m$, com $R_1, \cdots, R_m$ ideais à direita irredutíveis de R. Mas, cada R_i, sendo irredutível, automaticamente é Noetheriano. Daí, como soma de R-módulos Noetherianos é novamente um R-módulo Noetheriano (c.f. proposição 1.3.5.(iv)), segue que R é Noetheriano. Em particular, sendo ReR R-submódulo de R, temos ReR Noetheriano.

Provaremos agora que Re é Noetheriano como eRe-módulo. Seja $\{K_i\}_{i\in I}$ família de eRe-submódulos de Re. Temos $K_iR \subset ReR$, e ainda, cada K_iR é ReR-módulo à direita, ou seja, $\{K_iR\}_{i\in I}$ é família de submódulos de ReR, e então, existe um elemento maximal, digamos K_mR. Agora, assuma que existe K_i tal que $K_m \subsetneq K_i$. Por maximalidade de K_mR, temos $K_mR = K_iR$. Mas, note que $K_i = K_ieRe = K_ieRe$, o que implica

$$K_m = K_mRe = K_iRe = K_i$$

contradição. Daí K_m é um elemento maximal na primeira família e Re é eRe-submódulo Noetheriano. Em particular, Re é um eRe-espaço vetorial de dimensão finita e segue o resultado.

Por fim, assuma $R = M_n(D)$. Já foi demonstrado em um exemplo desta dissertação (exemplo na página 13) que $M_n(D)$ é anel simples, e é fácil ver que as linhas das matrizes são $M_n(D)$-submódulos irredutíveis e $M_n(D)$ é a soma das linhas, ou seja, $M_n(D)$ é completamente redutível. Isso conclui o teorema.

□

§2.7 Aplicações de Wedderburn-Artin em KG

O objetivo desta seção é provar alguns resultados básicos sobre KG-módulos, que serão úteis na caracterização dos S_n-módulos irredutíveis. Para esta seção, será necessário apenas a linguagem básica de representações (seção §1.6) e noções básicas de anéis completamente redutíveis e Teorema de Wedderburn-Artin (seção §2.6).

Toda a teoria desenvolvida aqui pode ser realizada de uma outra forma utilizando teoria de caracteres (por exemplo, vide Serre [35]). Mas, faremos uma abordagem mais abstrata, envolvendo mais a linguagem e estrutura de anéis e módulos em geral, e essa teoria será baseada no livro de Curtis (vide [8]).

Pelo teorema de Maschke (Corolário 1.6.8), segue que KG é completamente redutível, se $\mathrm{car}\, K = 0$, para G grupo finito; e como $\dim_K KG < \infty$, segue, pelo Teorema de Wedderburn-Artin, que $KG = A_1 \oplus \cdots \oplus A_m$, soma de anéis simples e completamente redutíveis. Daí, todo KG-módulo é completamente redutível (teorema 2.6.33).

Como, em particular, KG é semiprimo, todo KG-módulo à esquerda irredutível é isomorfo a um ideal minimal à esquerda (proposição 2.6.24), e este é sempre da forma $(KG)e$, com $e \in KG$ idempotente (corolário 2.6.26).

Pelo teorema de Wedderburn-Artin, podemos escrever

$$KG \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_m}(D_m)$$

com $D_1, \cdots, D_m$ anéis de divisão. Temos

$$Z(KG) = Z(M_{n_1}(D_1)) \oplus \cdots \oplus Z(M_{n_m}(D_m))$$

e como $Z(M_{n_i}(D_i)) \supset Z(D_i) \cdot 1 \supset K \cdot 1$, temos $\dim_K Z(M_{n_i}(D_i)) \geq 1$. Daí

$$\dim_K Z(KG) = \dim_K Z(M_{n_1}(D_1)) + \cdots + \dim_K M_{n_m}(D_m) \geq m$$

Ainda, sejam $C_1, \cdots, C_s$ as classes de conjugação de G, e defina o elemento $c_i = \sum_{x \in C_i} x \in KG$, $i = 1, \cdots, s$. Note que, para todo $g \in G$, $gc_ig^{-1} = c_i$ (uma vez que, para cada $x \in C_i$, temos $gxg^{-1} \in C_i$, e a conjugação é um isomorfismo de grupos). Essas duas observações permitem provar o seguinte resultado:

Proposição 2.7.1. *O número de componentes simples na decomposição de KG, é menor ou igual à quantidade de classes de conjugação de G.*

Demonstração. Pela observação e notação acima, temos $m \leq \dim_K Z(KG)$ e iremos mostrar que $\dim_K KG = s$, a quantidade de classes de conjugação de G. Seja $x \in Z(KG)$ e escreva $x = \sum_{g \in G} \alpha_g g$. Temos, para todo $h \in G$, $x = hxh^{-1} = \sum_{g \in G} \alpha_g hgh^{-1} = \sum_{g \in G} \alpha_{h^{-1}gh} g$, e comparando os coeficientes (uma vez que $\{g \in G\}$ é base de KG), temos $\alpha_g = \alpha_{h^{-1}gh}$, para todo $h \in G$, ou seja, os coeficientes de x são constantes nos elementos de uma mesma classe de conjugação, e daí, x é combinação linear de $c_1, \cdots, c_s$. Por outro lado, como os elementos que compõem cada c_i são distintos, segue que eles são linearmente independentes. Daí $\{c_1, \cdots, c_s\}$ é uma base de $Z(KG)$ e o resultado segue. □

Nota. No caso de K ser algebricamente fechado, temos

$$KG \simeq M_{n_1}(K) \oplus \cdots \oplus M_{n_m}(K)$$

e $Z(KG) \simeq Z(M_{n_1}(K)) \oplus \cdots \oplus Z(M_{n_m}(K)) = K \oplus \cdots \oplus K$, e daí $s = \dim_K Z(KG) = m$, e então, vale a igualdade no último teorema.

Ainda, olhando para a decomposição

$$KG \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_m}(D_m)$$

e lembrando que os ideais à esquerda de $M_n(D)$ são colunas, temos que um ideal minimal à esquerda $(KG)e$ de KG é tal que $\dim_K (KG)e = n_i$, $(KG)e$ aparece n_i vezes na composição de KG e $(KG)e$ está contido num ideal bilateral minimal de dimensão n_i^2.

Todas essas conclusões serão resumidas no seguinte teorema:

Teorema 2.7.2. *Sejam K um corpo de característica zero e G um grupo finito. Então*

(i) KG é um anel completamente redutível com unidade;

(ii) Todo (KG)-módulo irredutível é isomorfo a um ideal minimal à esquerda de KG;

(iii) Todo ideal minimal à esquerda de KG é da forma $(KG)e$, com $e \in KG$ idempotente;

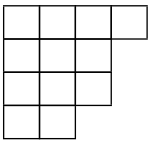
(iv) O número de ideais minimais à esquerda não isomorfos de KG é menor ou igual à quantidade de classes de conjugação de G. Se K é algebricamente fechado, então essas quantidades coincidem.

Aqui observamos que o teorema é válido numa situação um pouco mais geral: o corpo K pode ser qualquer desde que a sua característica não divida a ordem de G.

§2.8 Representação do Grupo Simétrico S_n

O objetivo desta seção será caracterizar todos os (KS_n)-módulos irredutíveis. Aqui, fixaremos $n \in \mathbb{N}$, o grupo simétrico S_n, um corpo de característica zero K e $A = KS_n$. Consideraremos aqui A-módulos à esquerda, e o produto de duas permutações $\sigma, \theta \in S_n$ será da direita para a esquerda. Assim, uma ação de S_n no conjunto $I_n = \{1, 2, \cdots, n\}$ é tal que $\sigma(\tau m) = (\sigma\tau)m$, para cada $m \in I_n$. Dada duas partições $\lambda = (n_1, \cdots, n_m)$ e $\lambda' = (n'_1, \cdots, n'_l)$, diremos que $\lambda > \lambda'$, se existe um índice i tal que $n_j = n'_j$, para $j = 1, \cdots, i-1$ e $n_i > n'_i$.

Seja $\lambda = (n_1, \cdots, n_k) \vdash n$ uma partição de n (vide definição 1.1.9) e considere uma tabela T_λ com n_1 espaços na primeira linha, n_2 espaços na segunda linha, etc. Por exemplo, se $\lambda = (4, 3, 3, 2)$, a tabela T_λ será



Caso exista um preenchimento com os números $1, 2, \cdots, n$ em cada caixa da tabela T_λ, denominaremos esta tabela com preenchimento de um **diagrama de Young** D_λ. Por exemplo, para a partição $\lambda = (4, 3, 3, 2)$, um diagrama associado a essa partição seria:

1	2	3	4
5	6	7	
8	9	10	
11	12		

Dado um diagrama D_λ, considere o subgrupo $R(D_\lambda) \subseteq S_n$, que permuta os números de cada linha, mas não levam elementos de uma linha em outra. Por exemplo, no caso $\lambda = (4, 3, 3, 2)$ e o diagrama D_λ igual ao exemplo acima, temos

$$R(D_\lambda) = S_4(1, 2, 3, 4) \oplus S_3(5, 6, 7) \oplus S_3(8, 9, 10) \oplus S_2(11, 12).$$

De forma análoga, defina $C(D_\lambda)$ como os elementos que permutam o conjunto dos números em cada coluna. É fácil verificar que ambos são subgrupos de S_n.

Temos que $R(D_\lambda) \cap C(D_\lambda) = 1$. De fato, se $\sigma \in R(D_\lambda) \cap C(D_\lambda)$, então σ não move nenhum elemento para outra linha e nem para outra coluna, logo, deve fixar cada elemento, e então, $\sigma = 1$.

Defina o elemento (recordamos que ϵ_τ é o sinal da permutação τ)

$$e(D_\lambda) = \sum_{\substack{\sigma \in R(D_\lambda) \\ \tau \in C(D_\lambda)}} \epsilon_\tau \sigma\tau = \left(\sum_{\sigma \in R(D_\lambda)} \sigma \right) \left(\sum_{\tau \in C(D_\lambda)} \epsilon_\tau \tau \right)$$

O objetivo aqui é mostrar que os elementos $e(D_\lambda)$ geram ideais minimais (não necessariamente são idempotentes, mas são múltiplos de algum idempotente); se D_λ e D'_λ são dois preenchimentos para uma mesma tabela T_λ (mesma partição), então $KS_n e(D_\lambda) \simeq KS_n e(D'_\lambda)$; e se λ e μ são duas partições distintas, então $KS_n e(D_\lambda)$ e $KS_n e(D_\mu)$ não são isomorfos. Combinando com a teoria desenvolvida anteriormente, isso irá compor todos os (KS_n)-módulos irredutíveis (proposição 2.7.1 e corolário 1.1.12).

Note que para cada $\sigma' \in R(D_\lambda)$ e $\tau' \in C(D_\lambda)$, temos

$$\sigma' e(D_\lambda) = \sum_{\substack{\sigma \in R(D_\lambda) \\ \tau \in C(D_\lambda)}} \epsilon_\tau (\sigma'\sigma)\tau = e(D_\lambda)$$

$$e(D_\lambda)\tau' = \sum_{\substack{\sigma \in R(D_\lambda) \\ \tau \in C(D_\lambda)}} \epsilon_\tau \sigma(\tau\tau') = \epsilon_{\tau'} \sum_{\substack{\sigma \in R(D_\lambda) \\ \tau \in C(D_\lambda)}} \epsilon_{\tau\tau'} \sigma(\tau\tau') = \epsilon_{\tau'} e(D_\lambda)$$

essas propriedades são de grande importância e constituirá de uma caracterização do elemento $e(D_\lambda)$, a menos de um múltiplo escalar.

Todos os lemas são técnicos, elementares e não triviais, mas fáceis de demonstrar. Elas são observações e manipulações muito bem arquitetadas, e ao mesmo tempo, bem simples, com consequências importantíssimas.

Dado um diagrama D_λ e $\sigma \in S_n$, defina σD_λ como o diagrama obtido de D_λ, aplicando σ nas entradas de D_λ.

Começaremos com um lema, cuja consequência será referenciada diversas vezes:

Lema 2.8.1. *Sejam $\theta, \rho \in S_n$, D_λ um diagrama e $D'_\lambda = \rho D_\lambda$. Considere θD_λ como obtido por D_λ movendo adequadamente as entradas de D_λ, então, o mesmo conjunto de movimentos irá modificar D'_λ a $\left(\rho\theta\rho^{-1}\right) D'_\lambda$. Em outras palavras, se a entrada (i,j) de D_λ é movida à entrada (i',j') de θD_λ, então a entrada (i,j) de D'_λ é movida à entrada (i',j') de $\left(\rho\theta\rho^{-1}\right) D'_\lambda$.*

Demonstração. Seja α um símbolo na posição (i,j) de D_λ, que é movido a (i',j') em θD_λ. Então, se β é o símbolo na posição (i',j') de D_λ, então $\theta(\beta) = \alpha$.

Segundo essa notação, $\rho(\alpha)$ é o símbolo na posição (i,j) de ρD_λ, e na posição (i',j') de $\left(\rho\theta\rho^{-1}\right) D'_\lambda$, temos

$$\left(\rho\theta\rho^{-1}\right) \rho(\beta) = \rho\theta(\beta) = \rho(\alpha)$$

ou seja, a (i,j)-ésima posição de D'_λ é movida à (i',j')-ésima posição de $\left(\rho\theta\rho^{-1}\right) D'_\lambda$. □

Como primeira consequência, temos o seguinte resultado, que será importante em vários argumentos:

Corolário 2.8.2. *Dado $\theta \in S_n$, valem $R(\theta D_\lambda) = \theta R(D_\lambda)\theta^{-1}$, $C(\theta D_\lambda) = \theta C(D_\lambda)\theta^{-1}$ e $e(\theta D_\lambda) = \theta e(D_\lambda)\theta^{-1}$*

Demonstração. Seja $\sigma \in R(D_\lambda)$. Então σ mantém as linhas de D_λ em suas linhas, e pelo lema 2.8.1, $\theta\sigma\theta^{-1}$ mantém as linhas de θD_λ em suas linhas, ou seja, $\theta\sigma\theta^{-1} \in R(\theta D_\lambda)$. Da mesma forma, se $\sigma \in R(\theta D_\lambda)$, então $\theta^{-1}\sigma\theta \in R(\theta^{-1}\theta D_\lambda) = R(D_\lambda)$. Daí $\sigma \in R(D_\lambda)$ se e só se $\theta\sigma\theta^{-1} \in R(\theta D_\lambda)$. O mesmo argumento vale para as colunas, e o resultado segue. □

Com isso, podemos mostrar que ideais $Ae(D_\lambda)$ que provêm de uma mesma partição, mas com preenchimentos diferentes, são isomorfos:

Proposição 2.8.3. *Se D_λ e D'_λ são diagramas associados a uma mesma partição λ, então $Ae(D_\lambda) \simeq Ae(D'_\lambda)$.*

Demonstração. Seja $\theta \in S_n$ tal que $D'_\lambda = \theta D_\lambda$. Então $e(D'_\lambda) = \theta e(D_\lambda)\theta^{-1}$, e daí $Ae(D'_\lambda) = A\theta e(D_\lambda)\theta^{-1} = Ae(D_\lambda)\theta^{-1}$. Considere a aplicação $\psi : x \in Ae(D_\lambda) \mapsto x\theta^{-1} \in Ae(D'_\lambda)$. Temos ψ bem definido, 1-1 e sobre, e ψ é um homomorfismo de A-módulos à esquerda, e o resultado segue. □

O próximo lema tem enunciado aparentemente excêntrico, mas ficará clara a sua importância, após apresentarmos uma artimanha utilizando esse resultado:

Lema 2.8.4. *Sejam $\lambda = (n_1, \cdots, n_m)$ e $\lambda' = (n'_1, \cdots, n'_l)$ duas partições distintas de n. Assuma $\lambda > \lambda'$. Então, sendo D_λ e $D_{\lambda'}$ dois diagramas associados a λ e a λ', respectivamente, existe $\pi \in S_n$ transposição tal que $\pi \in R(D_\lambda) \cap C(D_{\lambda'})$. Em outras palavras, existem símbolos α e β com α e β na mesma linha de D_λ e na mesma coluna de $D_{\lambda'}$.*

Demonstração. Temos $n_1 \geq n'_1$. Assuma que todo par de símbolos na mesma linha de D_λ não está na mesma coluna de $D_{\lambda'}$. Então, em particular, os n_1 símbolos da primeira linha de D_λ estão em diferentes colunas de $D_{\lambda'}$, e $D_{\lambda'}$ tem n'_1 colunas. Segue que $n_1 \leq n'_1$, e daí $n_1 = n'_1$.

Considere $\theta \in S_n$ tal que a primeira linha de $\theta D_{\lambda'}$ seja igual a de D_λ. Repetindo o argumento, obteremos que $n_2 = n'_2$, e continuando o processo, chegaremos a $\lambda = \lambda'$, contradição. □

Como consequência, temos um resultado que será útil para mostrar que $Ae(D_\lambda)$ não é isomorfo a $Ae(D_{\lambda'})$, se D_λ e $D_{\lambda'}$ são associados a diferentes partições:

Corolário 2.8.5. *Sejam λ e λ' partições diferentes de n e D_λ e $D_{\lambda'}$ diagramas quaisquer associados a λ e λ', respectivamente. Então $e(D_{\lambda'})e(D_\lambda) = 0$.*

Demonstração. Assuma $\lambda > \lambda'$, e, pelo lema 2.8.4, seja $\pi \in S_n$ transposição tal que $\pi \in R(D_\lambda) \cap C(D_{\lambda'})$. Então

$$e(D_{\lambda'})e(D_\lambda) = \underbrace{e(D_{\lambda'})\pi}_{\epsilon_\pi e(D_{\lambda'})} \underbrace{\pi e(D_\lambda)}_{e(D_\lambda)} = -e(D_{\lambda'})e(D_\lambda)$$

e o resultado segue. □

O próximo lema terá como consequência a chave para demonstrar o resultado principal desta seção:

Lema 2.8.6. *Seja $\theta \in S_n$. Então $\theta = \sigma\tau$, com $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$ se e só se cada dois símbolos na mesma linha de D_λ estão em colunas distintas de θD_λ.*

Demonstração. Assuma $\theta = \sigma\tau$, com $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$, e α e β na mesma linha de D_λ. Então α e β estão na mesma linha de σD. Como, pelo corolário 2.8.2, $\sigma\tau\sigma^{-1} \in C(\sigma D)$, temos α e β em diferentes colunas de $\left(\sigma\tau\sigma^{-1}\right)\sigma D = \theta D$.

Reciprocamente, assuma que cada dois símbolos numa mesma linha de D_λ estejam em colunas distintas de θD_λ. Então, em particular, os símbolos da primeira coluna de θD_λ estão em distintas linhas de D_λ, e daí, existe $\sigma_1 \in R(D_\lambda)$ tal que $\sigma_1 D_\lambda$ e θD_λ possuem os mesmos símbolos na primeira coluna.

Repetindo o processo, obtemos $\sigma_2 \in R(\sigma_1 D_\lambda) = \sigma_1 R(D_\lambda)\sigma^{-1} = R(D_\lambda)$ (pelo corolário 2.8.2 e por $R(D)$ ser subgrupo) tal que $\sigma_2\sigma_1 D_\lambda$ e θD_λ possuem os mesmos símbolos na primeira e na segunda coluna. Continuando o processo, obtemos $\sigma \in R(D_\lambda)$ tal que σD_λ e θD_λ possuem os mesmos símbolos em cada coluna. Daí, existe $\tau' \in C(\sigma D_\lambda)$ tal que $\theta D_\lambda = \tau'\sigma D$, mas, $\tau' = \sigma\tau\sigma^{-1}$, para algum $\tau \in C(D_\lambda)$ (pelo corolário 2.8.2), e portanto $\theta = \tau'\sigma = \sigma\tau\sigma^{-1}\sigma = \sigma\tau$. □

Lema 2.8.7. *Seja $x \in A$ tal que $\sigma x \tau = \epsilon_\tau x$, para todo $\sigma \in R(D_\lambda)$ e todo $\tau \in C(D_\lambda)$. Então, existe $\gamma \in K$ tal que $x = \gamma e(D_\lambda)$. Ainda, escrevendo $x = \sum_{g \in S_n} \alpha_g g$, temos $\gamma = \alpha_1$.*

Observação. A volta vale, uma vez que, se $x = \gamma e(D_\lambda)$, então, para todo $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$, temos

$$\sigma x \tau = \gamma \sigma e(D_\lambda)\tau = \gamma \epsilon_\tau e(D_\lambda) = \epsilon_\tau x$$

Demonstração. Escreva $x = \sum_{\theta \in S_n} \alpha_\theta \theta$. Então, para cada $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$, temos

$$\epsilon_\tau x = \sigma^{-1} x \tau^{-1} = \sum_{\theta \in S_n} \alpha_\theta (\sigma^{-1}\theta\tau) = \sum_{\theta' \in S_n} \alpha_{\sigma\theta'\tau}\theta'$$

e ainda, $\alpha_\theta = \epsilon_\tau \alpha_{\sigma\theta\tau}$. Em particular, tomando $\theta = 1$, obtemos $\alpha_1 = \epsilon_\tau \alpha_{\sigma\tau}$, para todo $\sigma \in R(D_\lambda), \tau \in C(D_\lambda)$. Daí, basta mostrar que $\alpha_\theta = 0$, se θ não é da forma $\sigma\tau$, com $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$, e então, obteremos que

$$x = \sum_{\theta \in S_n} \alpha_\theta \theta = \sum_{\substack{\sigma \in R(D_\lambda) \\ \tau \in C(D_\lambda)}} \alpha_1 \epsilon_\tau \sigma\tau = \alpha_1 e(D_\lambda)$$

Seja θ tal que θ não é da forma $\sigma\tau$, com $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$. Então, pelo lema 2.8.6, existe transposição $\pi \in S_n$ tal que $\pi \in R(D_\lambda) \cap C(\theta D_\lambda)$, logo, $\pi = \theta\pi'\theta^{-1}$, com $\pi' \in C(D_\lambda)$ (pelo corolário 2.8.2, e π' é transposição). Portanto, em particular,

$$\alpha_\theta = \epsilon_\pi \alpha_{\pi\theta\pi^{-1}} = -\alpha_{\theta\pi'\theta\theta^{-1}\pi'} = -\alpha_{\theta\pi'^2} = -\alpha_\theta$$

e segue que $\alpha_\theta = 0$. □

Com isso, podemos demonstrar o resultado principal desta seção, e começaremos mostrando que $e(D_\lambda)$ é múltiplo de um idempotente:

Corolário 2.8.8. *$e(D_\lambda)^2 = \gamma e(D_\lambda)$, com $\gamma \in \mathbb{Z}$ não nulo.*

Demonstração. Para cada $\sigma \in R(D_\lambda)$ e $\tau \in C(D_\lambda)$, temos

$$\sigma e(D_\lambda)^2 \tau = \sigma e(D_\lambda) e(D_\lambda)\tau = \epsilon_\tau e(D_\lambda)^2$$

e por consequência, pelo lema 2.8.7, $e(D_\lambda)^2 = \gamma e(D_\lambda)$, em que, escrevendo $e(D_\lambda)^2 = \sum_{\theta \in S_n} \alpha_\theta \theta$, temos $\gamma = \alpha_1$. Segue que γ é inteiro, por definição de $e(D_\lambda)$.

Considere a aplicação linear $T : x \in A \mapsto xe(D_\lambda) \in A$. Tomando a base $\{\theta : \theta \in S_n\}$, temos $\mathrm{tr}(T) = \alpha_1 n!$. Ainda, seja $B = \{e_1, \cdots, e_{n!}\}$ base de A de modo que $\{e_1, \cdots, e_m\}$ seja base de $Ae(D_\lambda)$ (como $e(D_\lambda) \neq 0$, temos $1 \leq m \leq n!$). Para cada $x = ae(D_\lambda) \in Ae(D_\lambda)$, temos $T(x) = T(ae(D_\lambda)) = ae(D_\lambda)e(D_\lambda) = \gamma ae(D_\lambda) = \gamma x$, e note que $T(a) = ae(D_\lambda) \in Ae(D_\lambda)$, para todo $a \in A$. Segue que a matriz de T na base B tem a forma:

$$[T]_B = \begin{pmatrix} \gamma I_{m\times m} & 0_{m\times(n!-m)} \\ * & 0_{(n!-m)\times(n!-m)} \end{pmatrix}$$

e então, $\mathrm{tr}(T) = m\gamma$. Como o traço não depende da escolha da base, temos $m\gamma = n! \neq 0$, e daí $\gamma \neq 0$. □

Seja $\gamma \in \mathbb{Z}$ tal que $e(D_\lambda)^2 = \gamma e(D_\lambda)$ e defina $u(D_\lambda) = \gamma^{-1}e(D_\lambda)$. Então $u(D_\lambda)$ é idempotente, uma vez que $u(D_\lambda)^2 = \gamma^{-1}e(D_\lambda)\gamma^{-1}e(D_\lambda) = \gamma^{-1}e(D_\lambda) = u(D_\lambda)$, e $Au(D_\lambda) = Ae(D_\lambda)$.

Proposição 2.8.9. *O ideal $Au(D_\lambda) = Ae(D_\lambda)$ é minimal.*

Demonstração. Pelo lema 2.6.29, basta mostrar que $u(D_\lambda)Au(D_\lambda)$ é anel de divisão. Para cada $x \in u(D_\lambda)Au(D_\lambda)$, temos que

$$\sigma x \tau = \epsilon_\tau x, \forall \sigma \in R(D_\lambda), \forall \tau \in C(D_\lambda)$$

e portanto, pelo lema 2.8.7, $x = \gamma_x e(D_\lambda)$, para algum $\gamma_x \in K$. É claro que dado $x = \gamma_x e(D_\lambda) \in Ke(D_\lambda)$, temos

$$x = \gamma_x \gamma^{-1} \underbrace{\gamma e(D_\lambda)}_{e(D_\lambda)^2} = e(D_\lambda)\gamma_x\gamma^{-1}e(D_\lambda) = u(D_\lambda)(\gamma\gamma_x \cdot 1)u(D_\lambda) \in u(D_\lambda)Au(D_\lambda)$$

Segue que $u(D_\lambda)Au(D_\lambda) = e(D_\lambda)Ke(D_\lambda) \simeq K$ é anel de divisão, e resulta que $Au(D_\lambda)$ é minimal. □

Proposição 2.8.10. *Sejam D_λ e D_μ diagramas associados a partições diferentes. Então $Ae(D_\lambda)$ não é isomorfo a $Ae(D_\mu)$.*

Demonstração. Assuma $Au(D_\lambda) \simeq Au(D_\mu)$. Pelo corolário 2.6.28, existe $a \in A$ tal que $Au(D_\lambda) = Au(D_\mu)a$. Em particular, existe $b \in A$ tal que $u(D_\lambda) = bu(D_\mu)a$, e daí $u(D_\lambda) = u(D_\lambda)^2 = u(D_\lambda)u(D_\lambda) = bu(D_\mu)au(D_\lambda)$.

Basta provar que $u(D_\mu)au(D_\lambda) = 0$, e para isso, é suficiente mostrar que $u(D_\mu)\theta u(D_\lambda) = 0$, para todo $\theta \in S_n$. Temos $u(D_\mu)\theta u(D_\lambda) = u(D_\mu)\theta u(D_\lambda)\theta^{-1}\theta$. Temos $u(D_\mu)$ múltiplo de $e(D_\mu)$ e $\theta u(D_\lambda)\theta^{-1}$ múltiplo de $\theta e(D_\lambda)\theta^{-1}$, mas, $\theta e(D_\lambda)\theta^{-1} = e(\theta D_\lambda)$ (corolário 2.8.2), e como D_μ e θD_λ estão associados a diferentes partições, pelo corolário 5, $e(D_\mu)e(\theta D_\lambda) = 0$, ou seja, $u(D_\mu)\theta u(D_\lambda)\theta^{-1} = 0$, o que implica $u(D_\lambda) = bu(D_\mu)au(D_\lambda) = 0$, contradição. Segue que $Au(D_\lambda)$ não é isomorfo a $Au(D_\mu)$. □

Isso conclui a demonstração do resultado principal desta seção, que será resumido no seguinte teorema:

Teorema 2.8.11. *Seja K um corpo de característica zero e $n \in \mathbb{N}$. Denote por $A = KS_n$. Para cada partição $\lambda = (n_1, \cdots, n_m) \vdash n$, considere uma tabela T_λ, e preencha com os números $1, \cdots, n$, obtendo um diagrama D_λ. Considere os subgrupos $R(D_\lambda)$ e $C(D_\lambda)$, que permutam as linhas e as colunas, respectivamente, do diagrama, e defina*

$$e(D_\lambda) := \sum_{\substack{\sigma \in R(D_\lambda) \\ \tau \in C(D_\lambda)}} \epsilon_\tau \sigma\tau$$

Então:

(i) $Ae(D_\lambda)$ é um ideal minimal à esquerda de A, e todo ideal minimal de A tem essa forma;

(ii) todo A-módulo irredutível à esquerda é isomorfo a um ideal minimal a esquerda de A;

(iii) Se D_μ é um diagrama associado a uma partição μ, então $Ae(D_\mu) \simeq Ae(D_\lambda)$ se e só se $\lambda = \mu$;

(iv) $e(D_\lambda) = \gamma u(D_\lambda)$, com $u(D_\lambda)$ idempotente e $\gamma \in \mathbb{Z}$;

(v) Se D_λ e D'_λ são diagramas associados a uma mesma partição e $D'_\lambda = \theta D_\lambda$, para algum $\theta \in S_n$, então $\psi : x \in Ae(D_\lambda) \mapsto x\theta^{-1} \in Ae(D'_\lambda)$ é bem definido e é um isomorfismo de A-módulos.

§2.9 Comutadores Básicos

Uma K-álgebra associativa livre gerada por $X = \{x_1, x_2, \cdots\}$, com X podendo ser infinito ou não, admite como K-base livre todas as palavras $x_{i_1} \cdots x_{i_k}, k \in \mathbb{N}, x_{i_1}, \cdots, x_{i_k} \in X$.

No caso de uma K-álgebra de Lie livre $L = L(X)$ gerada por X, o conjunto de todas as palavras $[x_{i_1}, \cdots, x_{i_k}]$ gera, mas não é K-base livre, pois, por exemplo

$$[x, y, y, x] = [x, y, x, y] + \underbrace{[[x, y], [y, x]]}_{0} = [x, y, x, y]$$

admite duas representações diferentes.

Nesta seção, baseado no artigo de Hall [18] (uma abordagem totalmente diferente pode ser encontrada em Bahturin [5]), apresentaremos uma K-base livre para a álgebra de Lie livre gerada por X, e essa base é constituída pelos denominados "**comutadores básicos**":

Definição 2.9.1. Define-se como comutadores básicos de grau 1 os elementos $x_1, x_2, \cdots \in X$. Por indução, tendo os comutadores básicos de grau $1, \cdots, n-1$, considere uma ordenação total nos comutadores básicos de forma que, se grau $u <$ grau v, então $u < v$. Um comutador $[u, v]$, de grau n, é definido por básico se

(i) u e v são básicos e $u > v$

(ii) se $u = [s, t]$, então $t \leq v$

Um elemento de L será dito estar na forma básica se for escrito como combinação linear de comutadores básicos.

Esses dois axiomas (i) e (ii) e a ordenação da definição nos comutadores básicos, apesar de poderem parecer estranhos, são muito bem arquitetados com relação aos monômios da álgebra de Lie livre. A exigência da condição (i) é muito natural e tem relação com a anticomutatividade do colchete, pois $[u, v]$ e $[v, u]$ são comutadores linearmente dependentes, e devemos "escolher" um deles. A condição (ii) já é um tanto mais estranho à primeira vista, mas quadra muito bem a Identidade de Jacobi: dados u, v, w comutadores básicos, com $u > v$ e $u > w$, considere o comutador $[u, v, w]$. Se $v \leq w$, então $[u, v, w]$ é básico, e caso contrário, aplicando a identidade de Jacobi, obtemos

$$[u, v, w] = [u, w, v] - [v, w, u]$$

e $[u, w, v]$ será básico, e $[v, w, u]$ é um comutador tal que o último termo do comutador é maior do que o último termo do comutador anterior (isto é, $u > w$). Essa observação permite o uso de "indução" para provar afirmações envolvendo comutadores: se uma afirmação vale para comutadores básicos, e fizermos essa manipulação adequadamente, obteremos dois novos comutadores, um em que a afirmação vale (pois é comutador básico) e o outro que terá o último termo maior. Podemos continuar com esse processo, e em algum momento, chegaremos em um comutador com o último termo "muito grande", e necessariamente será básico (dependendo das condições), e o processo irá terminar.

Tal argumento pode parecer confuso, mas esse é o tipo de argumento utilizado com comutadores básicos. Esse argumento será usado para demonstrar que os comutadores básicos geram e são linearmente independentes, e será utilizado novamente num dos resultados principais desta dissertação. Mostraremos inicialmente que os comutadores básicos geram o espaço L, e para isso, definiremos o processo canônico:

Definição 2.9.2. Seja w comutador e escreva $w = [u, v]$. O processo canônico será definido pelos seguintes passos:
Passo 1: Escreva $u = \sum_{i=1}^{m_1} \alpha_i u_i$ e $v = \sum_{i=1}^{m_2} \beta_i v_i$ na forma básica.
Passo 2: Para cada u e v básicos, escreva

$$\begin{array}{rcll} [u,v] & = & 0 & , \text{ se } u = v \\ [u,v] & = & [u,v] & , \text{ se } u > v \\ [u,v] & = & -[v,u] & , \text{ se } u < v \end{array}$$

Passo 3: Sendo $u > v$ comutadores básicos e $u = [s, t]$, escreva

$$\begin{array}{rcll} [u,v] & = & [s,t,v] & , \text{ se } v \geq t \\ [u,v] & = & [s,v,t] - [t,v,s] & , \text{ se } v < t \end{array}$$

Passo 4: Retornar ao passo 1.

Lema 2.9.3. *Seja u um comutador mônico de grau m. Então u pode ser escrito na forma básica.*

Demonstração. A demonstração será feita por indução em $n = \operatorname{grau} u$. Se $n = 1$, então u já está na forma básica e nada a fazer, e se $n = 2$, então o processo canônico termina no passo 2.

Por indução, assuma $n > 2$ e que os comutadores de grau menor que n podem ser escritos na forma básica. Seja $u_0 = [u, v]$, e então, escrevendo $u = \sum a_i u_i$ e $v = \sum b_i v_i$ na forma básica, basta mostrar que $[u_i, v_j]$ pode ser escrito na forma básica. Então, assuma $u_0 = [u, v]$, com u, v básicos. Assumindo $u > v$ (pelo passo 2), escreva $u = [s, t]$ (como u é básico, s e t são básicos e $s > t$). Se v é "grande o suficiente", por exemplo, se $\operatorname{grau} v > n/3$, segue que necessariamente $v \geq t$, e daí, $[s, t, v]$ é básico. Então, assuma por hipótese de indução, que $[s', t', v']$ pode ser escrito na forma básica, sempre que $v' > v$ ou $v' = v$ e $t' > t$.

Se $v \geq t$, então u_0 é básico e nada a fazer, e caso contrário, pelo passo 3, temos

$$[u, v] = [s, t, v] = [s, v, t] - [t, v, s].$$

Temos $[s, v, t]$ básico, e como $s > t > v$, por indução, $[t, v, s]$ pode ser escrito na forma básica, e daí, u_0 pode ser escrito na forma básica. □

Dado um comutador u, denote por u^* a combinação linear por comutadores básicos dado pelo processo canônico. Defina $(u + v)^* := u^* + v^*$.

Agora, iremos demonstrar que os comutadores básicos formam uma base para a álgebra de Lie, e para isso, basta mostrar que o processo canônico não depende da representação de um comutador (e.g. vimos que $[x, y, y, x] = [x, y, x, y]$), e para isso, basta mostrar que o processo canônico aplicado nas representações de zero da álgebra de Lie (isto é, comutadores da forma $[u, u], [u, v] + [v, u], [u, v, w] + [v, w, u] + [w, u, v]$ e $[0, v]$) são levados na representação nula.

A seguir, ao utilizarmos um sinal de igualdade, queremos indicar igualdade na representação (ou, equivalentemente (e mais preciso), igualdade na álgebra livre não associativa gerada por X).

Valem as seguintes propriedades:

Proposição 2.9.4. $[u, v]^* = [u^*, v^*]^*$

Demonstração. Segue pela definição do processo canônico. □

Proposição 2.9.5. *Sejam u, v, w comutadores básicos. Então*

(1) $[u, u]^* = 0$

(2) $[u,v]^* = -[v,u]^*$

(3) $[u,v,w]^* + [v,w,u]^* + [w,u,v]^* = 0$

Demonstração. As afirmações (i) e (ii) seguem direto pelo passo 2 do processo canônico.

Para (iii), por simetria, podemos supor $u > v$ e $u > w$. Utilizando a proposição anterior e (ii), se necessário (isto é, podemos trocar v com w e trocar sinal e ordem dos comutadores, pois a representação será a mesma), podemos assumir $v > w$.

A demonstração será feita por indução em $n = \operatorname{grau}[u,v,w]$. Se $n = 3$, então não há alterações nos passos 1 e 2 do processo canônico, e no passo 3, obtemos $[u,v,w] = [u,w,v] - [v,w,u]$, soma de comutadores básicos (u, v, w são de grau 1, neste caso).

Assuma $n > 3$ e o resultado válido para comutadores de grau menor que n. Se $[u,v]$ é um comutador básico, não há alterações no passo 1 e, uma vez que $[u,v] > w$, não há alterações no passo 2. No passo 3, uma vez que $v > w$, obtemos

$$[u,v,w] = [u,w,v] - [v,w,u].$$

Daí

$$\underbrace{[u,v,w]^*}_{[u,w,v]^* - [v,w,u]^*} + [v,w,u]^* + [w,u,v]^* = [u,w,v]^* + [w,u,v]^*$$

e isso é igual a zero, por (ii) e pela proposição anterior.

A demonstração, para $[u,v]$ não necessariamente básico, será feita por indução, assumindo a validade de (iii) para comutadores básicos u', v', w', sempre que $\operatorname{grau} w' > \operatorname{grau} w$ ou $w' = w$ e $\operatorname{grau} v' > \operatorname{grau} v$. Por linearidade, podemos supor a validade para u', v', w', satisfazendo $w' > w$ ou $w' = w$ e $v' > v$, sem necessariamente u', v', w' serem básicos.

Se $\operatorname{grau} w$ for suficientemente grande, por exemplo, se $\operatorname{grau} w > \frac{n}{4}$, então $\operatorname{grau} u \geq \frac{3n}{8}$, e se $u = [s,t]$, então $\operatorname{grau} t \leq \frac{3n}{16} < \frac{n}{4} \leq \operatorname{grau} v$, e daí $[u,v]$ é comutador básico e vale, e isso mostra a base de indução.

Se $[u,v]$ não é básico, então $u = [s,t]$, com $s > t > v$, e daí, aplicando as hipóteses de indução (para grau de comutador menor que n e para comutadores $[u', v', w']$ satisfazendo aquelas relações) e omitindo a estrela, obtemos

$$\begin{aligned}
&[u,v,w] = [s,t,v,w] = -[t,v,s,w] + [s,v,t,w] \\
&= -[t,v,w,s] + [s,w;t,v] + [s,v,w,t] - [t,w;s,v] \\
&= -[t,w,v,s] + [v,w,t,s] + [s,w;t,v] + [s,v;t,w] + [s,w,v,t] - [v,w,s,t] \\
&= -[t,w,v,s] + \cancel{[v,w,t,s]} + [s,w;t,v] + [s,v;t,w] + [s,w,v,t] - \cancel{[v,w,t,s]} + [s,t;v,w].
\end{aligned}$$

Para os outros comutadores:

$$[v,w,u] = [v,w;s,t] = -[s,t;v,w]$$

$$\begin{aligned}
&[w,u,v] = -[u,w,v] = -[s,t,w,v] \\
&= -[s,w,t,v] + [t,w,s,v] \\
&= -[s,w,v,t] + [t,v;s,w] + [t,w,v,s] - [v,s;w,t]
\end{aligned}$$

somando $[u,v,w]^* + [v,w,u]^* + [w,u,v]^*$ obtém-se 0, provando a afirmação. □

Isso prova que a representação na forma básica é única, ou seja, vale o seguinte teorema:

Teorema 2.9.6. *Os comutadores básicos formam uma base para a álgebra de Lie livre.*

Exemplo: *Considere $X = \{x, y\}$, com ordenação $x > y$. Os comutadores básicos são:*

$$x, y, [x, y], [x, y, y], [x, y, x], [x, y, y, y], [x, y, y, x], [x, y, x, x], \cdots$$

□

§2.10 Identidades Multilineares e Aplicações

Nesta seção, serão apresentados alguns resultados na teoria de PI-álgebras importantes e básicos, e algumas aplicações da teoria desenvolvida anteriormente.

Nosso foco será o estudo em corpos de característica zero, e, a menos que se diga ao contrário, todos os corpos mencionados serão assumidos de característica zero (muitos resultados aqui se generalizam, ou incluem casos de corpos de característica positiva).

Começaremos com um conceito que será muito explorado neste trabalho.

Definição 2.10.1. Seja $f(x_1, \cdots, x_m) \in K\langle X\rangle$. Dizemos que f é **multilinear** se f é multihomogêneo e de multigrau $(1, 1, \cdots, 1)$. Denota-se por P_n o espaço dos polinômios multilineares de grau n nas variáveis $x_1, \cdots, x_n$.

Observação.

1. Se K tem característica zero, então f é multilinear se e só se a aplicação $(a_1, \cdots, a_m) \in A^n \mapsto f(a_1, \cdots, a_m) \in A$ for uma aplicação m-linear de espaços vetoriais, para toda álgebra A. Essa equivalência não é verdade se $\operatorname{car} K = p > 0$, pois, por exemplo, $f(x, y) = x^p y$ induz uma aplicação bi-linear.

2. P_n é um espaço vetorial e $\{x_{\sigma(1)} \cdots x_{\sigma(n)} : \sigma \in S_n\}$ é uma base de P_n.

Teorema 2.10.2. *Seja $f(x_1, \cdots, x_m) \in K\langle X\rangle$ e escreva $f = \sum_{i=0}^{n} f_i$, com f_i homogêneo em x_1 de grau i. Então:*

(i) Se K contém mais que n elementos (e.g. K é infinito), então $f_i = 0$ é consequência de $f = 0$, para cada $i = 0, 1, \ldots, n$.

(ii) Se $\operatorname{car} K > \operatorname{grau} f$ ou $\operatorname{car} K = 0$, então $f = 0$ é equivalente a um conjunto de polinômios multilineares.

Demonstração. (i) Sejam $\alpha_0, \alpha_1, \cdots, \alpha_n \in K$ distintos e seja $T = \langle f\rangle^T$ o T-ideal gerado por f. Então, como T é fechado por endomorfismos, segue que

$$f(\alpha_j x_1, x_2, \cdots, x_m) = \sum_{i=0}^{n} \alpha_j^i f_i(x_1, x_2, \cdots, x_m) \in T$$

para $j = 0, 1, \cdots, n$.

Então, escrevendo em forma matricial, temos

$$\begin{pmatrix} f(\alpha_0 x_1, x_2, \cdots, x_m) \\ f(\alpha_1 x_1, x_2, \cdots, x_m) \\ \vdots \\ f(\alpha_n x_1, x_2, \cdots, x_m) \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^n \end{pmatrix}}_{M} \begin{pmatrix} f_0(x_1, \cdots, x_m) \\ f_1(x_1, \cdots, x_m) \\ \vdots \\ f_n(x_1, \cdots, x_m) \end{pmatrix}$$

mas, a matriz M tem determinante $\prod_{i<j}(\alpha_i - \alpha_j) \neq 0$, e daí é invertível. Segue que f_i é combinação linear de $f(\alpha_0 x_1, x_2, \cdots, x_m), \cdots, f(\alpha_n x_1, \cdots, x_m) \in T$, e consequentemente $f_i = 0$ é consequência de $f = 0$, $i = 0, 1, \cdots, n$.

(ii) Podemos assumir f multi-homogêneo, por (i). Seja $d = \operatorname{grau}_{x_1} f$ e considere

$$f'(y_1, \cdots, y_d, x_2, \cdots, x_m) = f(y_1 + \cdots + y_d, x_2, \cdots, x_m)$$

e tome a componente multi-homogênea de multigrau $(\underbrace{1, \cdots, 1}_{d}, \operatorname{grau}_{x_2} f, \cdots, \operatorname{grau}_{x_m} f)$, e denomine tal componente de $g(y_1, \cdots, y_d, x_2, \cdots, x_m)$. Temos g consequência de f, e ainda, $g(x, \cdots, x, x_2, \cdots, x_m) = d! f(x, x_2, \cdots, x_m) \neq 0$, pois $\operatorname{car} K = 0$ ou $\operatorname{car} K > d$, e então $d! \neq 0$. Segue que f é equivalente a g, e repetindo o argumento às demais variáveis, chega-se ao resultado.

□

Observação. Dado um polinômio multi-homogêneo $f(x_1, \cdots, x_m)$, o processo de considerar a componente multi-homogênea de multigrau $(1, \cdots, 1, \operatorname{grau}_{x_2} f, \cdots, \operatorname{grau}_{x_m} f)$ do polinômio $f(y_1 + \cdots + y_d, x_2, \cdots, x_m)$, como na demonstração do último teorema, é denominado **linearização total em uma variável** do polinômio f em x_1. Quando o processo é feito para todas as variáveis de f, denomina-se **linearização total** de f.

Ainda nessa linha, costuma-se denominar **linearização parcial** a componente homogênea de $f(y_1 + y_2, x_2, \cdots, x_m)$ de multigrau $(\operatorname{grau}_{x_1} - 1, 1, \operatorname{grau}_{x_2} f, \cdots, \operatorname{grau}_{x_m} f)$. Uma linearização total em uma variável pode ser obtida por sucessivas linearizações parciais.

Este teorema é importante, pois reduz o estudo das identidades polinomiais ao estudo das identidades multi-homogêneas (caso o corpo seja infinito), e reduz ao estudo das multilineares, caso estejamos em característica zero; e estejamos interessados em determinar uma base de identidades.

Ainda, se quisermos verificar que uma álgebra satisfaz uma identidade multilinear, basta verificarmos se a álgebra satisfaz a identidade nos elementos da base. De fato, se $\{e_i\}_{i \in I}$ é base de A, então, dados $f(x_1, \cdots, x_m)$ polinômio multilinear e $a_1, \cdots, a_m \in A$, escrevemos $a_i = \sum_{j=1}^{m_i} \alpha_{ij} e_{n_j^{(i)}}$ (com $n_j^{(i)} \in \mathbb{N}$, para cada i, j) combinação linear dos elementos da base. Daí

$$f(a_1, \cdots, a_m) = \sum_{j_1, \cdots, j_m}^{m_1, \cdots, m_m} \alpha_{1 j_1} \cdots \alpha_{m j_m} f(e_{n_{j_1}}^{(1)}, \cdots, e_{n_{j_m}}^{(m)})$$

e então, $f(a_1, \cdots, a_m) = 0$ se todo $f(e_{n_{j_1}^{(1)}}, \cdots, e_{n_{j_m}^{(m)}}) = 0$.

Utilizando a linearização parcial, e algumas manipulações geniais, pode-se demonstrar o famoso e importante teorema de Dubnov–Ivanov–Nagata–Higman (historicamente, primeiramente demonstrado por Nagata em 1953 [19], generalizado por Higman em 1956 [22], e muito depois descobriu-se que esse teorema foi primeiramente enunciado por Dubnov e Ivanov em 1943 [12]).

Teorema 2.10.3. *Seja A uma PI-álgebra que satisfaz a identidade $x^n = 0$. Então existe um natural d, dependendo apenas do inteiro n, tal que A satisfaz a identidade $x_1 \cdots x_d = 0$.*

Demonstração. A demonstração será feita por indução em n. Se $n = 1$, então nada a fazer. Então, considere o caso $n > 1$, e assuma por hipótese de indução que existe $d \in \mathbb{N}$ tal que $f_d = x_1 \cdots x_d$ é consequência do polinômio x^{n-1}, ou seja, que $f_d = \sum_i u_i v_i^{n-1} w_i$, para u_i, v_i, w_i polinômios, e tome a linearização parcial de x^n:

$$f(x,y) = x^{n-1}y + x^{n-2}yx + \cdots + xyx^{n-2} + yx^{n-1}.$$

Então, temos que $f(x, yz^j)z^{k-j-1}$ é identidade de A, para cada $j, k \in \mathbb{N}$ e x, y, z variáveis. Ainda, temos:

$$f(x,yz^j)z^{k-j-1} = x^{k-1}yz^{k-1} + x^{k-2}yz^jxz^{k-j-1} + \cdots + xyz^jx^{k-2}z^{k-j-1} + yz^jx^{k-1}z^{k-j-1}$$

somando variando valores de j de 0 a $k-1$, obtemos a identidade de A:

$$\sum_{j=0}^{k-1} f(x,yz^j)z^{k-j-1} = kx^{k-1}yz^{k-1} + \sum_{i=0}^{k-2} x^i y f(z, x^{k-i-1})$$

então, uma vez que f é identidade, segue que $h = x^{k-1}yz^{k-1}$ é identidade de A. Daí, $x_1 \cdots x_{2d+1}$ é uma identidade de A, pois

$$\underbrace{x_1 \cdots x_d}_{\sum_i u_i v_i^{n-1} w_i} \; x_{d+1} \underbrace{x_{d+2} \cdots x_{2d+1}}_{\sum_j u'_j v'^{n-1}_j w'_j} = \sum_{i,j} u_i \underbrace{v_i^{n-1}(w_i x_d^n u'_j) v'^{n-1}_j}_{\text{consequência de } x^n} w'_j$$

e então $x_1 \cdots x_{2d+1}$ é consequência de x^n, e isso prova o teorema. □

Uma pergunta pertinente e interessante nesta direção é a seguinte. Relacionar os números n e d do Teorema de Nagata e Higman. Este problema é muito difícil e ainda não resolvido no caso geral. Pode-se verificar diretamente que se $n = 2$ temos $d = 3$ (isto é, toda álgebra nil de índice 2 é nilpotente de índice 3, e existem álgebras nil de índice dois que não são nilpotentes de índice 2 - ou seja, $d = 3$ é o índice mínimo para $n = 2$). Higman observou que se $n = 3$ teremos $d = 6$, e mostrou que para n qualquer, $d = d(n) \leq 2^n - 1$. (Tal fato decorre da demonstração do teorema dado acima.) Décadas mais tarde Razmyslov, utilizando métodos da teoria das identidades com traço, mostrou que $d(n) \leq n^2$, e Kuzmin obteve a desigualdade $d(n) \geq n(n+1)/2$. Essas são as melhores cotas gerais conhecidas até agora. Kuzmin conjecturou que $d(n) = n(n+1)/2$ para todo n. Esta conjectura foi confirmada para $n = 4$ por Vaughan-Lee (por meio de computações pesadas e bastante diretas). Shestakov e Zhukavets confirmaram a conjectura para $n = 5$, no caso de álgebras e superálgebras de 2 geradores. Sabe-se também que a conjectura é válida se $n = 5$, para álgebras com 3 geradores.

Pode-se provar que qualquer PI-álgebra satisfaz uma identidade multilinear (mas, não necessariamente que toda identidade é equivalente a uma identidade multilinear), mesmo não exigindo restrições ao corpo base. No caso de corpo de característica 0, isso já foi demonstrado.

Proposição 2.10.4. *Seja A uma PI-álgebra. Então A satisfaz uma identidade multilinear.*

Demonstração. Seja $f(x_1, \cdots, x_m)$ uma identidade de A, e defina

$$\text{grmax } f := \max\{\text{grau}_{x_1} f, \cdots, \text{grau}_{x_m} f\}.$$

Dividiremos a demonstração em duas partes.
Afirmação 1: A satisfaz uma identidade f', com grmax $f' = 1$.
Por indução em $n = \text{grmax } f$. Se $n = 1$, nada a fazer, e caso contrário, seja $i \in \mathbb{N}$ tal que $\text{grau}_{x_i} f = n$. Então, definindo

$$\begin{aligned} g_1(x_1, \cdots, x_{i-1}, x_i', x_i'', x_{i+1}, \cdots, x_m) = f(x_1, \cdots, x_{i-1}, x_i' + x_i'', x_{i+1}, \cdots, x_m) - \\ - f(x_1, \cdots, x_{i-1}, x_i', x_{i+1}, \cdots, x_m) - f(x_1, \cdots, x_{i-1}, x_i'', x_{i+1}, \cdots, x_m) \end{aligned}$$

obtemos que g_1 é identidade de A (note que $\text{grau}_{x_i} g_1 < \text{grau}_{x_i} f$). Se não existir $j \in \mathbb{N}$, tal que $\text{grau}_{x_j} g_1 = n$, então grmax $g_1 < n$, e segue por indução, e caso contrário, repita o processo para x_j. Como temos apenas um número finito de variáveis no polinômio f, o processo termina, e isso prova a afirmação.
Afirmação 2: A satisfaz uma identidade multilinear.
Temos que A satisfaz uma identidade $g(x_1, \cdots, x_m) \neq 0$, com $\text{grau}_{x_i} g \leq 1, i = 1, \cdots, m$. A demonstração será por indução em m.

Se $m = 1$, segue que $g(x_1) = \alpha x_1 \neq 0$ é multilinear, e nada a fazer. Então, assuma $m > 1$. Se todo x_i aparece com grau 1 em todas as componentes de g, implica que g é multilinear e vale o resultado. Então, assuma que x_1 aparece com grau 0 e grau 1, e escreva $g = g_1 + g_0$, com $\text{grau}_{x_1} g_i = i, i = 0, 1$, $g_0 \neq 0$.

Se $g_1 = 0$, resulta g_0 é uma identidade de A em $m - 1$ variáveis e segue por indução. Se $g_1 \neq 0$ e $g_0 \neq 0$, temos, definindo

$$g'(x_2, \cdots, x_m) = g(0, x_2, \cdots, x_m) = g_0(x_2, \cdots, x_m) \neq 0$$

ainda, g' é não nulo e é identidade de grau $m - 1$ de A, e o resultado segue por indução. □

Um resultado muito simples e muito útil é o seguinte:

Teorema 2.10.5. *Sejam A uma PI-álgebra sobre K que satisfaz uma identidade multilinear $f(x_1, \cdots, x_m)$ e B uma álgebra comutativa sobre K. Então $A \otimes_K B$ satisfaz f.*

Demonstração. Sejam $a_1 \otimes b_1, \cdots, a_m \otimes b_m \in A \otimes_K B$. Então

$$f(a_1 \otimes b_1, \cdots, a_m \otimes b_m) = f(a_1, \cdots, a_m) \otimes (b_1 \cdots b_m) = 0$$

No caso geral, temos

$$f\left(\sum_{i_1=1}^{n_1} a_{i_1} \otimes b_{i_1}, \cdots, \sum_{i_m=1}^{n_m} a_{i_m} \otimes b_{i_m}\right) = \sum_{i_1, \cdots, i_m}^{n_1, \cdots, n_m} f(a_{i_1} \otimes b_{i_1}, \cdots, a_{i_m} \otimes b_{i_m}) = 0.$$

□

Como consequência desse resultado, obtemos que as identidades são invariantes por extensões do corpo base, isto é, o seguinte teorema:

Teorema 2.10.6. *Sejam K um corpo, L uma extensão de K e A uma álgebra sobre K. Então, o ideal de identidades de $A \otimes_K L$ satisfaz $T(A \otimes_K L) = T(A) \otimes_K L$.*

Demonstração. O último teorema mostra que (fazendo as devidas identificações de espaços) $T(A \otimes_K L) \supset T(A) \otimes_K L$, e como $A \subset A \otimes_K L$ (na verdade $A \otimes 1$), segue que $T(A) \otimes_K L \supset T(A \otimes_K L)$, e segue o resultado. □

O próximo resultado será de grande importância no estudo de PI-álgebras em geral, mesmo tendo um enunciado simples e específico para matrizes:

Teorema 2.10.7. *Seja K um corpo. Então, a álgebra de matrizes $n \times n$, $M_n(K)$, não satisfaz identidades multilineares de grau menor que $2n$.*

Antes de demonstrar, vale introduzir a seguinte notação muito útil para trabalhar com matrizes $n \times n$: denotaremos por $e_{ij}, 1 \leq i, j \leq n$, as matrizes que possuem 1 na i-ésima linha e j-ésima coluna, e 0 nas demais entradas. Essas matrizes satisfazem $e_{ij}e_{kl} = \delta_{jk}e_{il}$, com δ_{kl} o delta de Kronecker ($\delta_{kl} = 1$ se $k = l$, e $\delta_{kl} = 0$ caso $k \neq l$).

Demonstração. Se uma álgebra satisfaz uma identidade multilinear de grau d, então ela satisfaz uma identidade multilinear de grau d', para todo $d' \in \mathbb{N}$ com $d' \geq d$. Mostraremos que $M_n(K)$ não satisfaz identidades de grau $2n-1$. Seja f um polinômio multilinear não nulo de grau $2n-1$, e escreva

$$f(x_1, \cdots, x_{2n-1}) = \alpha x_1 \cdots x_{2n-1} + \sum_{\sigma \in S_{2n-1}} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(2n-1)}$$

com S_{2n-1} o grupo de permutações de $\{1, 2, \cdots, 2n-1\}$, $\alpha_\sigma \in K, \forall \sigma \in S_{2n-1}$ e $\alpha \in K$ e podemos assumir $\alpha \neq 0$, pois $f \neq 0$. Então

$$f(e_{11}, e_{12}, e_{22}, e_{23}, \cdots, e_{n-1,n-1}, e_{n-1,n}, e_{nn}) = \alpha e_{1n} + \sum_{\sigma \in S_{2n-1}} \alpha_\sigma 0 \neq 0$$

e isso conclui o teorema. □

Exemplo: *Para cada $n \in \mathbb{N}$, denote por $T(M_n(K))$ o T-ideal das identidades polinomiais da álgebra matricial $M_n(K)$. Então*

$$\bigcap_{n \in \mathbb{N}} T(M_n(K)) = 0$$

□

Esse último teorema com enunciado simples tem grandes consequências na estrutura de PI-álgebras. Uma delas é a seguinte:

Teorema 2.10.8. *Seja A uma álgebra primitiva sobre um corpo K que satisfaz uma identidade de grau d. Então o centro de A, $Z = Z(A)$, é um corpo e $dim_Z A \leq (d/2)^2$.*

Demonstração. Pelo corolário 2.1.9, temos $A = M_n(D)$, para D uma álgebra de divisão. Então $Z = Z(A)$ é um corpo. Temos $\dim_Z A = \dim_L (A \otimes_Z L)$, para qualquer $L \supset Z$ corpo, e em particular, tomando L subcorpo maximal de D (c.f. Definição 2.3.6), temos $A \otimes_Z L = M_u(L)$ (Teorema 2.3.8), e $u \leq d/2$. Daí $\dim_Z A = u^2 \leq (d/2)^2$. □

Exemplo: *Seja A uma PI-álgebra. Então $P \lhd A$ é primitivo se e só se é maximal. De fato, se $P \lhd A$ é primitivo, então A/P é uma PI-álgebra primitiva, e então, da forma $M_n(D)$, e em particular, simples. Segue que P é maximal. Em particular, uma PI-álgebra primitiva é simples.* □

Corolário 2.10.9. *Uma PI-álgebra semiprimitiva é o produto subdireto de álgebras simples, cada uma de dimensão finita sobre seu centro, e as dimensões são limitadas. Ainda mais: uma PI-álgebra semiprimitiva é o produto subdireto de álgebras matriciais $M_n(K)$, para algum $n \in \mathbb{N}$ fixo.*

Com o auxílio dessa teoria extra, podemos melhorar um exemplo da seção §2.2:
Exemplo: *Uma PI-álgebra primitiva A sobre um corpo K que satisfaz uma identidade multilinear não satisfeita por $M_2(K)$ é comutativa.*

De fato, seja $Z = Z(A)$, que é corpo, e ainda $dim_Z A < \infty$ (pelo Teorema 2.10.8). Então, sendo $L \subset D$ subcorpo maximal, temos que $A \otimes_Z L$ satisfaz a identidade multilinear f (Teorema 2.10.5), e $A \otimes_Z L = M_u(K)$ (Corolário 2.3.9), para algum $u \in \mathbb{N}$, e se $u > 1$, então $M_u(K) \supset M_2(K)$, o que implicaria que $M_2(K)$ satisfaz f, contradição. Segue que A é comutativo.

Em particular, uma PI-álgebra semiprimitiva que satisfaz uma identidade multilinear não satisfeita por $M_2(K)$ é comutativa. □

Vamos agora exibir um resultado interessantíssimo devido a Levitzki [26], que relaciona elementos nilpotentes com radical de Baer no caso de PI-álgebras. Uma das ideias da demonstração (além de muitas manipulações muito bem colocadas) é que, como A satisfaz uma identidade polinomial (então, ela satisfaz uma identidade multilinear, pela proposição 2.10.4, de algum grau d), então podemos "permutar" os elementos de um produto de d elementos da álgebra, e utilizar esse fato de alguma maneira inteligente. Essa manipulação é uma evidência de que os anéis não-comutativos mais próximos dos anéis comutativos são as PI-álgebras.

Teorema 2.10.10. *Seja A uma PI-álgebra, e assuma que A satisfaz uma identidade polinomial de grau d. Para cada elemento nilpotente $a \in A$, seja $n \in \mathbb{N}$ tal que*

$$a^n \notin B(R), \quad a^{n+1} \in B(R)$$

(em que $B(R)$ é o radical de Baer de R). Então $n < d/2$.

Demonstração. Fixe um $a \in A$ nilpotente e $n \in \mathbb{N}$ como no enunciado. Defina os subanéis

$$\begin{aligned} A_{2j-1} &= a^{n-j+1}(A + \mathbb{Z})a^{j-1} \quad , \quad j = 1, \cdots, n+1 \\ A_{2j} &= a^{n-j+1}(A + \mathbb{Z})a^{j} \quad , \quad j = 1, \cdots, n \end{aligned}$$

e defina

$$B_j = A_1 \cdots A_j, \quad j = 1, \cdots, 2n+1.$$

Note que

$$\begin{aligned} B_{2j-1} &= (a^n(A + \mathbb{Z}))^{2j-1}a^{j-1} \quad , \quad j = 1, \cdots, n+1 \\ B_{2j} &= (a^n(A + \mathbb{Z}))^{2j}a^{j} \quad , \quad j = 1, \cdots, n \end{aligned}$$

Ainda, se $s > t$, temos $A_s A_t \subset (A + \mathbb{Z})a^{n+1}(A + \mathbb{Z})$. Em particular, se $r \in \mathbb{N}$ é tal que $r \leq 2n + 1$, então $a_{\sigma(1)} \cdots a_{\sigma(r)} \in (A + \mathbb{Z})a^{n+1}(A + \mathbb{Z})$, para todo $a_i \in A_i, i = 1, \cdots, r$ e para todo $\sigma \in S_r$

diferente da identidade. Pela proposição 2.10.4, temos que A satisfaz uma identidade multilinear, e podemos escrever que A satisfaz

$$x_1 \cdots x_d = \sum_{\sigma \in S_d, \sigma \neq 1} b_\sigma x_{\sigma(1)} \cdots x_{\sigma(d)}, \quad b_\sigma \in K.$$

Em particular, assumindo por absurdo $n \geq d/2$, temos $n \geq (d-1)/2$, e então, $d \leq 2n+1$, e daí, para todo $a_1 \in A_1, \cdots, a_d \in A_d$, temos

$$a_1 \cdots a_d = \sum_{\sigma \in S_d, \sigma \neq 1} b_\sigma a_{\sigma(1)} \cdots a_{\sigma(d)} \in (A+\mathbb{Z})a^{n+1}(A+\mathbb{Z})$$

o que implica $(a^n(A+\mathbb{Z}))^d a^q = B_d \subset (A+\mathbb{Z})a^{n+1}(A+\mathbb{Z})$, em que $q = d/2$ ou $q = (d-1)/2$, dependendo da paridade de d. Multiplicando ambos por $a^{n-q}(A+\mathbb{Z})$ pela direita, temos, em particular, $(a^n(A+\mathbb{Z}))^{d+1} \subset (A+\mathbb{Z})a^{n+1}(A+\mathbb{Z}) \subset B(R)$, e segue que $a^n(A+\mathbb{Z}) \subset B(R)$ (proposição 2.6.10), e em particular, $a^n \in B(R)$, contradição. Daí, necessariamente $n < d/2$. □

Como consequência, temos o seguinte resultado:

Corolário 2.10.11. *Seja A uma PI-álgebra semiprima e $I \subset A$ um ideal (bilateral, à direita ou à esquerda) nil. Então I é nilpotente (ou seja, A, sendo semiprima, não admite ideais nil).*

Demonstração. De fato, como $S = \{a \in A : a \text{ é nilpotente}\}$ é um subanel de A, o Teorema 2.10.10 diz que S satisfaz a identidade polinomial $x^m = 0$, para algum $m \in \mathbb{N}$. Pelo Teorema de Dubnov–Ivanov–Nagata–Higman 2.10.3, segue que S satisfaz a identidade polinomial $x_1 \cdots x_l = 0$, para algum $l \in \mathbb{N}$. Se $I \subset A$ é um ideal nil, então, $I \subset S$, e então, seus elementos satisfazem $x_1 \cdots x_l = 0$, e em particular, $I^l = 0$, e daí, I é nilpotente. Como, em particular, uma álgebra semiprima não admite ideais nilpotentes, segue que A não admite ideais nil. □

Aqui vale ressaltar que o teorema de Levitzki (ainda em forma muito mais geral) pode ser obtido como um corolário imediato do teorema de Shirshov sobre a altura, um tópico que não trataremos nesta dissertação.

A seguir, provaremos alguns teoremas, devidos a Amitsur (em [1]), que seguem da estrutura de álgebras não comutativas e da estrutura de PI-álgebras.

Lema 2.10.12. *Sejam $T \subset K\langle X\rangle$ um T-ideal, com X infinito, $A = K\langle X\rangle/T$ e $p(x_1, \cdots, x_n) \in K\langle X\rangle$ homogêneo em x_1. Então, $p(x_1, \cdots, x_n) \in J(A)$ se e só se p é nilpotente em A.*

Demonstração. Se p é nilpotente em A, então já sabemos que $p \in J(A)$.

Reciprocamente, se $p \in J(A)$, então existe $q \in J(A)$ tal que $p + q - pq = 0$, o que implica (igualdade em A) em

$$q = pp + pq = -p - p^2 + p^2 q = \cdots = -p - p^2 - \cdots - p^n + p^n q$$

Olhando p e q como polinômios em $K\langle X\rangle$, escreva $q = \sum_{i=1}^m q_i$, com q_i homogêneo em x_1 de grau i em x_1. Então

$$q + \sum_{i=1}^n p^i - p^n q = \sum_{j=0}^m q_j + \sum_{j=1}^n p^i - \sum_{j=0}^m p^n q_j \in T$$

tomando $n > m$, obtemos que p^n é uma componente homogênea em x_1, e então, $p^n \in T$, concluindo o resultado. □

Teorema 2.10.13. *Se A é uma PI-álgebra semiprima, então a álgebra relativamente livre $F := K\langle X\rangle/T(A)$ é semiprimitiva.*

Demonstração. Seja $p(x_1, \cdots, x_m) \in J(F)$. Então $p(x_1, \cdots, x_m)x_{m+1} \in J(F)$ e, pelo lema anterior 2.10.12, $p(x_1, \cdots, x_m)x_{m+1}$ é nil. Isso implica, em particular, que fixados $a_1, \cdots, a_m \in A$, o ideal $p(a_1, \cdots, a_m)(A + \mathbb{Z}) \subset A$ é nil, e portanto, pelo corolário 2.10.11, necessariamente o ideal é nulo, e em particular, $p(a_1, \cdots, a_m) = 0$. Mas então, como $a_1, \cdots, a_m \in A$ são arbitrários, segue que $p(x_1, \cdots, x_m)$ é uma identidade polinomial de A, de onde segue que $p \in T(A)$, ou seja, $p = 0$ em F, e em particular, F é semiprimitiva. □

Como consequência desse teorema, obtemos:

Teorema 2.10.14. *Seja $T \subset K\langle X\rangle$ um T-ideal. Então o radical de Jacobson $J/T = J(K\langle X\rangle/T)$ é nil. Ainda mais: J é um T-ideal.*

Demonstração. Seja $B/T = B(K\langle X\rangle/T)$ o radical de Baer da álgebra relativamente livre e defina a álgebra $A := K\langle X\rangle/B \simeq (K\langle X\rangle/T)/(B/T)$. Como A é uma imagem homomórfica de $K\langle X\rangle/T$, segue que A é uma PI-álgebra e A satisfaz todas as identidades em T. Ainda, pelo teorema anterior, temos que $K\langle X\rangle/T(A)$ é semiprimitivo, pois A é semiprima. Note que $T \subset T(A) \subset B$ por construção, e ainda, por um dos teoremas do isomorfismo:

$$K\langle X\rangle/T(A) \simeq \frac{K\langle X\rangle/T}{T(A)/T}$$

o que implica, em particular (lema 2.2.3), que $J \subset T(A) \subset B$, e como já sabemos, $B \subset J$, o que implica $J = B$, e resulta que $J/T = B/T$ é nil. Ainda mais, dessa continência de conjuntos, conclui-se também que $J = T(A)$, e em particular, J é um T-ideal. □

Por fim, segundo a teoria desenvolvida de estrutura, iremos caracterizar o radical de Jacobson de uma álgebra relativamente livre (resultado de Amitsur, [1]).

Teorema 2.10.15. *Os ideais $T(M_n(K))$ são os únicos T-ideais P tal que $K\langle X\rangle/P$ é semiprimitivo.*

Demonstração. Seja P um T-ideal tal que $F := K\langle X\rangle/P$ é semiprimitivo. Então, pelo corolário 2.10.9, segue que F é produto subdireto de álgebras matriciais $M_n(K)$, e em particular, necessariamente $P = T(M_n(K))$ (c.f. Teorema 2.2.12). □

Como consequência, obtemos de imediato:

Teorema 2.10.16. *Seja $T \subset K\langle X\rangle$ um T-ideal. Então o radical de Jacobson $J(K\langle X\rangle/T) = T(M_n(K))/T$, para algum $n \in \mathbb{N}$.*

Por fim, iremos comentar como podemos aplicar a teoria desenvolvida sobre representações de S_n.

Temos que P_n admite uma estrutura natural de S_n-módulo, dada pela seguinte ação:

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

para cada $\sigma \in S_n$ e $x_{i_1} \cdots x_{i_n} \in P_n$. Os conjuntos $PL_n := P_n \cap L(X)$ (os polinômios lineares de Lie) e $\Gamma_n =$ (combinação linear de produto de comutadores) $\cap P_n$ (os polinômios próprios lineares, definição 3.3.1) também admitem naturalmente uma estrutura de S_n-módulo.

Dada uma PI-álgebra A, denotaremos por $P_n(A) = P_n/(P_n \cap T(A))$, $PL_n(A) = PL_n/(PL_n \cap T(A))$ e $\Gamma_n(A) = \Gamma_n/(\Gamma_n \cap T(A))$ (o caso $PL_n(A)$ também pode ser definido para uma álgebra de Lie). Note que, dados $f, g \in P_n$, f é consequência de g se e só se $f \in KS_n g$. Também $g \in KS_n f$, se e só se g é consequência de f. Então, em particular, os conjuntos $P_n(A), PL_n(A), \Gamma_n(A)$ também admitem uma estrutura natural de S_n-módulo.

Utilizaremos a notação trabalhada na seção §2.8 (resumido totalmente no Teorema 2.8.11). Dado um diagrama D_λ, tomando o elemento gerador do S_n-módulo irredutível $e(D_\lambda)$ relacionado ao diagrama D_λ, e dado um polinômio multilinear $f(x_1, \cdots, x_n)$, note que o polinômio g obtido identificando as variáveis que estão na mesma linha do diagrama D_λ de $e(D_\lambda)f$ é equivalente a $e(D_\lambda)f$. De fato, g é obtido de $e(D_\lambda)f$ por identificação de variáveis, e então, g é consequência de $e(D_\lambda)f$, e reciprocamente, $e(D_\lambda)f$ pode ser obtido de g a partir de sua linearização total (e então, com K adequado (por exemplo, característica zero), obtemos a equivalência das identidades). Por exemplo, assuma $f(x_1, \cdots, x_n) = x_1 \cdots x_n$, e considere uma tabela relacionado a partição $\lambda = (n_1, \cdots, n_l) \vdash n$, e tome um diagrama D_λ preenchendo os números de 1 a n em sequência, iniciando de cima para baixo na primeira coluna, seguindo de cima para baixo na segunda coluna, e assim sucessivamente. Então, fazendo as identificações das variáveis na mesma linha do diagrama D_λ, obtemos

$$g(x_1, \cdots, x_{m_1}) = s_{m_1}(x_1, \cdots, x_{m_1}) s_{m_2}(x_1, \cdots, x_{m_2}) \cdots s_{m_p}(x_1, \cdots, x_{m_p})$$

em que $s_m(x_1, \cdots, x_m)$ é a identidade standard e $(m_1, \cdots, m_p) \vdash n$ é a **partição conjugada** de $(n_1, \cdots, n_l)$, ou seja, m_1 é a quantidade de elementos na primeira coluna da tabela T_λ, m_2 é a quantidade de elementos na segunda coluna de T_λ, e assim sucessivamente. A vantagem dessa identificação é a simplificação ao exibir o polinômio gerador do S_n-módulo irredutível.

Se M_λ é um S_n-submódulo irredutível de P_n (PL_n, Γ_n, $P_n(A)$, $PL_n(A)$ ou $\Gamma_n(A)$, com A uma PI-álgebra), então M_λ é isomorfo como S_n-módulo a $S_n e(D_\lambda)$, e é um S_n-submódulo da soma dos S_n-submódulos irredutíveis de P_n isomorfos a $S_n e(D_\lambda)$. Então, exite um polinômio $f(x_1, \cdots, x_n) \in M_\lambda$ tal que

$$M_\lambda = (KS_n)(e(D_\lambda)f)$$

ou, em outras palavras, existem elementos $a_\sigma \in K$, com $\sigma \in S_n$, tais que

$$e(D_\lambda) \left(\sum_{\sigma \in S_n} a_\sigma \sigma \right) x_1 \cdots x_n$$

é um gerador de M_λ. A decomposição de P_n é relativamente fácil, pois os S_n-módulos irredutíveis são gerados simplesmente por elementos da forma $e(D_\lambda)x_1 \cdots x_n$ (e então, bastaríamos encontrar todos os $e(D_\lambda)$, que dependem apenas dos diferentes diagramas D_λ obtidos da mesma partição λ, que geram S_n-módulos diferentes - e existem teoremas que classificam isso), é um processo trabalhoso, mas pode ser obtido de forma sistemática com um algoritmo.

Para as decomposições de $PL_n, \Gamma_n, P_n(A), PL_n(A), \Gamma_n(A)$ o processo já se torna bem mais difícil, e exige muito mais paciência, contas, astúcia e existe uma vasta teoria nesse sentido para refinamento das contas.

Na seção seguinte, iremos refinar muitos resultados nessa área, e iremos trabalhar principalmente com polinômios de Lie lineares e polinômios próprios lineares, obtendo assim muitas técnicas no estudo das identidades de uma álgebra.

Capítulo 3

Resultados Preliminares em PI-álgebras

Neste capítulo, serão apresentados resultados importantíssimos para os resultados principais desta dissertação, e alguns bem específicos (mas não deixando de ser muito importantes para a teoria geral).

Nas seções 3.1 e 3.2, seguiremos os estudos de Amitsur ([2, 3, 1]), e estudaremos com mais profundidade o Radical de Jacobson de uma Álgebra. Na seção 3.1, provaremos que o Radical numa álgebra finitamente gerada sobre um corpo não enumerável é nil. Este resultado será fundamental na seção 3.2, em que (desenvolvendo uma belíssima teoria) será provado que o Radical de Jacobson de uma PI-álgebra é nil (sem restrições ao corpo).

Na seção 3.3 e 3.4, exibiremos, respectivamente, definições e noções básicas sobre polinômios próprios e matrizes genéricas. A importância desses objetos ficará claro nas seções seguintes, que aplicaremos a teoria desenvolvida anteriormente, combinando técnicas com polinômios próprios e matrizes genéricas. Toda a exposição foi baseada no livro de Drensky [9].

Na seção 3.5, apresentaremos noções básicas e enunciaremos diversos resultados importantíssimos sobre representações do Grupo Geral Linear. A exposição será baseada nos livros de Drensky [9] e no livro de Bahturin [5].

Na seção 3.6, apresentaremos resultados de aplicações de representações de S_n-módulos em polinômios multilineares. A seção será baseada nos trabalhos e livro de Drensky [10, 9] e no livro de Bahturin [5], e será combinação das técnicas de representações apresentadas na seção anterior, e das técnicas das matrizes genéricas e polinômios próprios.

Na seção 3.7, definiremos um conceito devido a Razmyslov (identidades fracas, [28]), e provaremos alguns resultados envolvendo manipulações de identidades fracas, que podem ser encontradas nos artigos de Razmyslov [29, 30]. Essas manipulações serão utilizadas diretamente nas demonstrações dos teoremas nas 4 primeiras seções do próximo capítulo, e serão referenciadas constantemente.

§3.1 Radical de Jacobson nil

Esta seção irá explorar a estrutura do Radical de Jacobson de uma álgebra, e provaremos que o radical de uma álgebra finitamente gerada sobre um corpo não-enumerável é nil (Teorema de Amitsur [2]). Este resultado será a base para demonstrar que o radical de uma PI-álgebra finitamente gerada é nil (independente do corpo).

Toda a linguagem e estudo desenvolvidos nesta seção serão utilizados exclusivamente para demonstrar o resultado principal da seção, e não serão referenciados posteriormente.

A teoria desenvolvida sobre o Radical de Jacobson nas seções §2.2 e §2.4 será suficiente para esta seção.

Começaremos com uma definição que trará uma descrição muito boa sobre o radical:

Definição 3.1.1. Sejam A uma álgebra sobre um corpo K com unidade 1 e $a \in A$. Dizemos que a é **algébrico** se a subálgebra I_a de A gerada por a e 1 tem dimensão finita sobre o corpo K. Caso contrário, dizemos que a é transcendente.

Lema 3.1.2. *Sejam A uma álgebra com unidade 1 e $J(A)$ seu radical de Jacobson. Então, os elementos de $J(A)$ são transcendentes ou nilpotentes.*

Demonstração. Seja $a \in J(A)$ algébrico e seja I_a a subálgebra de A gerada por 1 e a. Então, existe $m \in \mathbb{N}$ tal que $a^m I_a = a^{m+1} I_a$, uma vez que $a^m I_a$ e $a^{m+1} I_a$ são subálgebras da álgebra de dimensão finita I_a e $a^{m+1} I_a \subset a^m I_a$. Daí, existe $b \in I_a$ tal que $a^{m+1} b = a^{m+1}$, uma vez que $a^{m+1} \in a^m I_a$. Como $b \in I_a \subset J(A)$, segue que existe $c \in J(A)$ tal que $b \odot c = 0$. Então

$$0 = a^{m+1}(b \odot c) = a^{m+1}(b + c - bc) = \underbrace{a^{m+1}b}_{a^{m+1}} + a^{m+1}c - \underbrace{a^{m+1}b}_{a^{m+1}}c = a^{m+1}$$

e logo a é nilpotente. □

Nosso objetivo será mostrar que, em certas hipóteses, todos os elementos de $J(A)$ são algébricos.

Exemplo: *Se todos os elementos de uma álgebra são algébricos, então $J(A)$ é nil.* □

Fixado $a \in A$ e considerando a álgebra I_a gerada por 1 e a, existe uma relação entre o anel de polinômios $K[x]$ e I_a, dada pelo seguinte homomorfismo:

$$\psi_a : f(x) \in K[x] \mapsto f(a) \in I_a$$

em que $f(a)$ é a avaliação do polinômio f em a. Temos que ψ_a é um homomorfismo de álgebras sobrejetor, e a é transcendente se e só se $\operatorname{Ker} \psi_a = 0$ (ou seja, se ψ_a é isomorfismo).

No que segue nesta seção, iremos trabalhar livremente com polinômios $f(x) \in K[x]$, e iremos passar para I_a avaliando f em a, sem mencionar ψ_a.

Exemplo: *Utilizando o algoritmo de divisão, pode-se mostrar que $K[x]$ é um domínio de ideais principais. Com isso, podemos demonstrar facilmente os seguintes fatos, (que não serão necessários nesta seção):*

1. *$\operatorname{Ker} \psi_a$ é gerado por um polinômio mônico, que será denotado por $p_a(x)$.*
2. *$\operatorname{Ker} \psi_a \neq 0$ se e só se existe $f(x) \in K[x]$, $f \neq 0$, tal que $f(a) = 0$. Neste caso, p_a divide f.*

3. *Seja $b \in I_a$ e escreva $b = f(a)$, com $f \in K[x]$. Então b é invertível em I_a se e só se $mdc(f, p_a) = 1$.*

□

Até o fim desta seção, a menos que se diga o contrário, A será uma álgebra com unidade 1, $a \in A$ fixo e I_a a álgebra gerada por 1 e a.

Definição 3.1.3. Um elemento $\alpha \in K$ é dito estar no **espectro** de a se $a - \alpha \cdot 1$ for não invertível em I_a. Denota-se o conjunto de elementos do espectro de a por $\sigma(a)$. O complementar de $\sigma(a)$ é denominado o conjunto **resolvente** de a e será denotado por $\rho(a)$.

O próximo lema será o principal argumento para demonstrar o resultado principal desta seção:

Lema 3.1.4. *Sejam $\alpha_1, \cdots, \alpha_m \in \rho(a)$ distintos. Então $(a - \alpha_1 \cdot 1)^{-1}, \cdots, (a - \alpha_m \cdot 1)^{-1}$ são linearmente independentes ou a é algébrico.*

Demonstração. Assuma que existem $\beta_1, \cdots, \beta_m \in K$ não todos nulos tais que

$$\beta_1(a - \alpha_1 \cdot 1)^{-1} + \cdots + \beta_m(a - \alpha_m \cdot 1)^{-1} = 0.$$

Multiplicando por $\prod_{i=1}^{m}(a - \alpha_i \cdot 1)$, obtemos que

$$\beta_1 f_1(a) + \cdots + \beta_m f_m(a) = 0$$

em que $f_i(x) = \prod_{j \neq i}(x - \alpha_j)$. Seja $f(x) = \sum_{i=1}^{m} \beta_i f_i(x)$. Temos $f \neq 0$, pois caso contrário, para cada $i \in \{1, \cdots, m\}$, teríamos $0 = f(\alpha_i) = \beta_i f_i(\alpha_i)$, e uma vez que $\alpha_1, \cdots, \alpha_m$ são distintos, teríamos $f_i(\alpha_i) \neq 0$, o que implicaria $\beta_i = 0, i = 1, \cdots, m$, contradição.

Daí $f \neq 0$, e ainda, $f(a) = \beta_1 f_1(a) + \cdots + \beta_m f_m(a) = 0$, o que implica que a é algébrico. □

Com isso, podemos demonstrar o resultado principal desta seção:

Teorema 3.1.5. *Seja A uma álgebra (não necessariamente com unidade) sobre um corpo K tal que a cardinalidade de K seja maior que (o número cardinal) $dim_K A$. Então o radical $J(A)$ é nil.*

Demonstração. Seja $A^* = 1 \cdot K \oplus A$ a álgebra obtida adicionando uma unidade 1 a A. Como $A \subset A^*$ e $J(A) = J(A^*)$ (Corolário 2.4.5), basta trabalharmos com A^* e mostrar que $J(A^*)$ é nil.

Fixe $a \in J(A^*)$. Então $1 - a\alpha$ é invertível para todo $\alpha \in K$, e daí, $\alpha^{-1} \in \rho(a)$, para todo $\alpha \in K$, $\alpha \neq 0$.

Então devem existir $\alpha_1, \cdots, \alpha_m \in \rho(a)$ distintos tais que $(a - \alpha_1 \cdot 1)^{-1}, \cdots, (a - \alpha_m \cdot 1)^{-1}$ são linearmente dependentes, pois caso contrário, teríamos um conjunto de elementos linearmente independentes maior do que $\dim_K A^*$ (note que, no máximo, $\dim_K A^* = \dim_K A + 1$), contradição, e daí, a será algébrico, pelo lema 3.1.4. Pelo lema 3.1.2, a é nilpotente, e isso prova o resultado. □

Corolário 3.1.6. *Uma álgebra finitamente gerada sobre um corpo não enumerável tem radical de Jacobson nil.*

§3.2 Extensão de Hilbert's Nullstellensatz

Seja K um corpo. Nesta seção, denotaremos por $K[\xi_1, \cdots, \xi_n]$ o anel de polinômios com variáveis comutativas $\xi_1, \cdots, \xi_n$, e $K\langle x_1, \cdots, x_n\rangle$ (ou simplesmente por $K\langle X_n\rangle$) a álgebra associativa não comutativa com unidade nas variáveis $x_1, \cdots, x_n$ e $\bar{K}$ o fecho algébrico de K.

Uma das equivalentes formas de enunciar o clássico teorema de zeros de Hilbert é a seguinte:

> Sejam $f \in \bar{K}[\xi_1, \cdots, \xi_n]$ e $G \subset \bar{K}[\xi_1, \cdots, \xi_n]$. Então, se $f(\alpha_1, \cdots, \alpha_n) = 0$ sempre que $g(\alpha_1, \cdots, \alpha_n) = 0, \forall g \in G$, $\alpha_1, \cdots, \alpha_n \in \bar{K}$, então existe $m \in \mathbb{N}$ tal que f^m está no ideal gerado por G.

A teoria desenvolvida por Amitsur [3] generaliza e estende este resultado, e o teorema generalizado não será apresentado explicitamente aqui. Nosso objetivo principal será demonstrar que o radical de Jacobson de uma PI-álgebra finitamente gerada é nil.

Ao resto desta seção, fixaremos um corpo K, $n \in \mathbb{N}$, $G \subset K\langle X_n\rangle$ e $f \in K\langle X_n\rangle$.

Definição 3.2.1. Seja A uma álgebra sobre K. Uma n-upla $(a_1, \cdots, a_n)$ de elementos de A é dito ser um **zero** de G se $g(a_1, \cdots, a_n) = 0, \forall g \in G$.

Definição 3.2.2. Sejam A uma álgebra simples sobre K e $Z = Z(A)$ seu centro. Um conjunto $(a_1, \cdots, a_n)$ de elementos de A é dito ser um **zero regular** de G em A se $(a_1, \cdots, a_n)$ é zero de G e se $Z[a_1, \cdots, a_n] = A$ (a álgebra gerada por Z e por $a_1, \cdots, a_n$).

Definição 3.2.3. O polinômio f é dito satisfazer a propriedade (Z_k^R) (para algum $k \in \mathbb{N}$) se $f(a_1, \cdots, a_n) = 0$ para todo conjunto de zeros regulares $(a_1, \cdots, a_n)$ de G em $M_r(\bar{K})$, $r \leq k$.

Para o resto desta seção, fixe $k \in \mathbb{N}$, denote por $I(G)$ o ideal gerado por G em $K\langle X_n\rangle$, $T(M_k(\bar{K}))$ o T-ideal das identidades de matrizes $k \times k$, $T_n(M_k(\bar{K})) = T(M_k(\bar{K})) \cap K\langle X_n\rangle$, $Q_k = I(G) + T_n(M_k(\bar{K}))$ e $J_k \subset K\langle X_n\rangle$ ideal tal que o radical de Jacobson $J(K\langle X_n\rangle/Q_k) = J_k/Q_k$.

Lema 3.2.4. *Sejam $H = \bar{K}(\eta_1, \cdots, \eta_m)$ uma extensão de $\bar{K}$, com $\{\eta_1, \cdots, \eta_m\}$ algebricamente independente (definição 2.5.1) e $\{\lambda_1, \cdots, \lambda_l\} \subset H$ um conjunto finito. Então, existe uma especialização $\psi : H \to K$ (definição 2.5.9) tal que, se $\lambda_i \neq 0$, então $\psi(\lambda_i) \neq 0$ e $\psi(\lambda_i) \neq \infty$, para cada $i = 1, \cdots, l$.*

Demonstração. Se $\lambda_i \neq 0$, então escreva

$$\lambda_i = \frac{f_i(\eta_1, \cdots, \eta_m)}{g_i(\eta_1, \cdots, \eta_m)}$$

$i = 1, \cdots, l$. Sendo $\bar{K}$ infinito, existem $a_1, \cdots, a_m \in \bar{K}$ tais que $f_i(a_1, \cdots, a_m)g_i(a_1, \cdots, a_m) \neq 0, \forall i = 1, \cdots, l$ tal que $\lambda_i \neq 0$. Então, a especialização $\psi : H \to \bar{K}$ tal que $\psi(\eta_i) = a_i, i = 1, \cdots, l$, é a especialização requerida. □

Com isso, podemos demonstrar que a propriedade (Z_k^R) não é limitada a $M_k(\bar{K})$, isto é, o seguinte resultado:

Lema 3.2.5. *Se f se anula em todos os zeros regulares de G em $M_k(\bar{K})$, então f zera em todos os zeros regulares de G em $M_k(H)$, sendo H qualquer extensão de corpos $H|\bar{K}$.*

Demonstração. Assuma $H|K$ extensão de corpos e assuma por absurdo que existem $a_1, \cdots, a_n \in M_k(H)$ zero regular de G tal que $f(a_1, \cdots, a_n) \neq 0$. Considere os elementos $\{\lambda_1, \cdots, \lambda_l\}$ de H que aparecem nas entradas de $a_1, \cdots, a_n, f(a_1, \cdots, a_n)$ e tome $H' = \bar{K}(\lambda_1, \cdots, \lambda_l)$. Então, por teorema 2.5.4, existe um subconjunto algebricamente independente $\{\eta_1, \cdots, \eta_m\} \subset \{\lambda_1, \cdots, \lambda_l\}$ tal que $H' = \bar{K}(\eta_1, \cdots, \eta_m)$ e daí, pelo lema 3.2.4, existe especialização $\psi : H' \to \bar{K}$ tal que $\psi(\lambda_i) \neq 0$, se $\lambda_i \neq 0$ e $\psi(\lambda_i) \neq \infty, i = 1, \cdots, l$. Então, considerando a especialização induzida $\psi_k : M_k(H') \to M_k(\bar{K})$, e usando as suas propriedades (Proposição 2.5.11), temos que, para cada $g \in G$

$$0 = \psi_k(g(a_1, \cdots, a_n)) = g(\psi_k(a_1), \cdots, \psi_k(a_n)).$$

Logo $(\psi_k(a_1), \cdots, \psi_k(a_n))$ é um zero de G em $M_k(\bar{K})$. Note ainda que, por escolha da especialização, temos $f(\psi_k(a_1), \cdots, \psi_k(a_n)) \neq 0$. Ainda, como $(a_1, \cdots, a_n)$ é um zero regular de $M_k(H)$, temos $H(a_1, \cdots, a_n) = M_k(H)$ (a álgebra gerada por $H \cdot 1$ e $a_1, \cdots, a_n$). Dado $a \in M_k(\bar{K}) \subset M_k(H)$, temos $a = \sum \alpha_o a_1^{o_1} \cdots a_n^{o_n}$ (combinação linear de produtos de elementos de $a_1, \cdots, a_n$), então,

$$a = \psi_k(a) = \sum \alpha_o \psi_k(a_1)^{o_1} \cdots \psi_k(a_n)^{o_n}$$

o que implica que $(\psi_k(a_1), \cdots, \psi_k(a_n))$ é um zero regular de G em $M_k(\bar{K})$, e chega-se a uma contradição. □

Corolário 3.2.6. *Se f satisfaz (Z_k^R), então f zera para todos os zeros regulares de A, sendo A uma álgebra simples sobre K tal que $dim_Z A \leq k^2$, em que $Z = Z(A)$.*

Demonstração. Seja L um corpo tal que $A \otimes_K L \simeq M_o(L)$, em que $o = \dim_Z A$ (corolário 2.3.9), e considere um corpo H contendo $\bar{K}$ e L. Então, como $H = L \otimes_K H$, temos

$$A \otimes_K H = A \otimes_K L \otimes_K H \simeq M_o(L) \otimes_K H \simeq M_o(H).$$

Como $A \subset A \otimes_K H \simeq M_o(H)$, os zeros regulares de G em A são zeros regulares em $A \otimes_K H$, e pelo lema 3.2.5, segue o resultado. □

Com este resultado, podemos caracterizar o ideal J_k:

Lema 3.2.7. *$f \in J_k$ se e só se f satisfaz (Z_k^R).*

Demonstração. Assuma que f satisfaz (Z_k^R). Então, dado P ideal primitivo de $K\langle X_n\rangle$ contendo Q_k, temos $K\langle X_n\rangle/P$ PI-álgebra primitiva, logo, é simples (exemplo após Teorema 2.10.8) de dimensão sobre o centro menor ou igual a k^2 (uma vez que $K\langle X_n\rangle/P$ contém as identidades de $M_k(\bar{K})$). Definindo $\bar{x}_i = x_i + P \in K\langle X_n\rangle/P$, como $G \subset P$, temos $g(\bar{x}_1, \cdots, \bar{x}_n) = 0, \forall g \in G$, e pelo corolário 3.2.6, $f(\bar{x}_1, \cdots, \bar{x}_n) = 0$, o que implica $f \in P$, e segue que $f \in J_k$.

Reciprocamente, assuma $f \in J_k$ e seja $(a_1, \cdots, a_n)$ zero regular de G em $M_r(\bar{K})$, com $r \leq k$. Considere a álgebra $A = K[a_1, \cdots, a_n] \subset M_r(\bar{K})$ e tome o homomorfismo de álgebras $\pi : K\langle X_n\rangle \to A$ tal que $\pi(x_i) = a_i, i = 1, \cdots, n$. Seja $P = \operatorname{Ker}\pi$. Verifica-se facilmente que $Q_k \subset P$, uma vez que $T_n(M_k(\bar{K})) \subset T_n(M_r(\bar{K})) \subset P$ e $I(G) \subset P$ (pois $(a_1, \cdots, a_n)$ é zero de G).Temos A PI-álgebra e simples, e em particular, A é primitiva, e então, P é primitivo (pois $K\langle X_n\rangle/P \simeq A$) e contém Q_k. Como $f \in P$, segue que $f(a_1, \cdots, a_n) = 0$, ou seja, f satisfaz (Z_k^R). □

Com isso, podemos demonstrar a seguinte caracterização mais completa de J_k:

Teorema 3.2.8. *São equivalentes:*

(i) f *satisfaz* (Z_k^R)

(ii) $f \in J_k$

(iii) f *gera um ideal à direita (e/ou à esquerda) nil módulo* Q_k *(isto é,* $f + Q_k$ *gera um ideal nil em* $K\langle X_n\rangle/Q_k$*)*

Demonstração. $(i) \iff (ii)$: segue pelo lema 3.2.7.
$(iii) \Rightarrow (ii)$: por J_k/Q_k ser o radical de Jacobson de $K\langle X_n\rangle/Q_k$.
$(ii) \Rightarrow (iii)$: Seja $H|K$ uma extensão de corpos com H não enumerável. Então, pelo lema 3.2.5, f satisfaz (Z_k^R) para H. Pelo lema 3.2.7, temos $f \in J(H\langle X_n\rangle/Q_k(H))$, em que $Q_k(H) = H\langle X_n\rangle \cap (T_n(M_k(H))+I_H(G))$, com $I_H(G)$ o ideal gerado por G em $H\langle X_n\rangle$, e temos que $I_H(G) = I(G)\otimes_K H$ e, pelo lema 2.10.6, temos $H\langle X_n\rangle \cap T_n(M_k(H)) = (K\langle X_n\rangle \cap T_n(M_k(K)) \otimes_K H$. Então $Q_k(H) = Q_k \otimes H$. Pelo corolário 3.1.6, segue que $J(H\langle X_n\rangle/Q_k(H))$ é nil, e existe $o \in \mathbb{N}$ tal que $f^o \in Q_k(H)$, e como $f^o \in K\langle X_n\rangle$, segue que $f^o \in Q_k$.

Como f satisfaz (Z_k^R), claro que os elementos de $K\langle X_n\rangle$ (e $K\langle X_n\rangle f$) satisfazem (Z_k^R), e então f gera um ideal à direita (e à esquerda) nil módulo Q_k. □

Em particular, o radical de Jacobson de $K\langle X_n\rangle/Q_k$ é nil. Com essa teoria, podemos provar o resultado principal desta seção:

Teorema 3.2.9. *Seja* A *uma PI-álgebra finitamente gerada. Então o radical de Jacobson de* A *é nil.*

Demonstração. Denote por $A = K\langle a_1, \cdots, a_n\rangle$ e $K\langle X_\infty\rangle = K\langle x_1, x_2, \cdots\rangle$ a álgebra livre não comutativa com unidade em infinitas variáveis. Considere o homomorfismo $K\langle X_\infty\rangle \to A$ tal que $x_i \mapsto a_i, i = 1, \cdots, n$ e $x_i \mapsto 0$ para $i > n$, e tome Q_∞ seu núcleo. Note que $Q_\infty \supset T(A)$, o T-ideal das identidades de A. Seja $Q = Q_\infty \cap K\langle X_n\rangle$. Note que $K\langle X_n\rangle/Q \simeq K\langle X_\infty\rangle/Q_\infty \simeq A$.

Por teorema 2.10.14, temos $J(K\langle X_\infty\rangle/T(A))$ nil, e por teorema 2.10.16, temos $J(K\langle X_\infty\rangle/T(A)) = T(M_k(K))/T(A)$, para algum $k \in \mathbb{N}$.
Afirmação 1: $(T(M_k(K)) + Q_\infty)/Q_\infty$ é nil.
De fato, $(T(M_k(K)) + Q_\infty)/Q_\infty \simeq T(M_k(K))/(T(M_k(K) \cap Q_\infty)$, e este último é a imagem homomórfica de $T(M_k(K))/T(A)$, uma vez que $T(A) \subset Q_\infty \cap T(M_k(K))$.

Denote por $J(K\langle X_\infty\rangle/Q_\infty) = J_0/Q_\infty (\simeq J(A))$.
Afirmação 2: $J(K\langle X_\infty\rangle/(T(M_k(K)) + T(A))) = J_0/(T(M_k(K)) + T(A))$
De fato, como $(T(M_k(K))+T(A))/Q_\infty$ é nil, segue que $J_0 \supset T(M_k(K))+T(A)$, e ainda, $J(K\langle X_\infty\rangle/(T(M_k(K))+T(A)) = J_0/(T(M_k(K))+T(A))$, pois, por lema 2.4.2, $J_0/(T(M_k(K))+T(A)) \subset J(K\langle X_\infty\rangle/(T(M_k(K)+T(A)))$, e como

$$\frac{K\langle X_\infty\rangle/(T(M_k(K)) + T(A))}{J_0/(T(M_k(K)) + T(A))} \simeq K\langle X_\infty\rangle/J_0 \simeq \frac{K\langle X_\infty\rangle/Q_\infty}{J_0/Q_\infty}$$

é semiprimitivo, implica $J_0/(T(M_k(K)) + T(A)) \supset J(K\langle X_\infty\rangle/(T(M_k(K)) + T(A)))$ e vale a igualdade.

Considere o isomorfismo $\pi : K\langle X_\infty\rangle/Q_\infty \to K\langle X_n\rangle/Q$ tal que $x_i \mapsto x_i, i = 1, \cdots, n$ e $x_j \mapsto 0, j > n$. Seja J/Q a imagem de J_0/Q_∞ por esse isomorfismo.
Afirmação 3: $(T(M_k(K)) + Q_\infty)/Q_\infty \simeq (T_n(M_k(K)) + T(A))/Q$
De fato, o isomorfismo π mapeia $(T(M_k(K))+Q_\infty)/Q_\infty$ sobre $(T_n(M_k(K))+Q)/Q$, pois $T_n(M_k(K))+Q \subset T(M_k(K)) + Q_\infty$ (no sentido de, se $f(x_1, \cdots, x_n) \in T_n(M_k(K)) + Q$, então, visualizando $f(x_1, \cdots, x_n)$ como elemento de $K\langle X_\infty\rangle$, temos $f \in T(M_k(K)) + Q_\infty$). Como o núcleo de restrições

de π ainda são nulos, segue que vale o isomorfismo.
Afirmação 4: $J(K\langle X_n\rangle/(T_n(M_k(K))+T_n(A))) = J/(T_n(M_k(K))+T_n(A))$
Como π é isomorfismo, temos $J(K\langle X_n\rangle/Q) = J/Q = \pi(J_0/Q_\infty)$. Ainda, π induz isomorfismo $\bar{\pi}$ entre $K\langle X_\infty\rangle/(T(M_k(K))+Q)$ e $K\langle X_n\rangle/(T_n(M_k(K))+Q)$, pois

$$\frac{K\langle X_\infty\rangle}{(T(M_k(K))+Q_\infty)} \simeq \frac{K\langle X_\infty\rangle/Q_\infty}{(T(M_k(K))+Q_\infty)/Q_\infty} \simeq \frac{K\langle X_n\rangle/Q}{(T_n(M_k(K))+Q)/Q} \simeq \frac{K\langle X_n\rangle}{(T_n(M_k(K))+Q)}$$

Ainda

$$J_0/(T(M_k(K))+Q_\infty) \simeq \frac{J_0/Q_\infty}{(T(M_k(K))+Q_\infty)/Q_\infty} \simeq \frac{J/Q}{(T_n(M_k(K))+Q)/Q} \simeq J/(T_n(M_k(K))+Q)$$

e em particular, $J(K\langle X_n\rangle/(T_n(M_k(K))+Q)) = J/(T_n(M_k(K))+Q)$.
Afirmação 5: $J(A)$ é nil.
De fato, como $A \simeq K\langle X_n\rangle/Q$, temos $J(A) \simeq J(K\langle X_n\rangle/Q) = J/Q$. Mas, combinando a afirmação 3 e 1, temos $(T_n(M_k(K))+Q)/Q$ nil, e como $T_n(M_k(K))+Q$ é um ideal da forma Q_k (segundo a notação fixa desta seção), segue, pelo teorema 3.2.9, que $J/(T_n(M_k(K))+Q)$ é nil. Daí J/Q é nil, o que implica $J(A)$ nil. □

Recordamos que este teorema foi generalizado de maneira significativa por Razmyslov, Kemer e Braun. Razmyslov, em 1974, demonstrou que se A é uma PI-álgebra associativa e finitamente gerada, sobre corpo de característica 0, então $J(A)$ é *nilpotente* se e somente se A satisfaz alguma identidade de Capelli (vide [42]). Mais tarde, em 1980, Kemer provou que toda PI-álgebra, finitamente gerada sobre um corpo de característica 0, satisfaz alguma identidade de Capelli (vide [40]). Assim foi demonstrado que sobre corpos de característica 0, o radical de PI álgebras finitamente geradas é nilpotente. Mais tarde Braun, em 1984, mostrou que o teorema de Razmyslov–Kemer é válido se substituirmos o corpo por qualquer anel comutativo e noetheriano (vide [38]). Atualmente este teorema é conhecido com o nome Teorema de Razmyslov, Kemer e Braun.

§3.3 Polinômios Próprios

Nesta seção, apresentaremos noções básicas de polinômios próprios, e discutiremos a sua importância na teoria de PI-álgebras. A teoria aqui será baseada no livro de Drensky [9].

Nesta seção, será conveniente considerar $K\langle X\rangle$ como a álgebra associativa livre com unidade, isto é, assumiremos $K \subset K\langle X\rangle$. Começaremos com a definição de polinômio próprio:

Definição 3.3.1. Um polinômio $f \in K\langle X\rangle$ é denominado próprio se for combinação linear de produto de comutadores, isto é, se podemos escrever f na forma

$$f(x_1,\cdots,x_m) = \sum_i \alpha_i [x_{i_{11}},\cdots,x_{i_{1p_1}}]\cdots[x_{i_{m_{k_i}1}},\cdots,x_{i_{m_{k_i}p_{k_i}}}]$$

assumimos que 1 é o produto de um conjunto vazio de comutadores. Denotamos por B o espaço dos polinômios próprios de $K\langle X\rangle$; para cada $m \in \mathbb{N}$, denotam-se por $B_m = B \cap K\langle x_1,\cdots,x_m\rangle$, $B_m^{(n)}$ os polinômios próprios em m variáveis e homogêneos de grau n, e denota-se por $\Gamma_n = B \cap P_n, n \in \mathbb{N}$, o conjunto dos polinômios multilineares próprios.

O próximo resultado exibirá uma base para o espaço B, baseado numa base da álgebra de Lie livre $L(X)$:

Proposição 3.3.2. *Considere uma base ordenada da álgebra de Lie livre L(X) (c.f. seção §2.9):*

$$x_1, x_2, x_3, \cdots, [x_{i_1}, x_{i_2}], [x_{j_1}, x_{j_2}], \cdots, [x_{k_1}, x_{k_2}, x_{k_3}], \cdots$$

Então, o espaço vetorial $K\langle X\rangle$ admite como base

$$x_1^{a_1} \cdots x_m^{a_m} w_1^{b_1} \cdots w_l^{b_l}$$

com $m, l \in \mathbb{N}$, $a_1, \cdots, a_m, b_1, \cdots, b_l \geq 0$, $w_1, \cdots, w_l$ comutadores básicos com $w_1 < \cdots < w_l$. Os elementos da base que satisfazem (segundo a notação acima) $m = 0$ (ou seja, $a_1 = \cdots = a_m = 0$), constituem uma base para o espaço vetorial B.

Demonstração. A afirmação sobre a base de $K\langle X\rangle$ segue direto do Teorema de Poincaré-Birkhoff-Witt, uma vez que a álgebra universal envelopante de $L(X)$ é $K\langle X\rangle$.

Para a segunda afirmação, os elementos definidos no enunciado realmente são elementos do espaço B, e são linearmente independentes, uma vez que é um subconjunto de um conjunto linearmente independente. Dados $w_1 \cdots w_l \in B$, com $w_1, \cdots, w_l$ polinômios de Lie, podemos "organizar" a ordem e a forma do produto da seguinte forma:

1. Podemos supor que $w_1, \cdots, w_l$ são comutadores básicos. De fato, se não forem, basta escrevermos como combinação linear de comutadores básicos, e obteremos uma combinação linear de produto de comutadores básicos. Então, basta verificar cada componente dessa combinação linear.

2. Podemos tornar o produto de forma que $w_1 \leq \cdots \leq w_l$. De fato, se $w_i > w_{i+1}$, então, podemos inverter o produto da seguinte forma: $w_i w_{i+1} = w_{i+1} w_i - [w_i, w_{i+1}]$. Daí, obtemos soma de dois produtos de comutadores, em que o primeiro é o nosso polinômio original, com dois fatores trocados de ordem, e o segundo é um novo produto de comutadores - e podemos escrever como combinação linear de comutadores básicos.

Aplicando indução, com essas ideias em mente, prova-se o resultado. □

Uma consequência desse fato é a seguinte importantíssima afirmação:

Corolário 3.3.3. *Um polinômio $f(x_1, \cdots, x_m) \in K\langle X\rangle$ é próprio se e só se a avaliação $f|_{x_i=1} = 0$, para todo $i = 1, \cdots, m$, em que $f|_{x_i=1}$ é o polinômio obtido substituindo a variável x_i por 1.*

Um dos importantíssimos fatos envolvendo polinômios próprios é que eles formam uma base para as identidades de uma álgebra:

Teorema 3.3.4. *Seja A uma PI-álgebra com unidade 1 sobre um corpo infinito K. Então, todas as identidades de A seguem das identidades polinomiais próprias. Ainda, se $\operatorname{car} K = 0$, as identidades polinomiais de A seguem das identidades polinomiais próprias multilineares.*

Demonstração. Seja $f(x_1, \cdots, x_m) \in K\langle X\rangle$ uma identidade polinomial de A, assuma f multi-homogêneo e escreva

$$f = \sum_{a=(a_1,\cdots,a_m)} \alpha_a x_1^{a_1} \cdots x_m^{a_m} w_a(x_1, \cdots, x_m), \quad \alpha_a \in K$$

decomposição de f segundo a base de $K\langle X\rangle$ apresentada no teorema 3.3.2, com w_a próprio, e com o somatório indexado pelas sequências $a = (a_1, \cdots, a_m)$ adequadas.

Pelo corolário 3.3.3, substituir qualquer variável de w_a por 1, obteremos 0 (desde que a variável efetivamente apareçe em w_a). Temos que $f(1+x_1, x_2, \cdots, x_m)$ é identidade de A (e equivalente a f), e ainda

$$f(1+x_1, x_2, \cdots, x_m) = \sum_{a=(a_1,\cdots,a_m)} \alpha_a \sum_{i=0}^{a_1} \left(\begin{array}{c} a_1 \\ i \end{array} \right) x_1^i x_2^{a_2} \cdots x_m^{a_m} w_a(x_1, \cdots, x_m).$$

A componente homogênea em x_1 de grau minimal de $f(1+x_1, x_2, \cdots, x_m)$ é obtida entre os somandos com a_1 maximal (que é equivalente a tomar os somandos com grau $_{x_1} w_a$ minimal, pois f é multi-homogêneo). Seja a_0 esse inteiro maximal. Então, uma vez que a componente homogênea de uma identidade é consequência da própria identidade (teorema 2.10.2), segue que

$$w_1 := \sum_{\substack{a=(a_1,\cdots,a_m) \\ \text{com } a_1 = a_0}} \alpha_a x_2^{a_2} \cdots x_m^{a_m} w_a(x_1, \cdots, x_m)$$

é identidade de A. Repetindo esse mesmo argumento para $f - x^{a_0} w_1$, e seguindo por indução o mesmo argumento, obteremos que f é consequência de um conjunto de polinômios da forma

$$\sum \alpha_a x_2^{a_2} \cdots x_m^{a_m} w_a(x_1, \cdots, x_m).$$

Aplicando o mesmo argumento para as demais variáveis, obteremos que f é equivalente a um conjunto de polinômios da forma

$$\sum w_a(x_1, \cdots, x_m).$$

Isso prova que f é equivalente a um conjunto de polinômios próprios. Para a parte multilinear, podemos repetir o processo, e utilizar a linearização total, e concluir que f é equivalente a um polinômio próprio multilinear. □

O espaço Γ_n admite naturalmente uma estrutura de S_n-módulo, definida da mesma forma para os polinômios multilineares. Uma das vantagens de se trabalhar com polinômios próprios é que muitas manipulações com os elementos resultam em conclusões mais fortes, porém, não é fácil exibir explicitamente o espaço Γ_n como soma de S_n-módulos irredutíveis. Na seção seguinte, exibiremos dois resultados importantíssimos para a estrutura das identidades de $M_2(K)$ - utilizando a teoria de polinômios próprios, representações de S_n e matrizes genéricas.

Finalizaremos a seção exibindo uma base para Γ_n, e para isso, precisaremos encontrar uma base para PL_n (o espaço dos polinômios multilineares de Lie):

Lema 3.3.5. *Seja PL_n o espaço dos polinômios de Lie multilineares de grau n. Então PL_n admite como base o conjunto*

$$\{[x_n, x_{\sigma(1)}, \cdots, x_{\sigma(n-1)}] : \sigma \in S_{n-1}\}.$$

Demonstração. Seja w um monômio em PL_n. Provaremos por indução em n, com a validade trivial do caso $n = 2$. Então, se $w = [u', v']$, utilizando a anticomutatividade se necessário, podemos assumir que a variável x_n aparece em u' e utilizando a hipótese de indução sobre u', podemos escrever

$$w = \sum_i [x_n, x_{i_1}, \cdots, x_{i_k}, v_i].$$

Fixe $w' = [x_n, x_{i_1}, \cdots, x_{i_k}, v]$, e basta mostrar que w' é combinação linear dos elementos citados no lema. Se grau $v = 1$, então w' já está na forma requerida. Caso contrário, escreva $v = [z_1, z_2]$, e daí, utilizando a identidade de Jacobi, obtemos:

$$w' = [x_n, x_{i_1}, \cdots, x_{i_k}, [z_1, z_2]] = [x_n, x_{i_1}, \cdots, x_{i_k}, z_1, z_2] - [x_n, x_{i_1}, \cdots, x_{i_k}, z_2, z_1]$$

e obtemos dois comutadores com grau $(z_i) <$ grau $(v), i = 1, 2$, o que implica que podemos utilizar argumentos indutivos e concluir que w é combinação linear dos elementos citados no teorema.

Para mostrar que os dados elementos são linearmente independentes, note o seguinte: dado $\sigma \in S_{n-1}$ e representando $[x_n, x_{\sigma(1)}, \cdots, x_{\sigma(n-1)}]$ como combinação linear de polinômios em P_n, podemos escrever como:

$$[x_n, x_{\sigma(1)}, \cdots, x_{\sigma(n-1)}] = x_n x_{\sigma(1)} \cdots x_{\sigma(n-1)} + \sum_{\substack{\tau \in S_n \\ \tau \neq \sigma}} \alpha_\tau x_{\tau(1)} \cdots x_{\tau(n)}, \quad \alpha_\tau \in \{-1, 0, 1\}$$

Uma observação importantíssima é que entre os elementos $x_{\tau(1)} \cdots x_{\tau(n)}$, com $\alpha_\tau \neq 0$, a variável x_n não aparece como primeiro elemento do monômio.

Assim, uma combinação linear dando zero dos elementos candidatos à base resulta em:

$$0 = \sum_{\sigma \in S_{n-1}} \beta_\sigma [x_n, x_{\sigma(1)}, \cdots, x_{\sigma(n-1)}] = \underbrace{\sum_{\sigma \in S_{n-1}} \beta_\sigma x_n x_{\sigma(1)} \cdots x_{\sigma(n-1)}}_{x_n \left(\sum_{\sigma \in S_{n-1}} \beta_\sigma x_{\sigma(1)} \cdots x_{\sigma(n-1)} \right)} + \underbrace{\sum_{\tau \in S_n} \beta'_\tau x_{\tau(1)} \cdots x_{\tau(n)}}_{x_n \text{ não aparece na primeira posição}}$$

assim, utilizando as bases de P_n e P_{n-1}, vemos necessariamente que todo $\beta_\sigma = 0$, o que implica a validade do lema. □

Como consequência, podemos calcular uma base para Γ_n:

Teorema 3.3.6. *Uma base para Γ_n é formada pelos seguintes elementos:*

$$[x_{i_{1_1}}, \cdots, x_{i_{1_{m_1}}}] \cdots [x_{i_{l_1}}, \cdots, x_{i_{l_{m_l}}}]$$

em que:

1. *todos os produtos são multilineares em $x_1, \cdots, x_n$;*
2. *cada comutador tem tamanho maior ou igual a 2 e o maior índice de cada comutador está na primeira posição, isto é, $i_{j_1} > i_{j_2}, \cdots, i_{j_{m_j}}$, para $j = 1, \cdots, l$;*
3. *o produto está na ordem de tamanho de comutador, isto é, $m_1 \leq m_2 \leq \cdots \leq m_l$;*
4. *se dois comutadores seguidos possuem o mesmo tamanho, então a primeira variável do primeiro comutador é menor do que a primeira variável do segundo comutador, isto é, se ocorre $m_j = m_{j+1}$, para algum j, então $i_{j_1} < i_{j+1_1}$.*

Demonstração. Na proposição 3.3.2, considere uma base de $L(X)$ tal que os comutadores de tamanho menor precedem os comutadores de tamanho maior, e se dois comutadores seguidos possuem o mesmo tamanho, então o primeiro símbolo do primeiro comutador é menor do que o primeiro símbolo do segundo comutador. A demonstração desse teorema segue direto do teorema 3.3.2 com essa base e do lema 3.3.5. □

§3.4 Matrizes Genéricas

Nesta seção, desenvolveremos uma teoria que será muito importante para simplificação de contas: matrizes genéricas. Toda a teoria aqui será baseada no livro de Drensky [9].

Fixaremos um corpo K infinito e $n \in \mathbb{N}$. Denote o anel de polinômios (comutativos) em infinitas variáveis por

$$\Omega_n = K[x_{pq}^{(l)} : p, q \in \{1, \cdots, n\}, l = 1, 2, \cdots].$$

Definição 3.4.1. As matrizes

$$y_i = \begin{pmatrix} x_{11}^{(i)} & \cdots & x_{1n}^{(i)} \\ \vdots & & \vdots \\ x_{n1}^{(i)} & \cdots & x_{nn}^{(i)} \end{pmatrix}$$

são denominadas de **matrizes genéricas** $n \times n$. Denotaremos por R_n a álgebra gerada pelas matrizes genéricas, e denominaremos de **álgebra de matrizes genéricas** $n \times n$. Denotaremos por R_{nm} a subálgebra de R_n gerada pelas matrizes genéricas $y_1, \cdots, y_m$.

Exemplo: *Se C é uma K-álgebra comutativa, para cada conjunto de elementos $c_1, \cdots, c_l \in M_n(C)$, existe uma especialização (substituição de variáveis) $\psi : \Omega_n \to C$ tal que a especialização induzida $\psi_n : R_n \to M_n(C)$ satisfaz $\psi_n(y_i) = c_i, i = 1, \cdots, l$.* □

Lema 3.4.2. *Sejam H corpo contendo K e $f(x_1, \cdots, x_m) \in K\langle X\rangle$. Então, f é identidade de $M_n(H)$ se e só se $f(y_1, \cdots, y_m) = 0$, sendo $y_1, \cdots, y_m$ matrizes genéricas $n \times n$.*

Demonstração. Assuma $f(y_1, \cdots, y_m) = 0$. Dados $h_1, \cdots, h_m \in M_n(H)$, considere $\psi_n : R_n \to M_n(H)$ tal que $\psi_n(y_i) = h_i, i = 1, \cdots, m$. Então, sendo ψ_n homomorfismo de álgebras, segue que

$$f(h_1, \cdots, h_m) = f(\psi_n(y_1), \cdots, \psi_n(y_m)) = \psi_n(f(y_1, \cdots, y_m)) = 0$$

e daí f é identidade de $M_n(H)$.

Reciprocamente, assuma $y = f(y_1, \cdots, y_m) \neq 0$. Como H infinito (pois K é infinito), existe $\psi : \Omega_n \to H$ especialização tal que a induzida $\psi_n : R_n \to M_n(H)$ satisfaz $\psi_n(y) \neq 0$, e segue que, f não é identidade de $M_n(H)$, pois $f(\psi_n(y_1), \cdots, \psi_n(y_m)) = \psi_n(y) \neq 0$. □

Esse último lema é inocente, pois a única coisa que ele diz é que podemos trabalhar com matrizes, utilizando variáveis em suas entradas, para verificar se uma dada identidade é satisfeita por uma álgebra de matrizes.

Exemplo: *Verificaremos que o polinômio $f = [[x_1, x_2]^2, x_3]$ é uma identidade de $M_2(K)$ diretamente: considere as matrizes*

$$\xi = \begin{pmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{pmatrix}, \quad \eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix}, \quad \zeta = \begin{pmatrix} \zeta_{11} & \zeta_{12} \\ \zeta_{21} & \zeta_{22} \end{pmatrix}$$

então

$$\begin{aligned} [\xi, \eta] &= \begin{pmatrix} \xi_{12}\eta_{21} - \xi_{21}\eta_{12} & \xi_{11}\eta_{12} + \xi_{12}\eta_{22} - \eta_{11}\xi_{12} - \eta_{12}\xi_{22} \\ \eta_{11}\xi_{21} + \eta_{21}\xi_{22} - \xi_{11}\eta_{21} - \xi_{21}\eta_{22} & \eta_{12}\xi_{21} - \xi_{12}\eta_{21} \end{pmatrix} \\ [\xi, \eta]^2 &= -\det[\xi, \eta] \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ [[\xi, \eta]^2, \zeta] &= 0 \end{aligned}$$

(em que $\det[\xi,\eta] = -(\xi_{12}\eta_{21} - \xi_{21}\eta_{12})^2 - (\xi_{11}\eta_{12} + \xi_{12}\eta_{22} - \eta_{11}\xi_{12} - \eta_{12}\xi_{22})(\eta_{11}\xi_{21} + \eta_{21}\xi_{22} - \xi_{11}\eta_{21} - \xi_{21}\eta_{22})$*). Conclusão:* f *é identidade de* $M_2(K)$ *e parece não valer a pena realizar as contas diretamente.* □

Os próximos resultados serão úteis e mostrarão como podemos simplificar contas com esta teoria.

Lema 3.4.3. *Os autovalores da matriz genérica* y_1 *são dois a dois distintos.*

Demonstração. Seja $f(\lambda) \in \Omega_n[\lambda]$ o polinômio característico da matriz y_1. Para qualquer especialização $\psi : \Omega_n \to K$, e considerando a induzida $\psi_n : R_n \to M_n(K)$, o polinômio característico de $\psi_n(y_1)$ é $\psi(f)$, em que $\psi(f)$ é o polinômio obtido de f aplicando ψ em seus coeficientes.

Daí, se y_1 admitir autovalores repetidos, f admitirá raízes repetidas, e então, $\psi(f)$ admitirá raízes repetidas, para toda especialização $\psi : \Omega_n \to K$. Em particular, todos os elementos de $M_n(K)$ admitirão autovalores repetidos, o que não é verdade, uma vez que K é infinito. □

Lema 3.4.4. *Seja* Ω'_n *um fecho algébrico do corpo de frações de* Ω_n*. Então, existe* $\mu \in M_n(\Omega'_n)$ *invertível tal que*

$$\mu^{-1}y_1\mu = \begin{pmatrix} z_1 & & 0 \\ & \ddots & \\ 0 & & z_n \end{pmatrix}, \quad \mu^{-1}y_2\mu = \begin{pmatrix} z'_1 & z'_2 & \cdots & z'_n \\ z'_2 & z_{22} & \cdots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z'_n & z_{n2} & \cdots & z_{nn} \end{pmatrix}$$

com z_i, z'_j, z_{pq} *variáveis comutativas, e as entradas de* $\mu^{-1}y_i\mu, i \geq 3$*, são não nulas e algebricamente independentes sobre* K*.*

Demonstração. Pelo lema 3.4.3, existe $\rho \in M_n(\Omega'_n)$ invertível tal que $\rho^{-1}y_1\rho$ é diagonal. Considere uma matriz

$$\lambda = \begin{pmatrix} 1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix} \in M_n(\Omega'_n)$$

e denote por $(x''_{ij}) = \rho^{-1}y_2\rho$. Temos $\lambda^{-1}\rho^{-1}y_1\rho\lambda$ ainda diagonal e denotando $(z_{ij}) = \lambda^{-1}\rho^{-1}y_2\rho\lambda$, temos $z_{1p} = z_{p1}$ se e só se $\lambda_p x''_{1p} = \lambda_p^{-1}x''_{p1}$. Note que, como as entradas de ρ estão num fecho algébrico do corpo $K(x_{ij}^{(1)} : 1 \leq i,j \leq n)$ e $\{x_{ij}^{(2)} : 1 \leq i,j \leq n\}$ é algebricamente independente sobre esse subcorpo, segue que as entradas de $\rho^{-1}x_2\rho$ são não nulos, e em particular, $x''_{1p} \neq 0$. Daí, tomando $\lambda_p = \sqrt{x''_{p1}/x''_{1p}}, p = 2, \cdots, n$, e tomando $\mu = \lambda\rho$, o resultado segue.

Por mesmo argumento no caso de $\rho^{-1}y_2\rho$, segue que as entradas de $\mu^{-1}y_i\mu, i \geq 3$, são não nulos e algebricamente independentes sobre K. □

Teorema 3.4.5. *Sejam* $f(x_1, \cdots, x_m) \in K\langle X\rangle$ *e*

$$y'_1 = \begin{pmatrix} z_1 & & 0 \\ & \ddots & \\ 0 & & z_n \end{pmatrix}, \quad y'_2 = \begin{pmatrix} z'_1 & z'_2 & \cdots & z'_n \\ z'_2 & z_{22} & \cdots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z'_n & z_{n2} & \cdots & z_{nn} \end{pmatrix}, \quad y'_i = \begin{pmatrix} z_{11}^{(i)} & \cdots & z_{1n}^{(i)} \\ \vdots & & \vdots \\ z_{n1}^{(i)} & \cdots & z_{nn}^{(i)} \end{pmatrix}, i \geq 3$$

com $z_i, z'_j, z_{pq}, z^{(l)}_{p'q'}$ variáveis comutativas. Então f é identidade de $M_n(K)$ se e somente se $f(y'_1, \cdots, y'_m) = 0$.

Em particular, se todas as variáveis de f aparecem somente em comutadores (isto é, f é um polinômio próprio, definição 3.3.1), então podemos assumir que valem as relações entre as variáveis $tr(y'_i) = 0, i \geq 1$, ou equivalentemente, f é identidade se e só se

$$f\left(y'_1 - \frac{1}{n}tr(y'_1)I, \cdots, y'_m - \frac{1}{n}tr(y'_m)I\right) = 0$$

Demonstração. Pelo lema 3.4.2, basta mostrar que $f(y'_1, \cdots, y'_m) = 0$ se e só se $f(y_1, \cdots, y_m) = 0$, sendo $y_1, \cdots, y_m$ matrizes genéricas $n \times n$.

Pelo lema 3.4.4, existe matriz μ tal que $\mu^{-1}y_1\mu$ é diagonal, $\mu^{-1}y_2\mu$ está na forma requerida para y'_2 e $\mu^{-1}y_i\mu, i \geq 3$, possui entradas não nulas e algebricamente independentes sobre K. Em particular, denominando de R'_n a K-álgebra gerada por $y'_1, y'_2, y'_3, \cdots$, existe especialização $\mu^{-1}R_n\mu \to R'_n$ tal que $\mu^{-1}y_i\mu \mapsto y'_i, i \geq 1$, e em particular, essa especialização é um isomorfismo. Daí, temos isomorfismo de álgebras

$$R_n \to \mu^{-1}R_n\mu \to R'_n$$

tal que $y_i \mapsto y'_i, i \geq 1$.

Denomine de $\phi : R_n \to R'_n$ esse isomorfismo. Então

$$f(y'_1, \cdots, y'_m) = f(\phi(y_1), \cdots, \phi(y_m)) = \phi(f(y_1, \cdots, y_m))$$

portanto, $f(y'_1, \cdots, y'_m) = 0$ se e só se $f(y_1, \cdots, y_m) = 0$, e o resultado segue pelo lema 3.4.2.

Para a segunda parte do Teorema, denote por I a matriz identidade $n \times n$, e escreva $y'_i = y'_i - \frac{1}{n}\mathrm{tr}(y_i)I + \frac{1}{n}\mathrm{tr}(y_i)I, i \geq 1$. Como substituir qualquer variável de f por I (ou por um múltiplo de I) implica em zero, temos que

$$\begin{aligned} f(y'_1, \cdots, y'_m) &= f\left(\left(y'_1 - \frac{1}{n}\mathrm{tr}(y'_1)I\right) + \frac{1}{n}\mathrm{tr}(y'_1)I, \cdots, \left(y'_m - \frac{1}{n}\mathrm{tr}(y'_m)I\right) + \frac{1}{n}\mathrm{tr}(y'_m)I\right) \\ &= f\left(y'_1 - \frac{1}{n}\mathrm{tr}(y'_1)I, \cdots, y'_m - \frac{1}{n}\mathrm{tr}(y'_m)I\right) \end{aligned}$$

e claro que $\mathrm{tr}(y'_i - \frac{1}{n}\mathrm{tr}(y'_i)I) = 0, i \geq 1$. □

A primeira parte da demonstração desse teorema mostra exatamente a seguinte afirmação:

Proposição 3.4.6. *Utilizando a mesma notação do Teorema 3.4.5, seja R'_n a K-álgebra gerada por $y'_1, y'_2, y'_3, \cdots$. Então $R_n \simeq R'_n$ como K-álgebras.*

Com auxílio do Teorema 3.4.5, podemos simplificar as contas (sem contar que veremos aplicações dessa teoria na seção seguinte):

Exemplo: *Seja $f = [[x_1, x_2]^2, x_3]$. Para verificar que f é identidade de $M_2(K)$, pelo Teorema 3.4.5, basta substituir suas variáveis por*

$$\xi = \begin{pmatrix} \xi_{11} & 0 \\ 0 & -\xi_{11} \end{pmatrix}, \quad \eta = \begin{pmatrix} \eta_{11} & \eta_2 \\ \eta_2 & -\eta_{11} \end{pmatrix}, \quad \zeta = \begin{pmatrix} \zeta_{11} & \zeta_{12} \\ \zeta_{21} & -\zeta_{11} \end{pmatrix}$$

Temos

$$\begin{aligned} [\xi,\eta] &= \begin{pmatrix} 0 & 2\xi_{11}\eta_2 \\ -2\xi_{11}\eta_2 & 0 \end{pmatrix} \\ [\xi,\eta]^2 &= \begin{pmatrix} -4\xi_{11}^2\eta_2^2 & 0 \\ 0 & -4\xi_{11}^2\eta_2^2 \end{pmatrix} \\ [[\xi,\eta]^2,\zeta] &= 0 \end{aligned}$$

e então, f é identidade de $M_2(K)$. □

§3.5 Representações de $\mathrm{GL}_m(K)$

Nesta seção, exibiremos noções da teoria de representação de $\mathrm{GL}_m(K)$, e enunciaremos vários resultados nessa linha.

Definição 3.5.1. Seja $\phi : \mathrm{GL}_m(K) \to \mathrm{GL}_s(K)$ uma representação do grupo $\mathrm{GL}_m(K)$, para algum $s \in \mathbb{N}$. Denomina-se a representação ϕ de **polinomial** se cada entrada de $\phi(g)$ é um polinômio envolvendo as entradas de $g \in \mathrm{GL}_m(K)$. A representação polinomial ϕ é denominada **homogênea de grau** d se as entradas de $\phi(g)$ forem polinômios homogêneos de grau d nas entradas de $g \in \mathrm{GL}_m(K)$.

Um $\mathrm{GL}_m(K)$-módulo W é dito polinomial (homogêneo) se a correspondente representação for polinomial (homogênea).

Nesta seção, denotaremos por V_m o espaço vetorial formal gerado por $x_1, \cdots, x_m$ sobre o corpo K, $K\langle V_m\rangle := K\langle x_1, \cdots, x_m\rangle$, e por $(K\langle V_m\rangle)^{(n)}$ o subconjunto dos polinômios homogêneos de grau n em $K\langle V_m\rangle$. Trabalharemos identificando, sem maiores problemas, $K\langle V_m\rangle \subset K\langle X\rangle$.

Temos que $\mathrm{GL}_m(K) := \mathrm{GL}(V_m)$ age naturalmente no espaço $K\langle V_m\rangle$ pela seguinte ação: dados $x_{i_1}\cdots x_{i_l} \in K\langle V_m\rangle$ e $g \in \mathrm{GL}_m(K)$, define-se a ação pela esquerda por

$$g(x_{i_1}\cdots x_{i_l}) := (gx_{i_1})\cdots(gx_{i_l}).$$

Com essa ação, $K\langle V_m\rangle$ é um $\mathrm{GL}_m(K)$-módulo à esquerda.

O próximo resultado é fácil de ser demonstrado, e mostra que representações de $\mathrm{GL}_m(K)$ em $K\langle V_m\rangle$ se comportam bem para manipulações:

Teorema 3.5.2. *1. $(K\langle V_m\rangle)^{(n)}$, a componente homogênea de grau n, é um $GL_m(K)$-módulo e*

$$K\langle V_m\rangle = \bigoplus_{n\in\mathbb{N}} (K\langle V_m\rangle)^{(n)}.$$

2. Para cada T-ideal $T \subset K\langle X\rangle$, temos que $T \cap K\langle V_m\rangle$ e $T \cap (K\langle V_m\rangle)^{(n)}$ são $GL_m(K)$-submódulos de $K\langle V_m\rangle$.

3. Cada $GL_m(K)$-submódulo $W \subset K\langle V_m\rangle$ é soma direta das componentes homogêneas $W \cap (K\langle V_m\rangle)^{(n)}$.

O próximo resultado classifica os $\mathrm{GL}_m(K)$-módulos polinomiais homogêneos irredutíveis de grau n, e irá mostrar que $\mathrm{GL}_m(K)$-módulos irredutíveis e S_n-módulos irredutíveis estão relacionados de alguma forma:

Teorema 3.5.3. *1. Os $GL_m(K)$-módulos polinomiais homogêneos de grau $n \geq 0$ irredutíveis (a menos de isomorfismo) estão em correspondência 1-1 com as partições $\lambda = (n_1, \cdots, n_m) \vdash n$. Denota-se por $W_m(\lambda)$ o $GL_m(K)$-módulo irredutível relacionado a λ.*

2. Seja $\lambda = (n_1, \cdots, n_m)$ uma partição de n. O $GL_m(K)$-módulo $W_m(\lambda)$ é isomorfo a um submódulo de $(K\langle V_m\rangle)^{(n)}$. O $GL_m(K)$-módulo $(K\langle V_m\rangle)^{(n)}$ admite decomposição

$$(K\langle V_m\rangle)^{(n)} \simeq \sum d_\lambda W_m(\lambda)$$

em que d_λ é a dimensão do S_n-módulo irredutível $(KS_n)e(D_\lambda)$, e o somatório percorre todas as partições λ em não mais que m partes.

Convém introduzirmos uma ação pela direita de S_n sobre $(K\langle V_m\rangle)^{(n)}$, que será conveniente na notação do próximo teorema. Para cada $x_{i_1} \cdots x_{i_n} \in (K\langle V_m\rangle)^{(n)}$, e para cada $\sigma \in S_n$, defina

$$x_{i_1} \cdots x_{i_n}\sigma := x_{i_{\sigma^{-1}(1)}} \cdots x_{i_{\sigma^{-1}(n)}}.$$

Essa ação é diferente da ação definida anteriormente de S_n sobre P_n, pois essa ação pela direita permuta a posição das variáveis. Essa ação, por exemplo, não leva identidades em identidades.

Para cada partição $\lambda = (n_1, \cdots, n_m)$, seja $q_1, \cdots, q_l$ o tamanho das colunas do diagrama λ. Defina o polinômio s_λ em $K\langle V_m\rangle$ por

$$s_\lambda(x_1, \cdots, x_{q_1}) = \prod_{j=1}^{l} s_{q_j}(x_1, \cdots, x_{q_j})$$

em que cada $s_{q_j}(x_1, \cdots, x_{q_j})$ é o polinômio standard. Isso resulta em uma caracterização mais precisa dos $\mathrm{GL}_m(K)$-módulos polinomiais homogêneos de grau n irredutíveis:

Teorema 3.5.4. *Seja $\lambda = (n_1, \cdots, n_m)$ uma partição de n em não mais que m partes e seja s_λ o elemento definido acima.*

1. *O elemento s_λ gera um $GL_m(K)$-módulo irredutível isomorfo a $W_m(\lambda)$.*
2. *Cada $GL_m(K)$-módulo irredutível $W \subset (K\langle V_m\rangle)^{(n)}$, com $W \simeq W_m(\lambda)$, é gerado por um elemento não nulo da forma*

$$w_\lambda(x_1, \cdots, x_{q_1}) = s_\lambda(x_1, \cdots, x_q)\left(\sum_{\sigma \in S_n} \alpha_\sigma \sigma\right), \quad \alpha_\sigma \in K.$$

*O elemento w_λ é denominado o **vetor de peso máximo** de W. Ele é único, a menos de constante multiplicativa, e está contido no espaço unidimensional dos elementos multi-homogêneos de multigrau $(n_1, \cdots, n_m)$ em W.*

3. *Se os $GL_m(K)$-submódulos W' e W'' de $(K\langle V_m\rangle)^{(n)}$ são isomorfos a $W_m(\lambda)$, com w' e w'' os vetores de peso máximo, respectivamente, então cada aplicação $\phi_\alpha : w' \to \alpha w''$, para cada $\alpha \in K, \alpha \neq 0$, pode ser estendido unicamente a um isomorfismo de $GL_m(K)$-módulos. Cada isomorfismo $W' \simeq W''$ é obtido desta maneira.*

O próximo resultado é um resultado muito parecido com um existente entre S_n-módulos (que relacionam identidades que são consequências de outras), e, além de ser importante por si só, é importante na demonstração do importantíssimo teorema seguinte.

Teorema 3.5.5. *Sejam f_1 e f_2 polinômios homogêneos de grau n em $K\langle V_m\rangle$. Então f_2 é consequência de f_1 se e só se $f_2 \in (GL_m(K))f_1$.*

Como consequência, temos o seguinte corolário:

Corolário 3.5.6. *Dado $W_m(\lambda)$ um $GL_m(K)$-submódulo irredutível e $f(x_1, \cdots, x_m) \in W_m(\lambda)$, então a linearização total $lin(f) \in W_m(\lambda)$.*

Demonstração. De fato, a linearização total $\mathrm{lin}(f)$ é consequência de f (estamos assumindo car $K = 0$), e então, pelo último teorema, $\mathrm{lin}(f) \in \mathrm{GL}_m(K)f \subset W_m(\lambda)$. □

O próximo resultado é importantíssimo e caracteriza S_n-módulos irredutíveis por meio de $\mathrm{GL}_m(K)$-módulos polinomiais homogêneos irredutíveis de grau n:

Teorema 3.5.7. *Sejam $m \geq n$, $\lambda \vdash n$ e seja $W_m(\lambda) \subset K\langle V_m\rangle$. Então o conjunto $M := W_m(\lambda) \cap P_n$ de todos os polinômios multilineares nas primeiras n variáveis em $W_m(\lambda)$ é um S_n-submódulo de P_n isomorfo a $(KS_n)e(D_\lambda)$. Todo S_n-submódulo irredutível de P_n pode ser obtido desta maneira.*

Agora, iremos exibir alguns resultados sobre os polinômios próprios. Note que o espaço $B_m^{(n)}$, dos polinômios próprios homogêneos de grau n em m variáveis, é naturalmente um $\mathrm{GL}_m(K)$-submódulo de $K\langle V_m\rangle$. Ainda, vale o seguinte resultado:

Lema 3.5.8. *Sejam W_1 e W_2 dois $GL_m(K)$-módulos polinomiais. Então $W_1 \otimes W_2$ é também um $GL_m(K)$-módulo polinomial.*

O próximo teorema apresenta a decomposição do espaço B_m (e em particular, do espaço $B_m^{(n)}$). O mais interessante é que ela é obtida a partir do estudo de identidades das matrizes triangulares superiores:

Teorema 3.5.9. *O espaço B_m admite a seguinte decomposição como $GL_m(K)$-módulo:*

$$B_m = \sum_{r\geq 0} \sum_{\substack{p_i \geq 2 \\ i=1,\cdots,r}} W_m(p_1 - 1, 1) \otimes \cdots \otimes W_m(p_r - 1, 1).$$

Existe a Regra de Littlewood-Richardson para complementar essa teoria, que descreve a estrutura do produto tensorial $W_m(\lambda) \otimes W_m(\mu)$. Um caso particular é a Regra de Young:

Teorema 3.5.10 (Regra de Young)**.** *Seja $\lambda = (n_1, \cdots, n_m)$ uma partição de n e $q \geq 0$. Então*

$$W_m(\lambda) \otimes W_m(\underbrace{1, 1, \cdots, 1}_{q \text{ vezes}}) \simeq \sum W_m(n_1 + \epsilon_1, \cdots, n_m + \epsilon_m, \epsilon_{m+1}, \cdots, \epsilon_p)$$

em que o somatório é sobre todos os ϵ_i, com $\epsilon_i \in \{0, 1\}$, tais que $\epsilon_1 + \cdots + \epsilon_p = q$ e $n_i + \epsilon_i \leq n_{i-1} + \epsilon_{i-1}, i = 2, \cdots, p$ (em que assumimos $n_l = 0$, se $l > m$).

Exemplo: *Combinando os resultados do teorema 3.5.9 e a Regra de Young (teorema 3.5.10), podemos descobrir a decomposição de $B_m^{(n)}$ para $n = 0, 1, 2, 3, 4$ em $GL_m(K)$-módulos irredutíveis:*

$B_m^{(0)}$: Por convenção, $B_m^{(0)} = K$.

$B_m^{(1)}$ *: Não existem comutadores próprios de tamanho 1, logo,* $B_m^{(1)} = 0$.

$B_m^{(2)}$ *: Pelo teorema 3.5.9, temos* $B_m^{(2)} \simeq W_m(1,1)$.

$B_m^{(3)}$ *: Pelo mesmo teorema, temos* $B_m^{(3)} \simeq W_m(2,1)$

$B_m^{(4)}$ *: Segue, pelo mesmo teorema, que*

$$B_m^{(4)} \simeq W_m(3,1) \oplus W_m(1,1) \otimes W_m(1,1)$$

e pela regra de Young, temos

$$W_m(1,1) \otimes W_m(1,1) \simeq W_m(2,2) \oplus W_m(2,1,1) \oplus W_m(1,1,1,1)$$

e então, $B_m^{(4)} \simeq W_m(3,1) \oplus W_m(2,2) \oplus W_m(2,1,1) \oplus W_m(1,1,1,1)$.

□

Com muitos cálculos, e utilizando toda essa teoria, podemos provar os seguintes resultados (relembrando da convenção de que $a \circ b := ab + ba$, para a e b elementos de qualquer álgebra associativa):

Proposição 3.5.11. *O* S_5*-módulo* PL_5 *pode ser decomposto como a soma direta de submódulos irredutíveis gerados pelas linearizações*

$$\begin{aligned}
y_1 &= [x_2, x_1, x_1, x_1, x_1] \\
y_2 &= [x_2, x_1, x_1, [x_2, x_1]] \\
y_3 &= \sum (-1)^\sigma [x_{\sigma(1)}, x_1, x_1, [x_{\sigma(2)}, x_{\sigma(3)}]] \\
y_4 &= \sum (-1)^\sigma [x_2, x_1, x_{\sigma(1)}, [x_{\sigma(2)}, x_{\sigma(3)}]] \\
y_5 &= \sum (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}, x_1, [x_{\sigma(3)}, x_{\sigma(4)}]]
\end{aligned}$$

O complemento de PL_5*, com respeito a* Γ_5*, é gerado pelas linearizações*

$$\begin{aligned}
y_6 &= [x_2, x_1, x_1] \circ [x_2, x_1] \\
y_7 &= \sum (-1)^\sigma [x_{\sigma(1)}, x_1, x_1] \circ [x_{\sigma(2)}, x_{\sigma(3)}] \\
y_8 &= \sum (-1)^\sigma [x_2, x_1, x_{\sigma(1)}] \circ [x_{\sigma(2)}, x_{\sigma(3)}] \\
y_9 &= \sum (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}, x_1] \circ [x_{\sigma(3)}, x_{\sigma(4)}]
\end{aligned}$$

As partições correspondentes aos polinômios y_1*,* y_2 *e* y_6*,* y_3 *e* y_7*,* y_4 *e* y_8*,* y_5 *e* y_9*, são* $(4,1)$*,* $(3,2)$*,* $(3,1,1)$*,* $(2,2,1)$*,* $(2,1,1,1)$*, respectivamente.*

Ainda, temos que

$$N = \sum_{i=6}^{9} (KS_5) lin\, y_i = (KS_5)[x_1, x_2, x_3] \circ [x_4, x_5].$$

Demonstração. Iremos decompor $B_m^{(5)}$ como soma de $\mathrm{GL}_m(K)$-submódulos irredutíveis, com auxílio do teorema 3.5.9 e da Regra de Young 3.5.10, e então, como $\Gamma_5 = P_5 \cap B_m^{(5)}$, seguirá que Γ_5 será a soma dos S_n-módulos irredutíveis gerados pelas linearizações dos vetores de peso máximo w_λ, para cada $W_m(\lambda) \subset B_m^{(5)}$ (corolário 3.5.6, e a conclusão é consequência do teorema 3.5.7).

Segundo o teorema 3.5.9, temos

$$B_m^{(5)} \simeq W_m(4,1) \oplus W_m(2,1) \otimes W_m(1,1) \oplus W_m(1,1) \otimes W_m(2,1)$$

e pela regra de Young, temos

$$W_m(2,1) \otimes W_m(1,1) \simeq W_m(3,2) \oplus W_m(2,1,1) \oplus W_m(2,2,1) \oplus W_m(2,1,1,1) \simeq W_m(1,1) \otimes W_m(2,1)$$

e então, $B_m^{(5)} \simeq W_m(4,1) \oplus 2W_m(3,2) \oplus 2W_m(2,1,1) \oplus 2W_m(2,2,1) \oplus 2W_m(2,1,1,1)$.

Com a teoria desenvolvida (teorema 3.5.4), temos que cada y_i é um vetor de peso máximo, e é fácil e trabalhoso verificar que os vetores relacionados a mesma partição são não nulos e linearmente independentes (utilizamos como auxílio o teorema 3.3.6, que descreve uma base de $\Gamma_n, \forall n \in \mathbb{N}$). A maior dificuldade é ser o primeiro a encontrar os vetores de peso máximo, pois a verificação de que realmente são os vetores de peso máximo não é tão difícil, assumindo toda a teoria exposta e desenvolvida anteriormente.

Por fim, sejam

$$\begin{aligned} N &= \sum_{i=6}^{9} (KS_5)\mathrm{lin}\, y_i \\ N' &= (KS_5)[x_1, x_2, x_3] \circ [x_4, x_5]. \end{aligned}$$

Temos que cada polinômio $\mathrm{lin}(y_i) \in N'$, e então, $N \subset N'$. Utilizando a teoria de módulos completamente redutíveis, temos N'/N soma de alguns $(KS_n)\mathrm{lin}(y_i)$, com $i \in \{1, \cdots, 5\}$. Mas, N' não contém polinômios de Lie, e então, necessariamente $N'/N = 0$, e o resultado segue. □

De forma análoga, podemos calcular a decomposição de Γ_6 (nesse caso, precisaríamos da regra de Littlewood-Richardson):

Proposição 3.5.12. *O complemento de PL_6 com respeito a Γ_6 pode ser decomposto na soma direta $\oplus_{i=1}^{16} M_i$, em que $M_i = KS_6 lin(z_i)$, $i = 1, \cdots, 16$, e (as sequências indicam a correspondente*

partição):

$$
\begin{aligned}
(4,2)\quad & z_1 = [x_2,x_1][x_2,x_1,x_1,x_1]\\
& z_2 = [x_2,x_1,x_1]^2\\
(4,1,1)\quad & z_3 = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)}][x_{\sigma(3)},x_1,x_1,x_1]\\
(3,3)\quad & z_4 = [x_2,x_1]^3\\
(3,2,1)\quad & z_5 = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)}][x_2,x_1,x_1,x_{\sigma(3)}]\\
& z_6 = \sum(-1)^\sigma [x_{\sigma(1)},x_1][x_{\sigma(2)},x_{\sigma(3)},[x_2,x_1]] = 2[x_2,x_1][x_1,x_3,[x_2,x_1]]\\
& z_7 = \sum(-1)^\sigma [x_2,x_1,x_{\sigma(1)}][x_{\sigma(2)},x_{\sigma(3)},x_1]\\
(3,1,1,1)\quad & z_8 = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)}][x_{\sigma(3)},x_{\sigma(4)},x_1,x_1]\\
& z_9 = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)}][x_{\sigma(3)},x_1,[x_{\sigma(4)},x_1]]\\
& z_{10} = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)},x_1][x_{\sigma(3)},x_{\sigma(4)},x_1]\\
(2,2,2)\quad & z_{11} = \sum(-1)^\sigma(-1)^\pi [x_{\sigma(1)},x_{\sigma(2)}][x_{\pi(1)},x_{\pi(2)},[x_{\sigma(3)},x_{\pi(3)}]]\\
& z_{12} = \sum(-1)^\sigma(-1)^\pi [x_{\sigma(1)},x_{\sigma(2)},x_{\pi(1)}][x_{\pi(2)},x_{\pi(3)},x_{\sigma(3)}]\\
(2,2,1,1)\quad & z_{13} = [x_1,x_2]s_4(x_1,x_2,x_3,x_4)\\
& z_{14} = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)}][x_{\sigma(3)},x_{\sigma(4)},[x_2,x_1]]\\
(2,1,1,1,1)\quad & z_{15} = \sum(-1)^\sigma [x_{\sigma(1)},x_{\sigma(2)}][x_{\sigma(3)},x_{\sigma(4)},[x_{\sigma(5)},x_1]]\\
(1,1,1,1,1,1)\quad & z_{16} = s_6(x_1,x_2,x_3,x_4,x_5,x_6)
\end{aligned}
$$

Sejam $N_1 = M_4 + M_{13} + M_{16}$, $N_2 = M_1 + M_3 + M_5 + M_8$, $N_3 = M_6 + M_9 + M_{11} + M_{14} + M_{15}$ *e* $N_4 = M_2 + M_7 + M_{10} + M_{12}$. *Então, relativo a* PL_6, *temos*

$$
\begin{aligned}
N_1 + N_3 &= KS_6[x_1,x_2][x_3,x_4][x_5,x_6]\\
N_2 + N_3 &= KS_6[x_1,x_2][x_3,x_4,x_5,x_6]\\
N_3 &= KS_6[x_1,x_2][x_3,x_4,[x_5,x_6]]\\
N_4 &= KS_6[x_1,x_2,x_3][x_4,x_5,x_6]
\end{aligned}
$$

Por fim, exibiremos um resultado que pode ser encontrado no livro de Bahturin [5], muito importante na decomposição do espaço dos polinômios de Lie multilineares PL_n:

Teorema 3.5.13. *Cada* $GL_m(K)$*-submódulo irredutível* $W_m(\lambda)$ *de* $(K\langle V_m\rangle)^{(n)}$, *com* λ *diferente das partições* (n), $(1,\cdots,1)$, $(2,2)$, *e* $(2,2,2)$, *entra na decomposição em soma de* $GL_m(K)$*-submódulos irredutíveis do* $GL_m(K)$*-módulo* $L_n(X)$, *o espaço dos polinômios de Lie homogêneos de grau* n.

Combinando o teorema 3.5.7 e o corolário 3.5.6, e o fato de que $PL_n = L_n(X) \cap P_n$, segue que todo S_n-módulo irredutível (exceto às partições $(2,2)$, $(2,2,2)$, (n) e $(1,1,\cdots,1)$) participa na decomposição de PL_n como soma de S_n-submódulos irredutíveis.

§3.6 Identidades Multilineares de Matrizes e Aplicações de Representações S_n

Nesta seção, enunciarei alguns resultados cruciais na demonstração dos resultados principais desta dissertação, que serão aplicações diretas da teoria desenvolvida na seção 2.9. Esses resultados podem ser encontrados no livro de Bahturin [5] e no artigo e livro de Drensky [9, 10].

Recordemos notação e alguns fatos: denote por P_n o conjunto dos polinômios multilineares nas variáveis $x_1, \cdots, x_n$, PL_n os polinômios multilineares de Lie, Γ_n os polinômios próprios multilineares, e $P_n(A), PL_n(A), \Gamma_n(A)$ as identidades multilineares, multilineares de Lie, próprias multilineares, respectivamente, de uma PI-álgebra A.

Especificamente para o caso PL_n, conseguimos uma forma relativamente melhor dos S_n-módulos irredutíveis. Para cada diagrama de Young D_λ, considere o polinômio de Lie $f(D_\lambda) := e(D_\lambda)[x_1, x_2, \cdots, x_n]$. Um resultado importantíssimo na caracterização das identidades multilineares de Lie é o seguinte:

Teorema 3.6.1. *Seja K um corpo de característica zero. Então:*

(i) PL_n, como S_n-módulo, decompõe-se como soma direta de S_n-módulos irredutíveis da forma $KS_n f(D_\lambda)$;

(ii) qualquer conjunto de identidades multilineares de grau n é equivalente a um sistema de identidades da forma $f(D_\lambda) = 0$, para alguns diagramas D_λ;

(iii) se $\lambda \neq (2,2)$ (para $n = 4$) e $\lambda \neq (2,2,2)$ (para $n = 6$), para cada diagrama D_λ (exceto às partições $n = 1 + 1 + \cdots + 1$ e $n = n$), PL_n contém pelo menos um S_n-módulo irredutível isomorfo (como S_n-módulo) a $KS_n e(D_\lambda)$.

Demonstração. Podemos decompor $KS_n = \sum (KS_n)e(D_\lambda)$, e então, como $PL_n = (KS_n)[x_1, \cdots, x_n]$, segue que

$$PL_n = (KS_n)[x_1, \cdots, x_n] = \sum (KS_n)e(D_\lambda)[x_1, \cdots, x_n] = \sum (KS_n)f(D_\lambda)$$

e cada $(KS_n)f(D_\lambda)$ é nulo ou irredutível como S_n-módulo. Então, existe um subconjunto dessa soma que torna a soma direta. Isso prova (i) e (ii).

A afirmação (iii) segue direto do teorema 3.5.13 e 3.5.7 (detalhado no comentário após o enunciado do teorema 3.5.13). □

Utilizando esse teorema, podemos decompor PL_5 em S_5-módulos irredutíveis, de uma forma independente da apresentada na proposição 3.5.11:

Proposição 3.6.2. *A decomposição dos elementos multilineares de Lie de grau 5 PL_5 é dada por*

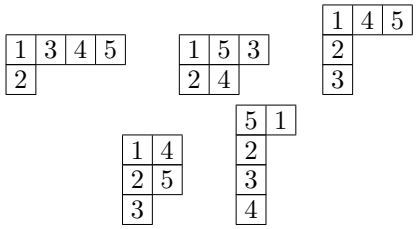
$$PL_5 = KS_5 f_1 \oplus KS_5 f_2 \oplus KS_5 f_3 \oplus KS_5 f_4 \oplus KS_5 f_5$$

em que

$$\begin{aligned} f_1 &= lin(x_2 ad(x_1)^4) \\ f_2 &= lin([x_2, x_1, x_1, [x_1, x_2]]) \\ f_3 &= lin([x_1 s_3(ad x_1, ad x_2, ad x_3), x_1]) \\ f_4 &= lin([x_1, x_2] s_3(ad x_1, ad x_2, ad x_3)) \\ f_5 &= lin(x_1 s_4(ad x_1, ad x_2, ad x_3, ad x_4)) \end{aligned}$$

em que as partições de 5 são $(4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$, respectivamente.

Demonstração. Considere todas as partições de 5, diferentes de (5) e $(1,1,1,1,1)$, e os seguintes preenchimentos formando os seguintes diagramas:



E temos os polinômios relativos a cada partição:

$$\begin{aligned}
f_1 &= \sum(-1)^{\sigma}[x_{\sigma(1)}, x_{\sigma(2)}, x_1, x_1, x_1] = 2[x_1, x_2, x_1, x_1, x_1] = -2x_2\mathrm{ad}(x_1)^4 \\
f_2 &= \sum(-1)^{\pi}(-1)^{\sigma}[x_{\sigma(1)}, x_{\sigma(2)}, x_1, x_{\pi(1)}, x_{\pi(2)}] = -2[x_2, x_1, x_1, [x_1, x_2]] \\
f_3 &= \sum(-1)^{\sigma}[x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_1, x_1] = -[x_1 s_3(\mathrm{ad}x_1, \mathrm{ad}x_2, \mathrm{ad}x_3), x_1] \\
f_4 &= \sum(-1)^{\sigma}(-1)^{\pi}[x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\pi(1)}, x_{\pi(2)}] \\
&= \sum(-1)^{\sigma}[x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\pi(1)}, [x_1, x_2]] = [x_1, x_2]s_3(\mathrm{ad}x_1, \mathrm{ad}x_2, \mathrm{ad}x_3) \\
f_5 &= \sum(-1)^{\sigma}[x_1, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}, x_{\sigma(1)}] = -x_1 s_4(\mathrm{ad}x_1, \mathrm{ad}x_2, \mathrm{ad}x_3, \mathrm{ad}x_4)
\end{aligned}$$

utilizando os comutadores básicos (seção §2.9), temos que todos esses polinômios são não nulos. Para concluir que essa é a decomposição de PL_5, podemos calcular a dimensão de cada S_5-módulo irredutível pela fórmula do gancho (enunciado sem demonstração a seguir), e ver que a soma delas resulta em $24 = 4! = \dim PL_5$. □

Teorema 3.6.3 (Fórmula do gancho)**.** *Seja $\lambda = (n_1, \cdots, n_m) \vdash n$ uma partição e considere a partição conjugada $\lambda' = (n'_1, \cdots, n'_l)$. Para cada coordenada (i,j) da tabela T_λ, defina o gancho (ou, do inglês, hook) em (i,j) por $h_{ij} := (n_i - j) + (n'_j - i) + 1$. Então*

$$dim\,(KS_n)e(D_\lambda) = \frac{n!}{\prod_{(i,j)} h_{ij}}$$

Da estrutura dos elementos de $M_2(K)$ e $\mathfrak{sl}(2,K)$, utilizando as técnicas de matrizes genéricas, temos que as identidades de $M_2(K)$ são equivalentes a identidades de no máximo três variáveis, ou seja, vale o seguinte resultado:

Proposição 3.6.4. *Os diagramas de Young correspondentes às componentes irredutíveis (como S_n-módulos) de $PL_n(\mathfrak{sl}(2,K))$ e $\Gamma_n(M_2(K))$ possuem no máximo 3 linhas.*

Demonstração. Considere $f \in \Gamma_n(M_2(K))$ (como $\Gamma_n(M_2(K)) \supset PL_n(M_2(K))$, isso inclui o caso dos polinômios de Lie), e considere um diagrama D_λ que contenha 4 linhas ou mais. Então, chamando de g o polinômio obtido identificando as variáveis na mesma linha de $e(D_\lambda)f$, obtemos que g possui pelo menos 4 variáveis. Concluiremos que g necessariamente será uma identidade polinomial de $M_2(K)$. Uma base de $M_2(K)$ é dada por $e_{11} - e_{12}, e_{12}, e_{21}, e_{11} + e_{22}$, e para verificar que g é identidade de $M_2(K)$, basta substituir as suas variáveis por esses elementos da base. Como g é um polinômio próprio, se qualquer variável for substituída por $e_{11} + e_{22}$, então g irá zerar. Como g é antissimétrico

em pelo menos 4 variáveis, ao substituir pelos elementos da base, ou teremos repetição de algum dos elementos e g irá zerar, ou um dos elementos que substituirmos será $e_{11}+e_{22}$. Segue que g é identidade, e então, os diagramas de Young de $\Gamma_n(M_2(K))$ possuem no máximo 3 linhas. □

Em particular, dado $f \in \Gamma_n$, e caso queiramos verificar que $e(D_\lambda)f$ é uma identidade de $M_2(K)$, basta considerarmos o polinômio g, obtido da identificação das variáveis na mesma linha do diagrama D_λ (são equivalentes, c.f. comentários no fim da seção §2.10), e substituirmos as variáveis de g por $\xi(e_{11}-e_{22}), \eta(e_{12}+e_{21}), \zeta(e_{12}-e_{21})$, e então, g será identidade se e só se g se anular nesses elementos; ou g é automaticamente identidade se tiver 4 ou mais variáveis. De fato, essa observação segue da argumentação feita na demonstração do teorema anterior e do teorema 3.4.5 (teoria de matrizes genéricas). Isso motiva a importância do próximo lema:

Lema 3.6.5. *Sejam $a_1 = e_{11}-e_{22}, a_2 = e_{12}+e_{21}, a_3 = e_{12}-e_{21} \in M_2(K)$. Considere um produtório $a_{i_1}\cdots a_{i_n}$, em que esse produtório é entre os elementos a_1, a_2, a_3, e o elemento a_i aparece n_i vezes, $i = 1,2,3$. Então, se $\epsilon_i \in \{0,1\}, i = 1,2,3$, com $n_i \equiv \epsilon_i (mod 2)$, vale*

$$a_{i_1}\cdots a_{i_n} = \pm a_1^{\epsilon_1} a_2^{\epsilon_2} a_3^{\epsilon_3}.$$

Demonstração. A demonstração do lema segue direto das seguintes relações, que podem facilmente ser verificadas:

$$a_1a_2 = -a_2a_1 = a_3, \quad a_2a_3 = -a_3a_2 = -a_1, \quad a_3a_1 = -a_1a_3 = -a_2,$$
$$a_1^2 = a_2^2 = e, \quad a_3^2 = -e$$

em que e é a matriz identidade 2×2. □

Corolário 3.6.6. *Se $f(x_1,x_2,x_3)$ é um polinômio multi-homogêneo de multigrau (n_1,n_2,n_3), então, se $\epsilon_i \in \{0,1\}, i = 1,2,3$, com $\epsilon_i \equiv n_i (mod 2)$, existe $\alpha \in K$ tal que*

$$f(e_{11}-e_{22}, e_{12}+e_{21}, e_{12}-e_{21}) = \alpha(e_{11}-e_{22})^{\epsilon_1}(e_{12}+e_{21})^{\epsilon_2}(e_{12}-e_{21})^{\epsilon_3}.$$

Isso refina o que foi comentado após a proposição 3.6.4, e vale registrar como corolário:

Corolário 3.6.7. *Seja $f \in \Gamma_n$, D_λ um diagrama relativo a uma partição λ e considere o polinômio g obtido de $e(D_\lambda)f$ identificando as variáveis na mesma linha do diagrama. Então, g é identidade de $M_2(K)$ se e só se ocorre de g ter 4 ou mais variáveis ou $g(e_{11}-e_{22}, e_{12}+e_{21}, e_{12}-e_{21}) = 0$.*

Como consequência, obtemos uma caracterização muito útil e muito forte de $PL_n(\mathfrak{sl}(2,K))$ e $\Gamma_n(M_2(K))$, que é a seguinte:

Teorema 3.6.8. *Para cada $n > 1$, os S_n-módulos $PL_n(\mathfrak{sl}(2,K))$ e $\Gamma_n(M_2(K))$ decompoem-se como soma de S_n-módulos irredutíveis não isomorfos correspondentes às partições $(p+q+r, p+q, p)$ de n, em que:*

(i) para $PL_n(\mathfrak{sl}(2,K))$, temos $p+q \neq 0$ e ocorre $q \equiv 1 (mod 2)$ ou $r \equiv 1 (mod 2)$,

(ii) para $\Gamma_n(M_2(K))$, temos $p+q \neq 0$, e se $q = r = 0$, então $p > 1$.

Demonstração. Para a primeira parte do teorema, basta mostrar que, dados um diagrama D_λ e $f_1, f_2 \in \Gamma_n(M_2(K))$ não nulos, de modo que $e(D_\lambda)f_1$ e $e(D_\lambda)f_2$ são não nulos, então $e(D_\lambda)f_1$ e $e(D_\lambda)f_2$ são equivalentes. Considere g_i o polinômio obtido de $e(D_\lambda)f_i$ identificando as variáveis da mesma linha do diagrama D_λ, $i = 1,2$. Note que g_1 e g_2 são multi-homogêneos de mesmo multigrau,

por construção. Então, sendo $a_1 = e_{11} - e_{22}, a_2 = e_{12} + e_{21}, a_3 = e_{12} - e_{21}$, temos $g_i(a_1, a_2, a_3) \neq 0, i = 1, 2$, e então, pelo corolário 3.6.6, temos $g_i(a_1, a_2, a_3) = \alpha_i e_0, i = 1, 2$, para algum $\alpha_1, \alpha_2 \in K$ e para algum $e_0 \in M_2(K)$. Daí, definindo o polinômio $h = \alpha_2 g_1 - \alpha_1 g_2$, temos que $h = 0$ é identidade polinomial de $M_2(K)$, pois, pelo corolário 3.6.7, $h(a_1, a_2, a_3) = 0$, e h ser identidade polinomial é o mesmo que dizer que $g_1 = \alpha_2^{-1}\alpha_1 g_2$ em $\Gamma_n(M_2(K))$, ou seja, g_1 é equivalente a g_2 em $\Gamma_n(M_2(K))$, o que implica que $e(D_\lambda)f_1$ e $e(D_\lambda)f_2$ são equivalentes em $M_2(K)$. Em particular, se $\Gamma_n(M_2(K))$ contém $(KS_n)e(D_\lambda)f$ e $(KS_n)e(D_\lambda)g$, com $(KS_n)e(D_\lambda)f \simeq (KS_n)e(D_\lambda)g$, então $f \in (KS_n)e(D_\lambda)g$ e $g \in (KS_n)e(D_\lambda)f$, o que implica $(KS_n)e(D_\lambda)f = (KS_n)e(D_\lambda)g$ (todas as igualdades e continências valem em $\Gamma_n(M_2(K))$). Isso prova que $\Gamma_n(M_2(K))$ (e $PL_n(\mathfrak{sl}(2, K))$) se decompõe como soma de S_n-módulos irredutíveis não isomorfos.

Agora, mostraremos que $PL_n(\mathfrak{sl}(2, K))$ não contém S_n-módulos irredutíveis correspondentes às partições não citadas no enunciado: seja $\lambda = (p + q + r, p + q, p)$, com $q \equiv r \equiv 0 (\mathrm{mod}\, 2)$, seja $f \in PL_n$, e considere g o polinômio obtido de $e(D_\lambda)f$ identificando as variáveis na mesma linha do diagrama D_λ. Então, pelo corolário 3.6.6, existe $\alpha \in K$ tal que

$$g(e_{11} - e_{22}, e_{12} + e_{21}, e_{12} - e_{21}) = \alpha(e_{11} - e_{22})^p(e_{12} + e_{21})^p(e_{12} - e_{21})^p = \alpha(-1)^p(e_{11} + e_{22})$$

como g é um polinômio de Lie, necessariamente $\mathrm{tr}(g(a, b, c)) = 0$, para quaisquer $a, b, c \in M_2(K)$ (basta escrever $g = [u, v]$, com u, v polinômios de Lie, e lembrar do fato de que um comutador de matrizes sempre tem traço zero). Então, é impossível obtermos $\alpha \neq 0$ na equação acima, o que implica que g e $e(D_\lambda)f$ são nulos em $PL_n(\mathfrak{sl}(2, K))$. E é claro que não existirá polinômio de Lie relativo à partição $(r, 0, 0)$, pois não existe polinômio de Lie não nulo em uma única variável.

Para a partição $\lambda = (1, 1, 1)$ de $\Gamma_3(M_2(K))$ (o único caso excluído de $\Gamma_n(M_2(K))$), temos que necessariamente, para todo $f \in P_3$, $e(D_\lambda)f = \alpha s_3(x_1, x_2, x_3)$, para algum $\alpha \in K$, e em particular, s_3 não é um comutador próprio, pois, $s_3(x_1, x_2, 1) = [x_1, x_2] \neq 0$ (c.f. corolário 3.3.3).

Por fim, basta mostrar que existe um S_n-módulo irredutível para cada uma das partições citadas.

1. Caso $r \equiv 1 (\mathrm{mod}\, 2)$. Se $q = 0$, defina

$$f_{p0r}(x_1, x_2, x_3) = \sum (-1)^\sigma x_{\sigma(1)} x_{\sigma(2)} (\mathrm{ad}\, x_1)^r (\mathrm{ad}\, x_{\sigma(3)}) s_3^{p-1}(\mathrm{ad}\, x_1, \mathrm{ad}\, x_2, \mathrm{ad}\, x_3)$$

se $q > 0$, defina

$$f_{pqr}(x_1, x_2, x_3) = [x_1, x_2](\mathrm{ad}\, x_1)^r (\mathrm{ad}([x_1, x_2]))^{q-1} s_3^p(\mathrm{ad}\, x_1, \mathrm{ad}\, x_2, \mathrm{ad}\, x_3).$$

2. Caso $r \equiv 0 (\mathrm{mod}\, 2)$ e $q \equiv 1 (\mathrm{mod}\, 2)$. Defina

$$f_{pqr}(x_1, x_2, x_3) = \\ \sum (-1)^\sigma [x_1, x_2](\mathrm{ad}\, x_1)^r (\mathrm{ad}\, x_{\sigma(1)})(\mathrm{ad}([x_1, x_2]))^{q-3} \mathrm{ad}([x_1, x_2, x_{\sigma(2)}]) s_3^p(\mathrm{ad}\, x_1, \mathrm{ad}\, x_2, \mathrm{ad}\, x_3).$$

3. Caso $q \equiv r \equiv 0 (\mathrm{mod}\, 2), n > 3$. Para $q = r = 0$ e $p > 1$, defina

$$f_{p00}(x_1, x_2, x_3) = \sum (-1)^\sigma x_{\sigma(1)} s_3^{p-1}(\mathrm{ad}\, x_1, \mathrm{ad}\, x_2, \mathrm{ad}\, x_3) x_{\sigma(2)} x_{\sigma(3)}$$

para $q = 0$ e $r > 0$, defina

$$f_{p0r}(x_1, x_2, x_3) = \sum (-1)^\sigma x_{\sigma(1)} (\mathrm{ad}\, x_1)^r s_3^{p-1}(\mathrm{ad}\, x_1, \mathrm{ad}\, x_2, \mathrm{ad}\, x_3) x_{\sigma(2)} x_{\sigma(3)}$$

e finalmente, para $q > 0$, defina

$$f_{pqr}(x_1, x_2, x_3) = f_{pq-1r}(x_1, x_2, x_3)[x_1, x_2].$$

Para verificar que esses polinômios são não nulos em $M_2(K)$, defina os elementos (podemos trabalhar em um fecho algébrico de K, e utilizar o teorema 2.10.6)

$$a = -\frac{e_{11} - e_{22}}{2}\sqrt{-1}, \quad b = \frac{e_{12} + e_{21}}{2}\sqrt{-1}, \quad c = \frac{e_{12} - e_{21}}{2}.$$

Note que valem as seguintes relações:

$$ab = -ba = \frac{c}{2}, \quad bc = -cb = \frac{a}{2}, \quad ca = -ca = \frac{b}{2}.$$

Ainda, se y_1, y_2, y_3 forem substituídos, sem repetir nenhum, por a, b ou c, temos que valem sempre:

$$\begin{aligned} [y_1, y_2] &= \pm y_3 \\ [y_1, y_2, y_2] &= -y_1 \\ ys_3(\operatorname{ad} y_1, \operatorname{ad} y_2, \operatorname{ad} y_3) &= -2y \end{aligned}$$

em que y é qualquer um dos a, b, c. Com isso, fica fácil verificar que os polinômios são não nulos, e ainda, que todos eles estão em PL_n ou Γ_n, adequadamente como no enunciado do teorema. Isso conclui a demonstração do resultado. □

§3.7 Identidades Fracas

Nesta seção, serão demonstrados alguns resultados específicos de identidades de matrizes, que serão úteis diretamente na demonstração dos resultados principais desta dissertação.

Daqui em diante fixe $K\langle X\rangle$ a álgebra associativa sem unidade livre gerada por $X = \{x_1, x_2, \cdots\}$ e $L(X)$ a álgebra de Lie livre gerada pelos mesmos elementos pelo comutador $[x, y] = xy - yx$. Utilizaremos o símbolo $\circ$ para denotar o produto simétrico, isto é, $x \circ y := xy + yx$, para x, y elementos de qualquer álgebra associativa.

Começaremos com uma definição que será muito útil para manipular identidades:

Definição 3.7.1. Sejam (A, L) um par, com A álgebra associativa, $L \subset A$ álgebra de Lie com respeito ao comutador $[x, y] = xy - yx$, e de tal forma que os elementos de L geram A (neste caso, dizemos que A é uma álgebra envelopante da álgebra de Lie L). Um polinômio $f(x_1, \cdots, x_n) \in K\langle X\rangle$ é dito **identidade fraca** do par (A, L) se $f(v_1, \cdots, v_n) = 0$ (produto em A), para todo $v_1, \cdots, v_n \in L$. No caso de $f(a_1, \cdots, a_n) = 0$, para todo $a_1, \cdots, a_n \in A$, diremos que f é uma **identidade forte** (ou ordinária) de A.

Definição 3.7.2. Sejam (A, L) como na definição 3.7.1. Um ideal $I \subset A$ é denominado **ideal verbal fraco** se, para todo endomorfismo $e : A \to A$, satisfazendo $e(L) \subset L$, tem-se $e(I) \subset I$. Dado $I \subset K\langle X\rangle$, definimos o ideal verbal fraco gerado por I como sendo o menor ideal verbal fraco de $K\langle X\rangle$ contendo I.

Diremos que uma identidade g é consequência de f se g está no ideal verbal fraco gerado por f. Se f é consequência de g e g é consequência de f, diremos que f e g são equivalentes.

Observação. As seguintes afirmações são simples, muito importantes e fáceis de serem provadas:

(i) Dados (A, L), como na definição 3.7.1, o conjunto I das identidades fracas do par (A, L) formam um ideal verbal fraco em $K\langle X\rangle$.

(ii) Seja $T = \{e : K\langle X\rangle \to A \text{ homomorfismo tal que } e(L(X)) \subset L \ (\iff e(x_i) \in L, \forall x_i \in X)\}$. - Então o ideal das identidades fracas de (A, L) é $\bigcap_{e\in T} \operatorname{Ker} e$.

(iii) Sejam $I \subset K\langle X\rangle$ um ideal verbal fraco, $A = K\langle X\rangle/I$ e $\varphi : K\langle X\rangle \to A$ a projeção canônica. Então $(\varphi(A), \varphi(L))$ é um par como na definição 3.7.1 e I é o conjunto das identidades fracas do par. Neste caso, denotando por $t_i = x_i + I \in A, i = 1, 2, \cdots$ e dado $f(x_1, \cdots, x_n) \in A$ tal que $f(t_1, \cdots, t_n) = 0$, temos que f é uma identidade fraca de (A, L). Essa importantíssima propriedade será utilizada posteriormente.

Definição 3.7.3. Sejam (A, L), com A álgebra associativa com conjunto de geradores $\{t_1, t_2, \cdots\}$ e L álgebra de Lie gerada pelo comutador pelos mesmos elementos. Dizemos que o par (A, L) é um **par livre** se para todo $f \in K\langle X\rangle$ tal que $f(t_1, \cdots, t_n) = 0$, resulta em f ser identidade fraca do par (A, L).

Note que o par $(M_2(K), \mathfrak{sl}(2, K))$ é tal que $M_2(K)$ é gerado (como álgebra associativa) pelos elementos de $\mathfrak{sl}(2, K)$.

Exemplo: *A identidade*

$$[x \circ y, z] = 0 \tag{1}$$

é uma identidade fraca do par $(M_2(K), \mathfrak{sl}(2, K))$. *De fato, essa identidade é a linearização de* $[x^2, z] = 0$, *que é uma identidade fraca, uma vez que uma matriz de traço zero ao quadrado é uma matriz escalar (o polinômio característico de uma matriz a de traço 0 será* $a^2 + \det(a)I = 0$, *donde* a^2 *será uma matriz escalar).* □

Veremos no capítulo seguinte que todas as identidades fracas do par $(M_2(K), \mathfrak{sl}(2, K))$ são consequências da identidade (1).

Para trabalharmos com pares (A, L) satisfazendo a identidade fraca (1), será importantíssimo o próximo resultado:

Proposição 3.7.4. *São consequências da identidade (1):*

$$[x, y, z] = 2(z \circ y)x - 2(z \circ x)y \tag{2}$$

$$(u \circ [y, x])z = (u \circ z)[y, x] + (z \circ y)[x, u] - (z \circ x)[y, u] \tag{3}$$

$$4(x \circ y)[z, u] = [y, u, x, z] + [x, u, y, z] - [y, z, u, x] - [x, z, u, y] \tag{4}$$

$$[x, y] \circ z = x \circ [y, z] \tag{5}$$

Demonstração. Note que, como $(x \circ y)$ comuta com todos os elementos $z \in L(X)$ módulo o ideal das identidades fracas geradas por 1 (pois $[x \circ y, z] = 0, \forall z \in L(X)$), podemos considerar $x \circ y$ como "escalares", comutando livremente com as demais variáveis.
Para (2), temos

$$[x, y, z] = xyz - yxz - zxy + zyx$$
$$2(z \circ y)x - 2(z \circ x)y = 2(zyx + yzx - zxy - xzy).$$

Tomando a diferença, obtemos

$$[x, y, z] - (2(z \circ y)x - 2(z \circ x)y) = xyz - yxz + zxy - zyx - 2(yzx - xzy) =$$
$$\underbrace{xzy + xyz}_{x(y\circ z)} \underbrace{-zyx - yzx}_{-(y\circ z)x} + \underbrace{zxy + xzy}_{(z\circ x)y} \underbrace{-yxz - yzx}_{-y(x\circ z)} = [x, y \circ z] + [z \circ x, y] = 0$$

e em particular, $[x,y,z] = 2(z\circ y)x - 2(z\circ x)y$.
Para (3), temos

$$[x,y,z,u] = [2(z\circ y)x - 2(z\circ x)y, u] = 2(z\circ y)[x,u] - 2(z\circ x)[y,u].$$

Por outro lado,

$$[[x,y],z,u] = [z,[y,x],u] = 2(u\circ [y,x])z - 2(u\circ z)[y,x]$$

e então, obtemos

$$(u\circ [y,x])z = (u\circ z)[y,x] + (z\circ y)[x,u] - (z\circ x)[y,u].$$

Para (4), temos

$$\begin{aligned}
[y,u,x,z] &= 2(x\circ u)[y,z] - 2(x\circ y)[u,z]\\
[x,u,y,z] &= 2(y\circ u)[x,z] - 2(y\circ x)[u,z]\\
-[y,z,u,x] &= -2(u\circ z)[y,x] + 2(u\circ y)[z,x]\\
-[x,z,u,y] &= -2(u\circ z)[x,y] + 2(u\circ x)[z,y]
\end{aligned}$$

somando os quatro termos, obtemos

$$4(x\circ y)[z,u] = [y,u,x,z] + [x,u,y,z] - [y,z,u,x] - [x,z,u,y].$$

Para (5), temos

$$\begin{aligned}
[x,y]\circ z &= xyz - yxz + zxy - zyx\\
x\circ [y,z] &= xyz - xzy + yzx - zyx
\end{aligned}$$

Formando a diferença, obtemos

$$[x,y]\circ z - x\circ [y,z] = -yxz + zxy + xzy - yzx = -y(x\circ z) + (x\circ z)y = [x\circ z, y] = 0$$

e $[x,y]\circ z = x\circ [y,z]$. □

Fixe $I \subset K\langle X\rangle$ um ideal verbal fraco, $\varphi : K\langle X\rangle \to K\langle X\rangle/I$ a projeção canônica, $A = K\langle X\rangle/I$ e $L = \varphi(L(X))$. Denote os elementos $\varphi(x_1), \varphi(x_2), \cdots$ por $x_1, x_2, \cdots \in A$, utilizando os mesmos símbolos.

Proposição 3.7.5. *Assuma que (1) é identidade fraca de um par (A, L). Então, cada elemento de A pode ser escrito como combinação linear dos seguintes tipos de elementos:*

$$\begin{aligned}
&\textit{tipo 1: } (x_{i_1}\circ x_{j_1})\cdots(x_{i_k}\circ x_{j_k});\quad (x_{i_1}\circ x_{j_1})\cdots(x_{i_k}\circ x_{j_k})([x_i,x_j]\circ x_t)\\
&\textit{tipo 2: } (x_{i_1}\circ x_{j_1})\cdots(x_{i_k}\circ x_{j_k})[x_i,x_j];\quad (x_{i_1}\circ x_{j_1})\cdots(x_{i_k}\circ x_{j_k})x_t
\end{aligned}$$

Demonstração. Note que, pelas identidades (5) e (2), temos

$$[u_1,u_2]\circ[u_3,u_4] = [u_1,u_2,u_3]\circ u_4 = 2(u_3\circ u_2)(u_1\circ u_4) - 2(u_3\circ u_1)(u_2\circ u_4) \tag{6}$$

(vale lembrar que $u\circ v$ são elementos centrais, para $u, v \in L$). Note também que, para quaisquer $a, b \in A$, vale $ab = \frac{1}{2}a\circ b + \frac{1}{2}[a,b]$ (essa igualdade vale em qualquer álgebra associativa).

Provaremos por indução em n que os elementos:

(i) $x_1 \cdots x_n$

(ii) $[x, y]x_1 \cdots x_n$

podem ser escritos como combinação linear dos elementos do tipo 1 e do tipo 2, para $n \in \mathbb{N}, x, y \in L$.

Se $n = 1$, então (i) já está na forma requerida, e note que

$$[x, y]x_1 = \frac{1}{2}[x, y] \circ x_1 + \frac{1}{2}[x, y, x_1]$$

em que o primeiro termo é do tipo 1 e, pela identidade (2), temos $[x, y, x_1] = 2(x_1 \circ y)x - 2(x_1 \circ x)y$, elemento do tipo 2, e isso prova (ii).

Então, fixe $n > 1$ e assuma, por hipótese de indução, que o resultado vale para todo $n' < n$. Dado um monômio $x_1 \cdots x_n$, utilizando o mesmo truque

$$x_1 \cdots x_n = \frac{1}{2}(x_1 \circ x_2)x_3 \cdots x_n + \frac{1}{2}[x_1, x_2]x_3 \cdots x_n,$$

segue por indução a validade da afirmação para (i). Para (ii), utilizando novamente o truque, temos

$$[x, y]x_1 \cdots x_n = \frac{1}{2}[x, y](x_1 \circ x_2)x_3 \cdots x_n + \frac{1}{2}[x, y][x_1, x_2]x_3 \cdots x_n$$

e o primeiro termo é combinação linear dos elementos do tipo 1 e 2 por indução (pois $\frac{1}{2}[x, y](x_1 \circ x_2)x_3 \cdots x_n = (x_1 \circ x_2)\frac{1}{2}[x, y]x_3 \cdots x_n$, e basta aplicar a hipótese de indução (ii) sobre $[x, y]x_3 \cdots x_n$, e vale, pois o produto pelo termo $(x_1 \circ x_2)$ manterá os elementos de cada tipo no mesmo tipo). Então, basta mostrar que $[x, y][x_1, x_2]x_3 \cdots x_n$ é combinação linear dos elementos do tipo 1 e tipo 2. Fazendo o truque novamente, obtemos

$$[x, y][x_1, x_2]x_3 \cdots x_n = \frac{1}{2}([x, y] \circ [x_1, x_2])x_3 \cdots x_n + \frac{1}{2}[[x, y], [x_1, x_2]]x_3 \cdots x_n$$

mas, o primeiro termo é combinação linear dos elementos do tipo 1 e 2, pois $[x, y] \circ [x_1, x_2] = 2(x_1 \circ y)(x \circ x_2) - 2(u_1 \circ y)(y \circ u_2)$ (por (6)), e segue aplicando indução sobre $x_3 \cdots x_n$. Então, basta mostrar que $[[x, y], [x_1, x_2]]x_3 \cdots x_n$ é combinação linear dos elementos do tipo 1 e 2. Aplicando a identidade de Jacobi, temos

$$[[x, y], [x_1, x_2]] = [x, y, x_1, x_2] - [x, y, x_2, x_1]$$

e basta mostrar que $[x, y, x_1, x_2]x_3 \cdots x_n$ é combinação linear dos elementos do tipo 1 e 2. Aplicando (2), obtemos

$$[x, y, x_1, x_2] = [2(x_1 \circ y)x - 2(x_1 \circ x)y, x_2] = 2(x_1 \circ y)[x, x_2] - 2(x_1 \circ x)[y, x_2]$$

e basta aplicar indução sobre $[x, x_2]x_3 \cdots x_n$ e $[y, x_2]x_3 \cdots x_n$, e o resultado segue. □

Vale ressaltar que os elementos do tipo 1 estão no centro de A. Então, podemos reescrever essa proposição na seguinte forma:

Corolário 3.7.6. *Assuma (1) identidade fraca do par (A, L). Então, cada elemento $a \in A$ pode ser escrito da forma*

$$a = c + \sum_{j=1}^{n} c'_j x_{a_j} + \sum_{k=1}^{m} c''_k [x_{b_k}, x_{b'_k}]$$

em que $c, c'_j, c''_k \in Z(A)$ e $x_{a_j}, x_{b_k}, x_{b'_k} \in X$.

Capítulo 4

Resultados Principais

Neste capítulo, serão apresentados os resultados principais desta dissertação. Sempre trabalharemos com corpo de característica 0.

Na primeira seção, mostraremos que as identidades fracas de $M_2(K)$ são geradas por uma única identidade:

Teorema 1. *Todas as identidades fracas de $(M_2(K), \mathfrak{sl}(2,K))$ são consequências da identidade*

$$[x \circ y, z] = 0.$$

Na seção seguinte, encontraremos uma base finita para as identidades da álgebra de Lie $\mathfrak{sl}(2,K)$:

Teorema 2. *As identidades*

$$\sum_{\sigma \in S_4} (-1)^\sigma [x_5, x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}] = 0$$
$$[y,z](adx)^3 = [y(adx)^3, z] + [y, z(adx)^3]$$

formam uma base para as identidades de $\mathfrak{sl}(2,K)$.

Na terceira seção, mostraremos o seguinte teorema:

Teorema 3. *Qualquer subvariedade própria da variedade de álgebras de Lie Var$(\mathfrak{sl}(2,K))$, com $car K = 0$, é subvariedade do produto $\mathscr{N}_l\mathscr{A}$, de uma variedade nilpotente $\mathscr{N}_l$ com a variedade abeliana $\mathscr{A}$.*

Uma consequência desse teorema é que Var$(\mathfrak{sl}(2,K))$ satisfaz a propriedade de Specht.
Na quarta seção, mostraremos

Teorema 4. *As identidades de $M_2(K)$ admitem uma base finita de identidades.*

E na última seção encontraremos uma base minimal de identidades das matrizes 2×2:

Teorema 5. *As identidades $s_4(x_1,x_2,x_3,x_4) = 0$ e $[[x_1,x_2]^2, x_1] = 0$ formam uma base minimal para as identidades de $M_2(K)$.*

§4.1 Identidades fracas de $(M_2(K), \mathfrak{sl}(2,K))$

O objetivo aqui é provar o seguinte teorema:

Teorema 4.1.1. *Se car $K = 0$, então toda identidade multilinear fraca de $(M_2(K), \mathfrak{sl}(2,K))$ é consequência de*

$$[x \circ y, z] = 0. \tag{1}$$

Caso $\operatorname{car} K = 0$, toda identidade fraca é consequência das identidades multilineares fracas (o argumento de linearização vale aqui, c.f. Teorema 2.10.2.(ii)), logo, uma consequência desse teorema é que toda identidade fraca de $(M_2(K), \mathfrak{sl}(2,K))$ é consequência de (1), caso $\operatorname{car} K = 0$.

Esse teorema é consequência da seguinte proposição:

Proposição 4.1.2. *Seja $f(x_1, \cdots, x_m)$ um polinômio multilinear. Defina $f'(x_1, \cdots, x_m) = f(x_2, x_1, x_3, \cdots, x_m)$. Então, existe um polinômio multilinear $v(y_0, y_1, \cdots, y_{m-2})$ tal que a identidade*

$$f(x_1, \cdots, x_m) - f'(x_1, \cdots, x_m) = v\left([x_1, x_2], x_3, \cdots, x_m\right)$$

é consequência de (1).

Demonstração. Por linearidade, basta mostrarmos a validade da proposição para os monômios. Suponha, em primeiro lugar, $f(x_1, \cdots, x_m) = x_1 x_{i_1} \cdots x_{i_l} x_2$.
Se $l = 0$, basta escrever $f(x_1, x_2) - f(x_2, x_1) = [x_1, x_2]$, (nesse caso, $v(y_0) = y_0$).
Caso $l > 0$, escreva $y = x_{i_1} \cdots x_{i_l}$. Pelo corolário 3.7.6, podemos escrever $y = c + \sum c'_i x_i + \sum c''_k [x_{b_k}, x_{b'_k}]$, com c, c'_i, c''_k centrais. Então, o elemento $x_1 c x_2 = c x_1 x_2$ cai no caso $l = 0$. Para os demais casos, seja $c = (x_{i_1} \circ x_{j_1}) \cdots (x_{i_k} \circ x_{j_k})$ ou $c = (x_{i_1} \circ x_{j_1}) \cdots (x_{i_k} \circ x_{j_k})([x_i, x_j] \circ x_o)$ e $t = x_i$ ou $t = [x_{b_k}, x_{b'_k}]$ (note que, ambos os casos, $t \in L(X)$ e c é central). Daí, assumindo $f = c x_1 t x_2$, temos

$$f - f' = c \left(\underbrace{x_1 t x_2 - x_2 t x_1 + t[x_1, x_2]}_{(x_1 \circ t) x_2 - (x_2 \circ t) x_1} - t[x_1, x_2] \right)$$

Uma vez que, pelo lema 3.7.4 (vale para qualquer elemento de $L(X)$), $(x_1 \circ t)x_2 - (x_2 \circ t)x_1 = \frac{1}{2}[x_2, x_1, t]$, temos que $f - f' = v([x_1, x_2], t, c)$, em que

$$v(y_0, t, c) = \frac{1}{2} c[t, y_0] - c t y_0$$

(em que $t = x$ é uma variável ou $t = [x, y]$ é um comutador, e $c = (v_{i_1} \circ v_{j_1}) \cdots (v_{i_k} \circ v_{j_k})$, com cada v_{i_l}, v_{j_l} variáveis ou comutadores).

O caso $f = x_2 x_{i_1} \cdots x_{i_l} x_1$ é análogo, e se $f = x_{i_1} \cdots x_{i_l} x_1 x_{j_1} \cdots x_{j_n} x_2 x_{p_1} \cdots x_{p_o}$, basta por em evidência as letras no início e no fim, e segue o resultado devido ao caso anterior. □

Demonstração (Teorema 4.1.1). Seja $f(x_1, \cdots, x_m)$ uma identidade multilinear fraca de $M_2(K)$. A demonstração será feita por indução em m. Caso $m = 2$, nada a fazer, pois, nesse caso não existem identidades multilineares de grau 2, logo, vale vacuosamente.
Agora, assuma que toda identidade fraca multilinear de grau menor que m seja consequência de (1). Pela proposição anterior, existe um polinômio multilinear $v(y_0, y_1, \cdots, y_{m-2})$ tal que

$$f - f' = v([x_1, x_2], x_3, \cdots, x_m)$$

é consequência de (1). Sendo f (e então f') identidades fracas, segue que $v([x_1,x_2],x_3,\cdots,x_m)$ é uma identidade fraca de $M_2(K)$. Dados quaisquer $g_0,g_1,\cdots,g_{m-2}\in\mathfrak{sl}(2,K)$, como a álgebra derivada de $\mathfrak{sl}(2,K)$ é ela própria, temos que existem $h_1,h_2,\cdots,h_{2p}$ tais que $g_0=[h_1,h_2]+\cdots+[h_{2p-1},h_{2p}]$, logo

$$v(g_0,g_1,\cdots,g_{m-2})=v([h_1,h_2],g_1,\cdots,g_{m-2})+\cdots+v([h_{2p-1},h_{2p}],g_1,\cdots,g_{m-2})=0$$

e $v(y_0,y_1,\cdots,y_{m-2})$ é identidade fraca de $M_2(K)$. Pela hipótese de indução, $v(y_0,y_1,\cdots,y_{m-2})$ é consequência de (1), e segue disso que $f-f'=0$ é consequência de (1). Como a troca de variáveis x_1 e x_2 é arbitrária, segue que, para cada permutação $\sigma\in S_m$, a identidade

$$f(x_1,\cdots,x_m)-f(x_{\sigma(1)},\cdots,x_{\sigma(m)})=0 \tag{7}$$

é consequência de (1). Sendo f multilinear, podemos escrever

$$f(x_1,\cdots,x_m)=\sum_{\tau\in S_m}a_\tau x_{\tau(1)}\cdots x_{\tau(m)}$$

daí, somando as equações (7) em relação a todo $\sigma\in S_m$, obtemos que

$$m!f(x_1,\cdots,x_m)-\sum_{\sigma\in S_m}\sum_{\tau\in S_m}a_\tau x_{\sigma\tau(1)}\cdots x_{\sigma\tau(m)}=m!f(x_1,\cdots,x_m)-\lambda\sum_{\sigma\in S_m}x_{\sigma(1)}\cdots x_{\sigma(m)}=0$$

é consequência de (1), para algum $\lambda\in K$ adequado. Tomando, em particular $x_1=\cdots=x_m=h=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, temos que $f(h,\cdots,h)=0$, e então

$$-\lambda m!h^m=0$$

ou seja, $\lambda=0$, e daí, $f(x_1,\cdots,x_m)=0$ é consequência de (1), provando o teorema. □

§4.2 Base de Identidades de $\mathfrak{sl}(2,K)$

O objetivo aqui é mostrar que as identidades

$$x_5s_4(\operatorname{ad}x_1,\operatorname{ad}x_2,\operatorname{ad}x_3,\operatorname{ad}x_4)=0 \tag{8}$$

$$[y,z](\operatorname{ad}x)^3=[y(\operatorname{ad}x)^3,z]+[y,z(\operatorname{ad}x)^3] \tag{9}$$

formam uma base para as identidades da álgebra de Lie $\mathfrak{sl}(2,K)$. Mais tarde, Filipov demonstrou que todas as identidades de Lie de $\mathfrak{sl}(2,K)$ seguem de $[y,z,[t,x],x]+[y,x,[z,x],t]=0$, vide [39].

Nesta seção, adotaremos algumas convenções que irão facilitar bastante a notação:

- Utiliza-se $\bar{x}$ para indicar soma alternada, e.g.

$$[x,\bar{x}_1,\cdots,\bar{x}_n]=\sum_{\sigma\in S_n}(-1)^\sigma[x,x_{\sigma(1)},\cdots,x_{\sigma(n)}].$$

- Utiliza-se $\tilde{x}$ para indicar soma simétrica, e.g.

$$[\tilde{x}_1,\cdots,\tilde{x}_n]=\sum_{\sigma\in S_n}[x_{\sigma(1)},\cdots,x_{\sigma(n)}].$$

Lema 4.2.1. *São identidades de* $\mathfrak{sl}(2,K)$*:*

$$[x_n, \bar{x}_1, \cdots, \bar{x}_{n-1}] = 0 \qquad ,\forall n \geq 4 \tag{10}$$
$$[y,z](ad\,x)^{2k+1} = [y(ad\,x)^{2k+1}, z] + [y, z(ad\,x)^{2k+1}] \quad ,\forall k \geq 1 \tag{11}$$
$$[u,z,y,x,x,x] = [u,x,x,z,y,x] - [z,x,u,x,y,x] \tag{12}$$
$$[y,x,x,x,u,z] = [y,x,u,x,x,z] - [z,x,[y,x,u],x] \tag{13}$$

Demonstração. A identidade (10) segue pelo fato de $\mathfrak{sl}(2,K)$ ter dimensão 3, e a identidade ser antissimétrica em pelo menos 4 variáveis. Para a identidade (11), note que, da identidade fraca (4), substituindo $y = z = x$, temos $4x^2[x,u] = [x,u,x,x] = -u(\mathrm{ad}\,x)^3 = [u,x](\mathrm{ad}\,x)^2$. Lembre-se também que, da identidade fraca (1), temos x^2 um elemento do centro. Daí

$$[y,z](\mathrm{ad}\,x)^{2k+1} = -[y,z,x](\mathrm{ad}\,x)^{2k} = -4^k x^{2k}[y,z,x] = -[4^k x^{2k}[y,x],z] - [y, 4^k x^{2k}[z,x]] =$$
$$= -[[y,x](\mathrm{ad}\,x)^{2k}, z] - [y,[z,x](\mathrm{ad}\,x)^{2k}] = [y(\mathrm{ad}\,x)^{2k+1}, z] + [y, z(\mathrm{ad}\,x)^{2k+1}]$$

provando a validade da identidade $\forall k \geq 1$.
Da identidade (4), tomando $y = x$, temos $4x^2[z,u] = [x,u,x,z] - [x,z,u,x]$ (ou, com o nome das variáveis que iremos utilizar,

$$\begin{aligned} 4x^2[u,z] &= [x,z,x,u] - [x,u,z,x] = [x,z,u,x] + [[x,z],[x,u]] - [x,u,x,z] - [[x,u],[z,x]] \\ &= [u,x,x,z] - [z,x,u,x] \end{aligned}$$

em que na penúltima igualdade foi utilizada a Identidade de Jacobi). Utilizando também que $4x^2[x,u] = [u,x](\mathrm{ad}\,x)^2$, temos

$$\begin{aligned} [u,z,y,x,x,x] &= [u,z,y,x](\mathrm{ad}\,x)^2 = 4x^2[u,z,y,x] = [4x^2[u,z],y,x] \\ &= [[u,x,x,z],y,x] - [[z,x,u,x],y,x] \end{aligned}$$

e isso prova a identidade (12). Para a última, utilizando as mesmas identidades que foram utilizadas (agora, utilizaremos $4x^2[z,[y,x,u]] = [x,[y,x,u],x,z] - [x,z,[y,x,u],x]$), temos

$$\begin{aligned} [y,x,x,x,u,z] &= [[y,x](\mathrm{ad}\,x)^2, u, z] = 4x^2[y,x,u,z] = -4x^2[z,[y,x,u]] \\ &= -[x,[y,x,u],x,z] + [x,z,[y,x,u],x] = [y,x,u,x,x,z] - [z,x,[y,x,u],x] \end{aligned}$$

e isso prova a identidade (13). □

Lema 4.2.2. *Denote por* $PL_5'(\mathfrak{sl}(2,K))$ *as identidades lineares de grau 5 de* $\mathfrak{sl}(2,K)$*. Então, utilizando a notação da proposição 3.6.2,*

$$PL_5'(\mathfrak{sl}(2,K)) = KS_5 f_3 \oplus KS_5 f_5$$

Demonstração. Segue da proposição 3.6.2 e do Teorema 3.6.8. □

A ideia da demonstração do teorema é parecida no caso das identidades fracas: tentaremos sempre "reduzir o grau" de um polinômio multilinear, até cair numa identidade de grau 5. Para isso, provaremos o seguinte resultado:

Lema 4.2.3. *Considere a variedade gerada pelas identidades (8) e (9). Dados $f(x_1,\cdots,x_l)$ polinômio multilinear e $i,j\in\mathbb{N}$, com $i\neq j$ e $1\leq i,j\leq l$, existem $c\in K$ e $v(y_0,y_1,\cdots,y_{l-2})$ multilinear tal que*

$$f-\sigma_{ij}f=c\big((1-\sigma_{ij})[x_i,\tilde{x}_1,\cdots,\hat{x}_i,\cdots,\hat{x}_j,\cdots,\tilde{x}_l,x_j]\big)+v([x_i,x_j],x_1,\cdots,\hat{x}_i,\cdots,\hat{x}_j,\cdots,x_l) \quad (14)$$

(em que $\sigma_{ij}=(i\quad j)$) e caso l seja ímpar, podemos tomar $c=0$.

A consequência desse lema será o nosso teorema:

Teorema 4.2.4. *Var$(\mathfrak{sl}(2,K))$ é gerado pelas identidades (8) e (9).*

Demonstração. Seja $f(x_1,\cdots,x_l)$ uma identidade multilinear de $\mathfrak{sl}(2,K)$. Considere $i\neq j$ e escreva $f-\sigma_{ij}f$ na forma (14). Se l for par, podemos também tomar $c=0$, pois, considere $x_i=e=\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $x_j=f=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ e $x_1=\cdots=\hat{x}_i=\cdots=\hat{x}_j=\cdots=x_n=\begin{pmatrix}1&0\\0&-1\end{pmatrix}=:h$. Então $v([e,f],h,\cdots,h)=-v(h,\cdots,h)=0$, uma vez que v é um polinômio de Lie. Ainda, $f(x_1,\cdots,x_l)=0$, uma vez que f é identidade. Por fim, temos

$$c([e,\tilde{h},\cdots,\tilde{h},f]-[f,\tilde{h},\cdots,\tilde{h},e])=c(l-2)!2^{l-2}\left([e,f]-(-1)^{l-k}[f,e]\right)=-c(l-2)!2^{l-1}h$$

e necessariamente $c=0$, pois $(l-2)!2^{l-1}\neq 0$ (estamos num corpo de característica zero).

Após essa consideração inicial, seja $f(x_1,\cdots,x_l)$ uma identidade de $\mathfrak{sl}(2,K)$. Provaremos por indução em l. Se $l=5$, então, segue pelo Lema 4.2.2. Se $l>5$, assumimos que todas as identidades de grau menor que l são consequências de (8) e (9), e seja σ_{ij} uma permutação. Escreva $f-\sigma_{ij}f=v([x_i,x_j],x_1,\cdots,\hat{x}_i,\cdots,\hat{x}_j,\cdots,x_n)$, conforme a representação (14), e sendo f (e portanto $\sigma_{ij}f$) identidade, temos que $v([x_i,x_j],x_1,\cdots,\hat{x}_i,\cdots,\hat{x}_j,\cdots,x_n)$ é identidade. Mas, sendo a álgebra de Lie $\mathfrak{sl}(2,K)$ simples (e então, coincide com sua álgebra derivada), $\mathfrak{sl}(2,K)$ é gerada pelos seus comutadores. Daí, $v(y_0,y_1,\cdots,y_{l-2})$ também é identidade. De fato, dados $g_0,g_1,\cdots,g_{l-2}\in\mathfrak{sl}(2,K)$, queremos concluir que $v(g_0,g_1,\cdots,g_{l-2})=0$, e assim, teremos que $v(y_0,\cdots,y_{l-2})=0$ é identidade da álgebra de Lie. Escreva $g_0=[g_1',h_1']+\cdots+[g_n',h_n']$, soma de comutadores (possível pois $\mathfrak{sl}(2,K)$ é simples). Então, sendo v polinômio multilinear, temos que $v(g_0,g_1,\cdots,g_{l-2})=v([g_1',h_1'],g_1,\cdots,g_{l-2})+\cdots+v([g_n',h_n'],g_1,\cdots,g_{l-2})=0$ e $v(y_0,\cdots,y_{l-2})$ é uma identidade, e por hipótese de indução, consequência de (8) e (9). Então $f-\sigma_{ij}f=0$ também é consequência de (8) e (9). Como f sendo identidade implica em $\sigma_{ij}f$ identidade, e todas as permutações são produtos de transposições, pode-se fazer uma soma telescópica e concluir que $f-\sigma f$ é consequência de (8) e (9), para qualquer permutação $\sigma\in S_l$. Fazendo a soma em todos as permutações, concluimos que a identidade

$$0=\sum_{\sigma\in S_l}(f-\sigma f)=l!f+c\sum_{\sigma\in S_l}[x_{\sigma(1)},\cdots,x_{\sigma(l)}]$$

é consequência de (8) e (9), para algum $c\in K$. Mas, temos $[\tilde{x}_1,\cdots,\tilde{x}_l]=0$ (vale em qualquer álgebra de Lie), e $f=0$ é consequência de (8) e (9), provando o Teorema. □

Lema 4.2.5. *Em qualquer álgebra de Lie L, dados $a,x_1,\cdots,x_n\in L$, vale*

$$n![a,x_1,\cdots,x_n]=[a,\tilde{x}_1,\cdots,\tilde{x}_n]+\sum_i[a,w_1^{(i)},\cdots,w_{n-2}^{(i)}]$$

em que os $w_k^{(i)}$ são alguns dos x_j ou algum comutador envolvendo dois dos x_j, sempre respeitando o grau do monômio sendo $n+1$, (não interessa muito o que seja, o mais importante é que a variável a não está inclusa nesses comutadores).

Demonstração. Provaremos por indução em n. Se $n = 1$ o resultado vale trivialmente. Se $n > 1$, então, utilizando a hipótese de indução, obtemos

$$n![a, x_1, \cdots, x_n] = n(n-1)![[a, x_1], \cdots, x_n] = n[[a, x_1], \tilde{x}_2, \cdots, \tilde{x}_n] + \sum_i [[a, x_1], w_2^{(i)}, \cdots, w_{n-2}^{(i)}]$$

separando os n's termos $[a, x_1, \tilde{x}_2, \cdots, \tilde{x}_n]$, e utilizando a identidade de Jacobi k vezes, com $k = 0, \cdots, n-1$, para cada termo, obtemos que $[a, x_1, \tilde{x}_2, \cdots, \tilde{x}_n]$ é igual a:

$$\begin{aligned}
k = 0 :&[a, x_1, \tilde{x}_2, \cdots, \tilde{x}_n] \\
k = 1 :&[a, \tilde{x}_2, x_1, \tilde{x}_3, \cdots, \tilde{x}_n] + [a, [x_1, \tilde{x}_2], \tilde{x}_3, \cdots, \tilde{x}_n] \\
k = 2 :&[a, \tilde{x}_2, \tilde{x}_3, x_1, \tilde{x}_4, \cdots, \tilde{x}_n] + [a, [x_1, \tilde{x}_2], \tilde{x}_3, \cdots, \tilde{x}_n] + [a, \tilde{x}_2, [x_1, \tilde{x}_3], \tilde{x}_4, \cdots, \tilde{x}_n] \\
&\vdots \\
k = n-1 :&[a, \tilde{x}_2, \cdots, \tilde{x}_n, x_1] + [a, [x_1, \tilde{x}_2], \tilde{x}_3, \cdots, \tilde{x}_n] + \cdots + [a, \tilde{x}_2, \cdots, \tilde{x}_{n-1}, [x_1, \tilde{x}_n]]
\end{aligned}$$

somando todas essas equações (note que x_1 está correndo todas as possibilidades de ficar entre $x_2, \cdots, x_n$, e estamos considerando todas as possibilidades de ordenação de $x_2, \cdots, x_n$ em cada somatório), obteremos

$$\begin{aligned}
n![a, x_1, \cdots, x_n] =& n[a, x_1, \tilde{x}_2, \cdots, \tilde{x}_n] + \sum_i [a, w_1^{(i)}, \cdots, w_{n-1}^{(i)}] = \\
=& [a, \tilde{x}_1, \cdots, \tilde{x}_n] + \sum_l [a, w_1^{(l)}, \cdots, w_{n-1}^{(l)}]
\end{aligned}$$

provando o lema. □

Lema 4.2.6. *Na variedade gerada por (8) e (9), dado $f(x_1, \cdots, x_l)$ identidade multilinear e $i \neq j$, com $l = 5$ ou $l = 6$, existem $c \in K$ e $v(y_0, y_1, \cdots, y_{l-2})$ multilinear tal que*

$$f - \sigma_{ij} f = c\big((1 - \sigma_{ij})[x_i, \tilde{x}_1, \cdots, \hat{x}_i, \cdots, \hat{x}_j, \cdots, \tilde{x}_l, x_j]\big) + v([x_i, x_j], x_1, \cdots, \hat{x}_i, \cdots, \hat{x}_j, \cdots, x_l)$$

com $c = 0$ caso $l = 5$.

Demonstração. Uma vez que $[x_1, x_{\sigma(2)}, \cdots, x_{\sigma(l)}], \sigma \in S(2, \cdots, l)$ formam uma base de PL_l (lema 3.3.5), podemos supor, sem perda de generalidade, $i = 1, j = l$ e $f = [x_1, x_{i_1}, \cdots, x_{i_{l-1}}]$.
Considere primeiro o caso $l = 5$. Se $f = [x_1, x_5, x_2, x_3, x_4]$, o resultado é trivial, e se $f = [x_1, x_2, x_5, x_3, x_4]$, basta aplicar a identidade de Jacobi para obtermos $f - \sigma_{15} f = [x_1, x_5, x_2, x_3, x_4]$, e atingimos o resultado.
Vamos assumir, por enquanto, que a variedade satisfaz a identidade fraca (1) (e então, suas consequências também). Lembre-se que, neste caso, g^2 (ou $g \circ h$) sempre é elemento central, para quaisquer monômios de Lie g, h, uma vez que estamos assumindo a identidade (1).

Seja então $f = [x_1, x_2, x_3, x_5, x_4]$. Utilizando a identidade (2) repetidamente, obtemos

$$\begin{aligned}
&[x_1, x_2, x_3, x_5, x_4] - [x_5, x_2, x_3, x_1, x_4] = \\
=&[2(x_3 \circ x_2)x_1 - 2(x_3 \circ x_1)x_2, x_5, x_4] - [2(x_3 \circ x_2)x_5 - 2(x_3 \circ x_5)x_2, x_1, x_4] = \\
=&4(x_3 \circ x_2)[x_1, x_5, x_4] - [x_2, \underbrace{2(x_3 \circ x_1)x_5 - 2(x_3 \circ x_5)x_1}_{[x_5, x_1, x_3]}, x_4] = \\
=&4(x_3 \circ x_2)[x_1, x_5, x_4] - [x_2, [x_5, x_1, x_3], x_4].
\end{aligned}$$

Aplicando a identidade (4) a $4(x_3 \circ x_2)[[x_1,x_5],x_4]$ obteremos uma soma de comutadores, e todos contêm o comutador $[x_1,x_5]$, e isso mostra o lema para esse caso.

Por fim, considere $f=[x_1,\cdots,x_5]$. Fazendo a mesma coisa acima - aplicar a identidade (2) repetidas vezes - e aplicando a identidade de Jacobi, obtemos

$$\begin{aligned}
&[x_1,x_2,x_3,x_4,x_5]-[x_5,x_2,x_3,x_4,x_1]=\\
=&[2(x_3\circ x_2)x_1-2(x_3\circ x_1)x_2,x_4,x_5]-[2(x_3\circ x_2)x_5-2(x_3\circ x_5)x_2,x_4,x_1]=\\
=&2(x_3\circ x_2)[x_1,x_5,x_4]-[x_2,x_4,\underbrace{2(x_3\circ x_1)x_5-2(x_3\circ x_5)x_1}_{[x_5,x_1,x_3]}]=\\
=&2(x_3\circ x_2)[x_1,x_5,x_4]-[x_2,x_4,[x_5,x_1,x_3]].
\end{aligned}$$

Aplicando a identidade (4) a $2(x_3 \circ x_2)[[x_1,x_5],x_4]$, obtemos uma soma de comutadores, todos contendo o comutador $[x_1,x_5]$, e o resultado vale também. Como todas as identidades de grau 5 de $\mathfrak{sl}(2,K)$ são consequências das identidades (8) e (9) (lema 4.2.2), e as identidades obtidas agora são identidades de $\mathfrak{sl}(2,K)$ (pois são consequências de (1)), segue que essas igualdades valem para qualquer variedade que satisfazem (8) e (9). Assim, prova-se o lema para o caso $l=5$.
Para $l=6$, se $f=[x_1,x_{i_1},\cdots,x_{i_5}]$, com $i_5\neq l$, basta olharmos o comutador $[x_1,x_{i_1},\cdots,x_{i_4}]$, e vale pelo caso $l=5$. Se $f=[x_1,x_2\cdots,x_6]$, basta aplicarmos o Lema 4.2.5, e obteremos

$$f=[x_1,\tilde{x}_2,\cdots,\tilde{x}_5,x_6]+\sum_i[x_1,w_1^{(i)},w_2^{(i)},w_3^{(i)},x_6].$$

Daí

$$f-\sigma_{16}f=1\big([x_1,\tilde{x}_2,\cdots,\tilde{x}_5,x_6]-[x_6,\tilde{x}_2,\cdots,\tilde{x}_5,x_1]\big)+(1-\sigma_{16})\left(\sum_i[x_1,w_1^{(i)},w_2^{(i)},w_3^{(i)},x_6]\right).$$

Escrevendo $g_i(x_1,w_1^{(i)},w_2^{(i)},w_3^{(i)},x_6)=[x_1,w_1^{(i)},w_2^{(i)},w_3^{(i)},x_6]$, temos que g_i é um polinômio de grau 5, e neste caso, provou-se acima que $g_i-\sigma_{16}g_i$ é um polinômio multilinear da forma $v_i([x_1,x_6],x_2,\cdots,x_5)$, e um somatório de polinômios dessa forma permanece nesta forma. Mas, isso mostra que $f-\sigma_{16}f$ pode ser representado na forma (14), e isso prova para o caso $l=6$. □

Note que, como demonstramos o Lema 4.2.3 para o caso $l=6$, o Teorema vale para as identidades de grau 6, ou seja, as identidades (12) e (13) são consequências das identidades (8) e (9), e daí, poderemos utilizá-los na demonstração do Lema 4.2.3. Ainda, podemos utilizar mais algumas outras identidades que são consequências das identidades de grau 5 e de grau 6, que nos auxiliarão na demonstração do lema:

Lema 4.2.7. *São consequências das identidades (8) e (9):*

$$[y,z](adx)^{2k+1}=[y(adx)^{2k+1},z]+[y,z(adx)^{2k+1}],\forall k\geq 1 \tag{15}$$

$$[u,z,y,\underbrace{x,\cdots,x}_{t\ vezes}]=[u,x,x,z,y,\underbrace{x,\cdots,x}_{t-2\ vezes}]-[z,x,u,x,y,\underbrace{x,\cdots,x}_{t-2\ vezes}] \tag{16}$$

$$[y,\underbrace{x,\cdots,x}_{t\ vezes},u,z]=[y,\underbrace{x,\cdots,x}_{t-2\ vezes},u,x,x,z]-[z,x,[y,\underbrace{x,\cdots,x}_{t-2\ vezes},u],x] \tag{17}$$

Demonstração. Pelo comentário acima, as identidades de grau 6 são consequências das identidades de grau 5 (e então, das identidades (8) e (9)). A equação (16) é consequência da identidade (12),

bastando aplicar $t-2$ vezes o comutador com x. A identidade (17) é consequência da identidade (13), bastando fazer a mudança de variável (que é um endomorfismo) $y \mapsto y(\operatorname{ad} x)^{t-3}$.

Para a identidade (15), note primeiramente que a identidade

$$[[z,x],[y,x],x] = 0 \tag{18}$$

é consequência de (9). De fato, aplicando a identidade de Jacobi, obtemos

$$[z,x,[y,x],x] = [z,x,[y,x,x]] + [z,x,x,[y,x]].$$

Olhando cada um dos termos:

$$\begin{aligned}[z,x,x,[y,x]] &= [z,x,x,y,x] - [z,x,x,x,y]\\ [y,x,x,[z,x]] &= -[y,x,x,z,x] + [y,x,x,x,z].\end{aligned}$$

Aplicando a identidade de Jacobi para o primeiro termo de cada uma das equações:

$$\begin{aligned}[z,x,x,y,x] &= [z,x,[x,y],x] + [z,x,y,x,x]\\ -[y,x,x,z,x] &= -[y,x,[x,z],x] - [y,x,z,x,x].\end{aligned}$$

Da identidade de Jacobi, temos $[z,x,y,x,x] - [y,x,z,x,x] = -[y,z,x,x,x]$. Segue que, utilizando a identidade (9)

$$[[z,x],[y,x],x] = -2[z,x,[y,x],x]$$

o que prova a identidade (18).

Note também que a relação

$$[z,y,y,x,y] = [z,y,x,y,y] \tag{19}$$

é identidade de $\mathfrak{sl}(2,K)$, consequência de (9). De fato, aplicando a identidade de Jacobi:

$$\begin{aligned}[z,y,y,x,y] &= [z,y,y,y,x] + [z,y,y,[x,y]]\\ [z,y,x,y,y] &= [z,x,y,y,y] + [z,[y,x],y,y]\end{aligned}$$

Note que, aplicando diversas vezes a identidade de Jacobi:

$$\begin{aligned}[z,[y,x],y,y] &= -[z,[x,y,y],y] + \underbrace{[[z,y],[y,x],y]}_{0}\\ &= -[z,[x,y,y,y]] - [z,y,[x,y,y]] \underbrace{-[z,y,y,[y,x]] + [z,y,[x,y,y]]}_{=-[z,y,[y,x],y]=0}\\ &= -[z,[x,y,y,y]] - [z,y,y,[y,x]]\end{aligned}$$

Daí, fazendo a diferença $[z,y,x,y,y] - [z,y,y,x,y]$ tendo em mente a identidade (9), temos que a diferença é nula, e a identidade realmente vale (e é consequência de (9)).

Assim, podemos provar a validade da identidade (15) por indução. Temos, aplicando a hipótese de indução:

$$[y,z](\operatorname{ad}(x))^{2k+1} = [y(\operatorname{ad}(x))^{2k-1},z]\operatorname{ad}(x)^2 + [y,z(\operatorname{ad}(x))^{2k-1}]\operatorname{ad}(x)^2$$

aplicando a identidade (19) e depois a identidade de Jacobi sobre $[y(\mathrm{ad}(x))^{2k-1},z]\mathrm{ad}(x)^2$, obtemos

$$[y(\mathrm{ad}(x))^{2k-1},z]\mathrm{ad}(x)^2=[y(\mathrm{ad}(x))^{2k-1},x,z,x]=\underbrace{[y(\mathrm{ad}(x))^{2k-1},x,x,z]}_{[y\mathrm{ad}(x)^{2k+1},z]}+[y(\mathrm{ad}(x))^{2k-1},x,[z,x]] \tag{20}$$

da mesma forma, obtemos

$$\begin{aligned}[y,z(\mathrm{ad}(x))^{2k-1}]\mathrm{ad}(x)^2&=-[z(\mathrm{ad}(x))^{2k-1},y]\mathrm{ad}(x)^2\\&=-\underbrace{[z(\mathrm{ad}(x))^{2k-1},x,x,y]}_{[z\mathrm{ad}(x)^{2k+1},y]}-[z(\mathrm{ad}(x))^{2k-1},x,[y,x]]\end{aligned} \tag{21}$$

Note ainda que, aplicando a hipótese de indução e a identidade (18)

$$\underbrace{[y(\mathrm{ad}(x))^{2k-1},x,[z,x]]}_{[[y,x]\mathrm{ad}(x)^{2k-1},[z,x]}-\underbrace{[z(\mathrm{ad}(x))^{2k-1},x,[y,x]]}_{[[z,x]\mathrm{ad}(x)^{2k-1},[y,x]}=[[y,x],[z,x]]\mathrm{ad}(x)^{2k-1}=0$$

e essa identidade é consequência (8) e (9). Daí, somando (20) e (21), obtemos que a identidade requerida é consequência de (8) e (9). □

Demonstração (Lema 4.2.3). Novamente, como $[x_1,x_{\sigma(2)},\cdots,x_{\sigma(l)}]$ constituem base de PL_l, podemos considerar, sem perda de generalidade, $i=1$ e $j=l$ e $f=[x_1,x_{i_1},\cdots,x_{i_{l-1}}]$, separando em casos, dependendo de onde x_l aparece no comutador. Faremos por indução em l, para $l\geq 5$, provando as seguintes afirmações:

(i) Se $l=2k+1$, existe representação da forma (14), com $c=0$

(ii) Se $l=2k$, existe representação da forma (14)

A base de indução $l=5$ foi provada no lema 4.2.6. Seja então $l>6$. Se $l=2k$ par, o argumento é idêntico ao utilizado no lema 4.2.6 para $l=6$, com auxílio da hipótese de indução. Considere então $l=2k+1$. Se $f=[x_1,x_{i_1},\cdots,x_{i_{l-2}},x_{i_{l-1}}]$, com $i_{l-2}\neq l$ e $i_{l-1}\neq l$, então, basta olharmos o comutador $[x_1,x_{i_1},\cdots,x_{i_{l-3}}]$ (ambos x_1 e x_l estão nesse pedaço do comutador), e o resultado seguirá por indução, pois o grau desse comutador é $l-2$ (ímpar).
Então, considere $f=[x_1,\cdots,x_{l-2},x_l,x_{l-1}]$. Por hipótese de indução, temos que

$$f-\sigma_{1l}f=c\big([x_1,\tilde{x}_2,\cdots,\tilde{x}_{l-2},x_l,x_{l-1}]-[x_l,\tilde{x}_2,\cdots,\tilde{x}_{l-2},x_1,x_{l-1}]\big)+v([x_1,x_l],x_2,\cdots,x_{l-1})$$

utilizando a linearização da identidade (17) (com $t=l-3$), e trocando $z=x_{l-1},u=x_l$ e $y=x_1$, obtemos

$$\begin{aligned}&[x_1,\tilde{x}_2,\cdots,\tilde{x}_{l-2},x_l,x_{l-1}]=\\&=[x_1,\tilde{x}_2,\cdots,\tilde{x}_{l-4},x_l,\tilde{x}_{l-3},\tilde{x}_{l-2},x_{l-1}]-[x_{l-1},\tilde{x}_2,[x_1,\tilde{x}_3,\cdots,\tilde{x}_{l-3},x_l],\tilde{x}_{l-2}]\end{aligned}$$

e o resultado segue por indução nos comutadores de grau ímpar $[x_1,x_{\sigma(2)},\cdots,x_{\sigma(l-4)},x_l,\tilde{x}_{\sigma(l-3)}]$, para cada permutação σ, e, utilizando a identidade de Jacobi nos outros monômios obtemos

$$\begin{aligned}[x_{l-1},x_{\sigma(2)},[x_1,x_{\sigma(3)},\cdots,x_{\sigma(l-3)},x_l],x_{\sigma(l-2)}]&=[x_{l-1},[x_1,x_{\sigma(3)},\cdots,x_{\sigma(l-3)},x_l],x_{\sigma(2)},x_{\sigma(l-2)}]\\&+[x_{l-1},[x_{\sigma(2)},[x_1,x_{\sigma(3)},\cdots,x_{\sigma(l-3)},x_l]],x_{\sigma(l-2)}]\end{aligned}$$

e daí, basta aplicar a hipótese de indução aos comutadores (de grau ímpar) $[x_{l-1},[x_1,x_{\sigma(3)},\cdots,x_{\sigma(l-3)},x_l]]$ e $[[x_{\sigma(2)},[x_1,x_{\sigma(3)},\cdots,x_{\sigma(l-3)},x_l]]$, para cada permutação σ.

Por fim, considere $f[x_1, \cdots, x_l]$. Escreva, segundo o lema 4.2.5, $f = [x_1, \tilde{x}_2, \cdots, \tilde{x}_{l-1}, x_l] + \sum_i [x_1, w_1^{(i)}, \cdots, w_{l-2}^{(i)}, x_l]$. Então

$$f - \sigma_{1l} f = \underbrace{[x_1, \tilde{x}_2, \cdots, \tilde{x}_{l-1}, x_l] - [x_l, \tilde{x}_2, \cdots, \tilde{x}_{l-1}, x_1]}_{[[x_1, x_l], [\tilde{x}_2, \cdots, \tilde{x}_{l-1}]]} + (1 - \sigma_{1l}) \left(\sum_i [x_1, w_1^{(i)}, \cdots, w_{l-1}^{(i)}, x_l] \right)$$

em que a igualdade segue da linearização da identidade (15) (com $2k + 1 = l - 2$). Daí, resta analisarmos os comutadores $[x_1, w_1^{(i)}, \cdots, w_{l-2}^{(i)}, x_l]$, que se reduzem ao caso $f = [x_1, \cdots, [x_i, x_{i+1}], \cdots, x_l]$, com $i \neq 1, i + 1 \neq l$. Neste caso, aplicando a hipótese de indução, obtemos

$$f - \sigma_{1l} f = c(1 - \sigma_{1l})[x_1, \tilde{x}_2, \cdots, [x_i, x_{i+1}]^{\sim}, \cdots, \tilde{x}_{l-1}, x_l] + v([x_1, x_l], x_2, \cdots, x_{l-1})$$

e basta verificarmos o primeiro termo (pois o segundo já está na forma requerida). Utilizando a identidade (16) muitas vezes, para $t = l - 2$ (ímpar), obtemos que

$$[u, z, y, \underbrace{x, \cdots, x}_{t \text{ vezes}}] = \sum_i [w_i, z, y, x] - \sum_i [u_i, v_i, y, x] \tag{22}$$

em que w_i, u_i, v_i são comutadores em x, u e z (e não em y). Escreva

$$g = [x_1, \tilde{x}_2, \cdots, [x_i, x_{i+1}]^{\sim}, \cdots, \tilde{x}_{l-1}, x_l]$$

como combinação linear de comutadores da forma $[x_1, [x_i, x_{i+1}], x_{\sigma(2)}, \ldots, x_{\sigma(l-1)}, x_l]$, sendo σ permutação do conjunto $\{2, \cdots, i-1, i+2, \cdots, l-1\}$. Temos g simétrico em $x_2, \cdots, x_{i-1}, x_{i+2}, \cdots, x_{l-1}$, e daí, linearizando a identidade (22) e substituindo as variáveis simétricas da linearização por $x_2, \cdots, x_{i-1}, x_{i+2}, \cdots, x_{l-1}$ e tomando $y = x_l, z = x_i, u = x_{i+1}$, chegamos que

$$[[x_1, \tilde{x}_2, \cdots, \widetilde{[x_i, x_{i+1}]}, \cdots, \tilde{x}_{l-1}], x_l] = \sum_k \alpha_k [x_1, [x_i, x_{i+1}], \tilde{x}_2, \cdots, \tilde{x}_{l-1}, x_l] =$$

$$\sum_k -\alpha_k [x_i, x_{i+1}, x_1, \tilde{x}_2, \cdots, \tilde{x}_{l-1}, x_l] = \sum_p [w_i', x_i, x_1, x_p, x_l] + \sum_p [u_i', v_i', x_1, x_p, x_l]$$

e reduzimos para um polinômios de grau 5, e o resultado segue por indução. □

Isso conclui a demonstração de que $\mathfrak{sl}(2, K)$ admite base finita de identidades.

§4.3 Variedade Var($\mathfrak{sl}(2, K)$)

O objetivo aqui é demonstrar o seguinte teorema:

Teorema 4.3.1. *Qualquer subvariedade própria da variedade de álgebras de Lie Var($\mathfrak{sl}(2, K)$), com car $K = 0$, é subvariedade do produto $\mathscr{N}_l\mathscr{A}$, de uma variedade nilpotente $\mathscr{N}_l$ com a variedade abeliana $\mathscr{A}$.*

Nesta seção, denotaremos por A a álgebra associativa livre gerada por $X = \{x_1, x_2, \cdots\}$, $L = L(X)$ a álgebra de Lie livre gerada pelos mesmos elementos, com respeito ao comutador, T o ideal das identidades fracas de $(M_2(K), \mathfrak{sl}(2, K))$, $A_1 = A/T$ e $L_1 = L/(T \cap L)$.

Lema 4.3.2. *Todo elemento $a \in A_1$ admite uma única representação da forma*

$$a = c + v$$

com $c \in Z(A_1)$ e v uma combinação linear de elementos do tipo 2, segundo a notação da proposição 3.7.5.

Demonstração. Uma tal representação existe, pela proposição 3.7.5. Para a unicidade, basta mostrar que se $0 = c + v$, então $c = v = 0$. Escreva $v = v(x_1, \cdots, x_l)$. Então, como $0 = [c + v, x_{l+1}] = [v(x_1, \cdots, x_l], x_l]$, temos que $[v, x_{l+1}] = 0$ é uma identidade fraca para $M_2(K)$. Logo v é uma identidade fraca também, pois dados $h_1, \cdots, h_l \in \mathfrak{sl}(2,K)$, temos $v(h_1, \cdots, h_l) \in \mathfrak{sl}(2,K)$, e ao mesmo tempo, $v(h_1, \cdots, h_l) \in Z(M_2(K))$ (pois $[v, x_l] = 0$, ou seja, v cai no centro). Mas, como $\mathfrak{sl}(2,K)$ não possui centro, isto é, $Z(M_2(K)) \cap \mathfrak{sl}(2,K) = 0$, temos necessariamente $v(h_1, \cdots, h_l) = 0$, e v é uma identidade fraca de $M_2(K)$.
Mas $v \in T$, ou seja, $v = 0$ em A_1, o que implica $c = 0$. O resultado segue. □

Lema 4.3.3. *Seja $u(x_1, \cdots, x_l) \in L_1$. Seja I o ideal em A_1 gerado por todos os elementos $[u(v_1, \cdots, v_l), v_{l+1}]$, com $v_1, \cdots, v_{l+1} \in L_1$ e $\mathscr{T}$ o ideal em L_1 gerado pelos mesmos elementos. Então $\mathscr{T} = I \cap L_1$.*

Demonstração. Claramente $\mathscr{T} \subset I \cap L_1$. Seja $x \in I$. Queremos concluir que, se $x \in L_1$ (ou seja, se $x \in I \cap L_1$), então $x \in \mathscr{T}$. Podemos supor que

$$x = x_{i_1} \cdots x_{i_t} [u(v_1, \cdots, v_l), v_{l+1}] x_{i_{t+1}} \cdots x_{i_k}$$

então $x = c + v$, com $x \in Z(A_1)$ e $v \in \mathscr{T}$. De fato, considere A_1' a álgebra associativa gerada por $x_{i_1}, \cdots, x_{i_k}, [u(v_1, \cdots, v_l), v_{l+1}], v_1, \cdots, v_{l+1}$, e L_1' a álgebra de Lie gerada pelo comutador pelos mesmos elementos. Segue, pela proposição 3.7.5, que $x = c + v$, com c e v combinação linear de elementos do tipo 1 e do tipo 2, respectivamente, em $x_{i_1}, \cdots, x_{i_k}, [u(v_1, \cdots, v_l), v_{l+1}]$.
Uma vez que sempre $[u(v_1, \cdots, v_l), v_{l+1}] \in L_1$, temos $c \in Z(A_1)$. Todo elemento $w \in \mathscr{T}$ é combinação linear de elementos da forma

$$w_1 = [w', u_{l+1}], w' \in \mathscr{T}, u_{l+1} \in L_1$$
$$w_2 = [u(v_1, \cdots, v_l), v_{l+1}], v_1, \cdots, v_{l+1} \in L_1.$$

Segue por (4) que $(x_i \circ x_j) w_q \in \mathscr{T}$ $(q = 1, 2)$, e por (3), combinado com (4), que $(w_q \circ x_t)[x_i, x_j], (w_q \circ x_i) x_j \in \mathscr{T}$ $(q = 1, 2)$. Daí, toda combinação linear de elementos do tipo 2 em $x_{i_1}, \cdots, x_{i_k}, [u(v_1, \cdots, v_l), v_{l+1}]$ é elemento de $\mathscr{T}$, e então, $v \in \mathscr{T}$.

Agora, se $x \in L_1$, então $x = c + v = z$, para $z \in L_1$. Como, por (2), z é combinação linear de elementos do tipo 2, de $c + (v - z) = 0$, segue, por unicidade da combinação (lema 4.3.2), que $c = 0$, e daí, $x = v \in \mathscr{T}$. Daí $I \cap L_2 = \mathscr{T}$. □

Lema 4.3.4. *Assuma que (1) seja uma identidade fraca ao par (A, L). Suponha $([x_1, x_2] \circ x_3)$ nil. Então a álgebra A', gerada por $[v_1, v_2] \circ v_3, v_1, v_2, v_3 \in L$, é nilpotente.*

Demonstração. Denote $\langle x_1, x_2, x_3 \rangle = \sum_{\sigma \in S_3} (-1)^\sigma x_{\sigma(1)} x_{\sigma(2)} x_{\sigma(3)}$. Segue de (5) que

$$3([x_1, x_2] \circ x_3) = [x_1, x_2] \circ x_3 + [x_2, x_3] \circ x_1 + [x_3, x_2] \circ x_1 = 2 \sum_{\sigma \in S_3} (-1)^\sigma x_{\sigma(1)} x_{\sigma(2)} x_{\sigma(3)}.$$

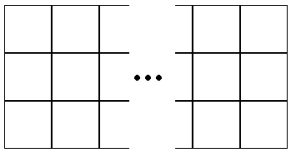
Então, a álgebra A' coincide com a álgebra gerada por $\langle x_1, x_2, x_3\rangle$. Assuma $f_0 = (\langle x_1, x_2, x_3\rangle)^m$ uma identidade fraca e considere $f = (\langle x_1, y_1, z_1\rangle)\cdots(\langle x_m, y_m, z_m\rangle)$. Considere o anel KS_{3m} como um KS_{3m}-módulo e escreva 1 como soma de idempotentes geradores dos ideais minimais (c.f. Teorema 2.8.11). Escreva primeiro $1 = e_1 + e_2$, com e_1 soma dos idempotentes relacionados com diagramas de Young com mais de 3 linhas. Então $f = 1f = e_1f + e_2f$.
Afirmação 1: $e_1f = 0$ é identidade fraca.
De fato, escreva $f = \sum_{\sigma\in S_{3m}} \alpha_\sigma\sigma(x_1y_1z_1\cdots x_my_mz_m)$, em que $\sigma \in S_{3m}$ age como permutação das variáveis (não importa muito agora uma notação precisa) $x_1, y_1, z_1, \cdots, x_m, y_m, z_m$. Então, denotando por R os elementos de S_{3m} que deixam as linhas invariantes, C os elementos que deixam as colunas invariantes, e podemos escrever sempre $C = S_{k_1}\times\cdots\times S_{k_o} = S_k \times C'$, com $k_1, \cdots, k_o$ o tamanho de cada coluna, $k = k_1$ e $C' = S_{k_2}\times\cdots S_{k_o}$ e, por suposição, $k > 3$, pois exigimos que o diagrama tenha mais de 3 linhas (ou seja, pelo menos a primeira coluna tem mais de 3 elementos), temos que um idempotente relacionado a um diagrama de Young com mais de 3 linhas é um múltiplo de um elemento da forma

$$\sum_{\rho\in R}\sum_{\gamma\in C}(-1)^\gamma\rho\gamma = \sum_{\rho\in R}\sum_{\sigma\in S_k,\gamma'\in C'}\rho(-1)^{\sigma\gamma'}\sigma\gamma' = \left(\sum_{\rho\in R}\sum_{\gamma\in C'}(-1)^{\gamma'}\rho\gamma'\right)\left(\sum_{\sigma\in S_k}(-1)^\sigma\sigma\right)$$

Mas qualquer que seja o polinômio multilinear g, temos que

$$g' = \left(\sum_{\sigma\in S_k}(-1)^\sigma\sigma\right)g$$

é antissimétrico em pelo menos 4 variáveis, e, como $\mathfrak{sl}(2, K)$ possui dimensão 3, temos $g' = 0$ identidade de $\mathfrak{sl}(2, K)$. Segue que $e_1f = 0$ é identidade fraca do par (A, L).
Agora, escreva $e_2 = e' + e''$, em que e' é combinação dos idempotentes relacionados aos diagramas com mais de m colunas.
Afirmação 2: $e'f = 0$.
De fato, se e_0 é um idempotente relacionado a um diagrama com mais de m colunas, então e_0f será simétrico em pelo menos $m + 1$ variáveis. Mas, f já é antissimétrico em conjuntos de 3 variáveis, então, o mesmo valerá para e_0f. Mas, então e_0f necessariamente terá pelo menos duas variáveis em que ele será simétrico e antissimétrico ao mesmo tempo, ou seja, $e_0f = 0$. Segue então que $e'f = 0$.
Afirmação 3: $e''f = 0$ é identidade fraca do par (A, L).
De fato, e'' é associado ao último diagrama restante



e é elementar verificar que $e''f$ é um múltiplo da linearização de f_0, e então, é identidade fraca.
Segue então que $f = 0$ é identidade fraca, provando o lema. □

Demonstração (Teorema 4.3.1). Seja $\mathscr{M} \subsetneq \mathrm{Var}(\mathfrak{sl}(2, K))$. Então existe $u(x_1, \cdots, x_l)$ identidade multilinear de $\mathscr{M}$ que não é identidade de $\mathfrak{sl}(2, K)$. Sejam $A_1, I, \mathscr{T}$ como no lema 4.3.3 e $\varphi : A_1 \to$

A_1/I a projeção canônica. Então $(\varphi(A_1), \varphi(L_1))$ é um par livre e $\varphi(L_1) = L_1/\mathscr{T}$ (por lema 4.3.3). Seja $\mathscr{M}_1 = \mathrm{Var}(\varphi(L_1))$. Então

$$\mathscr{M} \subsetneq \mathscr{M}_1 \subsetneq \mathrm{Var}(\mathfrak{sl}(2,K))$$

Afirmação 1: $\varphi(A_1)$ satisfaz uma identidade não satisfeita por $M_2(K)$.
De fato, dados $y_1, \cdots, y_{l+1} \in \varphi(A_1)$, escreva $y_1 = c_1 + v_1, \cdots, y_{l+1} = c_{l+1} + v_{l+1}$, como na proposição 3.7.5. Como

$$[u, x_{l+1}]\Big|_{x_1=c_1} = \cdots = [u, x_{l+1}]\Big|_{x_{l+1}=c_{l+1}} = 0$$

e $[u, x_{l+1}]\Big|_{x_1=v_1,\cdots,x_{l+1}=v_{l+1}} = 0$, temos que $[u, x_{l+1}] = 0$ é uma identidade forte de $\varphi(A_1)$. Como, pelo mencionado acima, $[u, x_{l+1}]$ não é identidade de $\mathfrak{sl}(2,K)$ (pois $\mathfrak{sl}(2,K)$ não tem centro), temos que $[u, x_{l+1}] = 0$ também não é identidade de $M_2(K)$, e isso prova a afirmação.
Afirmação 2: $\varphi(A_1)/J(\varphi(A_1))$ é comutativo, em que $J(\varphi(A_1))$ é o Radical de Jacobson de $\varphi(A_1)$.
De fato, $\varphi(A_1)/J(\varphi(A_1))$ é semiprimitivo e satisfaz $[u, x_{l+1}] = 0$, e então, pelo corolário 2.10.9, temos $\varphi(A_1)/J(\varphi(A_1)) \simeq \prod_{\alpha\in\mathscr{F}}^{S} M_{n_\alpha}(K)$. Em particular, cada $M_{n_\alpha}(K)$ satisfaz $[u, x_{l+1}] = 0$ (Teorema 2.2.11). Mas, se $n_\alpha > 1$, então $M_{n_\alpha}(K)$ contém uma álgebra de matrizes 2×2, e daí, pela afirmação 1, chega-se num absurdo. Segue que $n_\alpha = 1$, e então, $\varphi(A_1)/J(\varphi(A_1))$ é comutativo.
Afirmação 3: $[v_1, v_2, \cdots, v_{2m}] = 0$, para $v_1, \cdots, v_{2m} \in [\varphi(L_1), \varphi(L_1)]$ e para algum $m \in \mathbb{N}$.
De fato, considere a subálgebra A_2 de $\varphi(A_1)$ gerada por x_1, x_2, x_3. Então, A_2 é uma PI-álgebra, e daí, por teorema 3.2.9, temos $J(A_2)$ nil. Ainda, por mesmo argumento, temos $A_2/J(A_2)$ comutativo. Daí, temos $[A_2, A_2] = (\text{ideal gerado pelos comutadores}) =\subset J(A_2)$, e em particular, $[x_1, x_2] \circ x_3 \in J(A_2)$. Então, utilizando a identidade (5), temos

$$3[x_1, x_2] \circ x_3 = [x_1, x_2] \circ x_3 + [x_2, x_3] \circ x_1 + [x_3, x_1] \circ x_2 = 2\langle x_1, x_2, x_3\rangle$$

e então, $\langle x_1, x_2, x_3\rangle \in J(A_2)$ e daí é nil, e em particular, $\langle x_1, x_2, x_3\rangle$ é nil como elemento de $\varphi(A_1)$. Segue, pelo lema 4.3.4, que a álgebra A_3 gerada por $[v_1, v_2] \circ v_3$, com $v_1, v_2, v_3 \in \varphi(L_1)$ é nilpotente. Em particular, como para cada $v_1, v_2 \in [\varphi(L_1), \varphi(L_1)]$, temos $v_1 \circ v_2$ elementos de A_3, segue que existe $m \in \mathbb{N}$ tal que $(v_1 \circ v_2) \cdots (v_{2m-1} \circ v_{2m}) = 0$, e em particular, com auxílio da identidade (2) aplicada várias vezes, temos que $[v_1, \cdots, v_{2m}] = 0$, para $v_1, \cdots, v_{2m} \in [\varphi(L_1), \varphi(L_1)]$.
Afirmação 4: $\mathscr{M} \subset \mathscr{M}_1 \subset \mathscr{N}_l\mathscr{A}$.
De fato, com auxílio da identidade (2) e afirmação 3, temos

$$[v_m, v_{m-1}, \cdots, v_2, v_1] = 0$$

em $(\varphi(L_1))'$. Então $(\varphi(L_1))'$ é nilpotente, ou seja, $\varphi(L_1) \in \mathscr{N}_m\mathscr{A}$. Isso prova o teorema. □

§4.4 Base de Identidades de $M_2(K)$

O objetivo aqui é mostrar que existe um conjunto finito $\mathscr{M}$ tal que, sendo $\mathscr{P}$ o conjunto das identidades multilineares de $\mathfrak{sl}(2,K)$, $\mathscr{M} \cup \mathscr{P}$ gere todas as identidades de $M_2(K)$. Se $\mathrm{car}\, K = 0$, então existe $\mathscr{P}_0$ finito que gera $\mathscr{P}$, então, todas as identidades multilineares de $M_2(K)$ são consequências de um conjunto finito de identidades, e $M_2(K)$ admite base finita de identidades.

Seja $\mathscr{M}$ um conjunto finito de identidades de $M_2(K)$ e $\mathscr{M}_l$ o conjunto das identidades multilineares em $x_1, \cdots, x_l$. O objetivo é verificar quando $\mathscr{M}_l$ não é (ou é) consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$.

Daqui em diante, seja $f(x_1, \cdots, x_l) \in \mathscr{M}_l$ que, a princípio, não é consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$ (por enquanto, $\mathscr{M} = \emptyset$).

Observação. Podemos considerar que $f\Big|_{x_1=1} = \cdots = f\Big|_{x_l=1} = 0$.

Demonstração. Se $t \geq 0$ e $f\Big|_{x_1=1} = \cdots = f\Big|_{x_t=1} = 0$ e $f\Big|_{x_{t+1}=1} \neq 0$, então, definindo

$$g = f - f\Big|_{x_{t+1}=1} x_{t+1}$$

temos que $g\Big|_{x_1=1} = \cdots = g\Big|_{x_{t+1}=1} = 0$ e f é consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$ se e só se g é consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$, uma vez que $f\Big|_{x_{t+1}=1} \in \mathscr{M}_{l-1}$, e daí $f\Big|_{x_{t+1}=1} x_{t+1}$ é consequência de $\mathscr{M}_{l-1}$. □

Podemos escrever f como combinação linear de polinômios da forma $u_1 \cdots u_o$, com cada u_i um comutador de tamanho maior ou igual a 2.

Assuma que $\mathscr{M}$ contém as identidades, em que $v_1 = [x_1, x_2], v_2 = [x_3, x_4]$:

$$4[z, x](v_1 \circ v_2) = [z, v_1, v_2, x] + [z, v_2, v_1, x] - [x, v_1, z, v_2] - [x, v_2, z, v_1] \tag{23}$$

$$[[x_1, x_2] \circ [x_3, x_4], x_5] = 0 \tag{24}$$

Então, pela proposição 3.6.8, podemos assumir $f(x_1, \cdots, x_l) = c + v$, em que v é um polinômio de Lie e $c = \sum \beta_i (u_i' \circ [x_i, x_l])$, em que u_i' é um polinômio de Lie em $x_1, \cdots, \hat{x_i}, \cdots, x_{l-1}$ e $\beta_i \in K$.

Como já demonstrado anteriormente, sendo f uma identidade fraca (pois é identidade forte), temos c e v identidades fracas. Sendo v polinômio de Lie, temos que v é identidade forte, o que implica que c também é identidade forte.

Assuma que $\mathscr{M}$ contém uma base finita das identidades de $\mathfrak{sl}(2, K)$. Então v é consequência de $\mathscr{M}$. Temos já demonstrado a seguinte observação:

Observação. Podemos considerar $f = \sum \beta_i (u_i' \circ [x_i, x_l])$.

Lema 4.4.1. *A seguinte identidade é consequência de (24):*

$$[x_1, x_2] \circ [[x_3, x_4], x_5] = -[x_3, x_4] \circ [[x_3, x_4], x_5] \tag{25}$$

Demonstração. Segue pelas mesmas contas de (5) ser consequência de (1). □

Lema 4.4.2. *Seja $g = \sum \beta_i (u_i \circ [v_i, x_l])$, em que $\beta_i \in K$ e u_i, v_i são comutadores em $x_1, \cdots, x_{l-1}$, com tamanho de u_i maior ou igual a 2. Então g é identidade de $M_2(K)$ se e só se $\sum \beta_i [u_i, v_i]$ é identidade de $\mathfrak{sl}(2, K)$.*

Demonstração. Seja $g = \sum \beta_i (u_i \circ [v_i, x_l])$ uma identidade de $M_2(K)$. Então g é uma identidade fraca, logo, pela identidade fraca (5), temos que $\sum \beta_i [u_i, v_i] \circ x_l$ é identidade fraca de $M_2(K)$. Assuma $\sum \beta_i [u_i, v_i]$ não identidade fraca. Então, existem $h_1, \cdots, h_{l-1} \in \mathfrak{sl}(2, K)$ tais que

$$\sum \beta_i [u_i, v_i]\Big|_{x_1=h_1, \cdots, x_{l-1}=h_{l-1}} = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} \neq 0.$$

Verifica-se facilmente que

$$\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} \circ \begin{pmatrix} \alpha' & \beta' \\ \gamma' & -\alpha' \end{pmatrix} = (2\alpha\alpha' + \beta\gamma' + \gamma\beta') \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Então existe $h_l \in \mathfrak{sl}(2,K)$ tal que $\sum \beta_i[u_i,v_i]\circ x_l\Big|_{x_1=h_1,\cdots,x_l=h_l} \neq 0$, absurdo. Logo $\sum \beta_i[u_i,v_i]$ é identidade fraca de $M_2(K)$, e sendo polinômio de Lie, é identidade de $\mathfrak{sl}(2,K)$.

Reciprocamente, seja $h = \sum \beta_i[u_i,v_i]$ identidade de $\mathfrak{sl}(2,K)$. Então h é identidade fraca de $M_2(K)$, e $h\circ x_l$ também é identidade fraca, e por (5), segue que $\sum \beta_i u_i \circ [v_i,x_l]$ é identidade fraca. Como u_i é comutador de tamanho maior ou igual a 2 e $M_2(K) = \mathfrak{sl}(2,K)\oplus K$ (como espaços vetoriais), temos $\sum \beta_i u_i\circ[v_i,x_l]$ identidade de $M_2(K)$, pois todas as suas variáveis aparecem em comutadores. Assim a parte escalar zera. Isso prova o lema. □

Lema 4.4.3. *Sejam u e v polinômios de Lie em $x_1,\cdots,x_{l-1}$, com tamanho de u maior ou igual a 2. Denote, daqui adiante, o tamanho de um comutador por $\mathscr{L}(u)$. Escreva $[u,v] = \sum_{i=1}^{m}\delta_i[u_i,v_i]$, em que $[u_i,v_i]$ são comutadores básicos (c.f. seção §2.9) em $x_1,\cdots,x_{l-1}$. Então, a igualdade*

$$u\circ[v,x_l] = \sum_{i=1}^{m}\delta_i u_i\circ[v_i,x_l]$$

é consequência das identidades (24) e da identidade

$$[x_1,x_2]\circ[x_3,x_4] = [x_1,x_3]\circ[x_2,x_4] - [x_2,x_3]\circ[x_1,x_4] \tag{26}$$

Observação. Note que a identidade (26) é satisfeita por $M_2(K)$, e isso segue do lema 4.4.2 aplicado na identidade de Jacobi.

Demonstração. Antes de demonstrar, faremos duas considerações iniciais.
Afirmação 1: Podemos considerar apenas o caso em que u e v são comutadores básicos.
De fato, como os comutadores básicos formam uma base para a álgebra de Lie gerada por $X = \{x_1,x_2,\cdots\}$ pelo comutador, podemos escrever $u = \sum_{i=1}^{n_u}\alpha_i^{(u)}u_i^{(u)}$ e $v = \sum_{i=1}^{n_v}\alpha_i^{(v)}v_i^{(v)}$, com $u_i^{(u)}, v_i^{(v)}$ comutadores básicos. Escrevendo, para cada par de i,j, com $1\leq i\leq n_u, 1\leq j\leq n_v$, temos

$$[u_i^{(u)},v_j^{(v)}] = \sum_{k=1}^{n_{ij}}\delta_{ij}^k[u_{ij}^k,v_{ij}^k]$$

soma de comutadores básicos. Então, a decomposição de $[u,v]$ em comutadores básicos será

$$[u,v] = \sum_{i,j}\alpha_i^{(u)}\alpha_j^{(v)}[u_i^{(u)},v_j^{(v)}] = \sum_{i,j,k}\alpha_i^{(u)}\alpha_j^{(v)}\delta_{ij}^k[u_{ij}^k,v_{ij}^k].$$

Ainda, a validade da afirmação para cada termo $[u_i^{(u)},v_j^{(v)}]$, ou seja, provando que vale

$$u_i^{(u)}\circ[v_j^{(v)},x_l] = \sum_{k=1}^{n_{ij}}\delta_{ij}^k u_{ij}^k\circ[v_{ij}^k,x_l]$$

teremos a validade para $[u,v]$, pois

$$u\circ[v,x_l] = \sum_{i,j}\alpha_i^{(u)}\alpha_j^{(v)}u_i^{(u)}\circ[v_j^{(v)},x_l] = \sum_{i,j,k}\delta_{ij}^k\alpha_i^{(u)}\alpha_j^{(v)}u_{ij}^k\circ[v_{ij}^k,x_l].$$

Logo podemos nos restringir no caso de u e v comutadores básicos, com $\mathscr{L}(u)\geq 2$.

Afirmação 2: Podemos supor $u > v$.
De fato, se $v > u$, considere o comutador $[v, u]$. A validade para $[v, u]$, junto com a identidade (25), implicarão na validade para $[u, v]$, pois se $[v, u] = \sum_i \delta_i [u_i, v_i]$ e se $v \circ [u, x_l] = \sum_i \delta_i u_i \circ [v_i, x_l]$, então $[u, v] = \sum_i -\delta_i [u_i, v_i]$ e portanto vale

$$u \circ [v, x_l] = -v \circ [u, x_l] = \sum_i -\delta_i u_i \circ [v_i, x_l]$$

A demonstração será feita por indução em v.

Se v for tal que $[u, v]$ é um comutador básico, então o resultado vale trivialmente, pois $[u, v] = [u, v]$ já está na forma de combinação linear de comutadores básicos, e a afirmação se reduz a $u \circ [v, x_l] = u \circ [v, x_l]$, o que é trivialmente verdade.

Assuma que o resultado vale para todos os comutadores $[w_1, w_2]$, com $\mathscr{L}([w_1, w_2]) = \mathscr{L}([u, v])$, w_1 e w_2 comutadores básicos, $\mathscr{L}(w_1) \geq 2$ e $w_1 > w_2 > v$. Provaremos a validade para $[u, v]$.

Como $\mathscr{L}(u) \geq 2$, podemos escrever $u = [u_1, u_2]$. Se $u_2 \leq v$, então o comutador $[u, v]$ é básico e o resultado vale (como u é básico, temos u_1 e u_2 básicos e $u_1 > u_2$). Então, assuma $u_2 > v$. Temos $[u_1, u_2, v] = [u_1, v, u_2] - [u_2, v, u_1]$. De (26), temos

$$[u_1, u_2] \circ [v, x_l] = [u_1, v] \circ [u_2, x_l] - [u_2, v] \circ [u_1, x_l].$$

Uma vez que, se a decomposição em comutadores básicos for $[u_2, v, u_1] = \sum_j \delta''_j [w''_j, w'''_j]$ ($[u_1, v, u_2]$ é básico), então $[u_1, u_2, v] = [u_1, v, u_2] - \sum_j \delta''_j [w''_J, w'''_j]$ será a decomposição em comutadores básicos, e a validade para $[u_1, v, u_2]$ e $[u_2, v, u_1]$ implicarão na validade para $[u_1, u_2, v]$. Como $[u_1, v, u_2]$ é básico, segue sua validade.

Escreva $[u_2, v] = \sum_k \beta_k w'_k$, com w'_k comutadores básicos. Se $w'_k = u_1$, então $[w'_k, u_1] = 0$, e por (25), temos $w'_k \circ [u_1, x_l] = -u_1 \circ [w'_k, x_l] = -w'_k \circ [u_1, x_l]$. Daí $w'_k \circ [u_1, x_l] = 0$ e vale. Se $w'_k > u_1$, então, como $u_1 > u_2 > v$, vale para $[w'_k, u_1]$ por hipótese de indução. Se $w'_k < u_1$, então, como $\mathscr{L}(w'_k) = \mathscr{L}([u_2, v])$, temos $w'_k > v$, e por hipótese de indução, o resultado vale para $[u_1, w'_k]$. Então, por (25), o resultado vale também para $[w'_k, u_1]$. Logo vale para $[u_2, v, u_1]$, provando o lema. □

Lema 4.4.4. *Se vale a igualdade em $L(X)$ (a álgebra de Lie livre gerada pelo comutador pelos elementos $X = \{x_1, x_2, \cdots\}$):*

$$\sum_{i=1}^{m} \delta_i [u_i, v_i] = 0$$

com u_i, v_i comutadores em $x_1, \cdots, x_{l-1}$ e $\mathscr{L}(u_i) \geq 2$, então a identidade

$$\sum_{i=1}^{m} \delta_i u_i \circ [v_i, x_l] = 0$$

é consequência de (24) e (26).

Demonstração. Como os comutadores básicos formam uma base para $L(X)$, podemos escrever a primeira igualdade como

$$0 = \sum_{i=1}^{m} \delta_i [u_i, v_i] = \sum_{i,j} \delta_{ij} [u_i^{(j)}, v_i^{(j)}]$$

mas, sendo os comutadores básicos uma base para $L(X)$, e o somatório acima igual a zero em $L(X)$, temos $\delta_{ij} = 0, \forall i, j$. Pelo lema 4.4.3, a identidade

$$\sum_{i=1}^{m} \delta_i u_i \circ [v_i, x_l] = \sum_{i,j} \delta_{ij} u_i^{(j)} \circ [v_i^{(j)}, x_l] = 0$$

é consequência de (24) e (26). Isso prova o lema. □

Escreva a base das identidades de $\mathfrak{sl}(2, K)$ na forma $f_1 = 0$ e $f_2 = 0$, passando os comutadores a um lado. Temos que $f_i = \sum_j \beta_{ij}[u_{ij}, v_{ij}]$, com $\mathscr{L}(u_{ij}) \geq 2$, $i = 1, 2$. Defina

$$f_i' = \sum_j \beta_{ij} u_{ij} \circ [v_{ij}, y], \quad i = 1, 2$$

e tome $\mathscr{M} = \{(23), (24), (26), f_1, f_2, f_1', f_2'\}$. Dado $f \in \mathscr{M}_l$, pelas observações anteriores, reduzimos a analisar apenas o caso $f = \sum_i \beta_i u_i' \circ [x_i, x_l]$. Pelo lema 4.4.2, temos então $g = \sum_i \beta_i [u_i', x_i]$ identidade de $\mathfrak{sl}(2, K)$, e, sendo $\{f_1, f_2\}$ base das identidades, temos que

$$\sum_i \beta_i [u_i', x_i] = \sum_{i=1}^{m} \gamma_i \phi_i + \sum_{i=1}^{m'} \gamma_i' [\phi_i', v_i]$$

em que os ϕ_i, ϕ_i' são os polinômios f_1 ou f_2 com suas variáveis trocadas por polinômios de Lie e v_i são polinômios de Lie. Mas daí, temos que em $L(X)$,

$$\sum_i \beta_i [u_i', x_i] + \sum_{i=1}^{m} -\gamma_i \phi_i + \sum_{i=1}^{m'} -\gamma_i' [\phi_i', v_i] = 0$$

a partir disso, pelo lema 4.4.4, a identidade seguinte é consequência de (24) e (26)

$$h = \sum_i \beta_i u_i' \circ [x_i, x_l] + \sum_{i=1}^{m} -\gamma_i \phi_i^0 + \sum_{i=1}^{m'} -\gamma_i' \phi_i' \circ [v_i, x_l] = 0$$

em que ϕ_i^0 são polinômios f_1' ou f_2' com as mesmas trocas de variáveis e com a variável $y = x_l$. Daí h é consequência de elementos em $\mathscr{M} \cup \mathscr{M}_{l-1}$. Mas, como cada ϕ_i^0 é consequência de f_1', f_2', temos que $\sum_{i=1}^{m} -\gamma_i \phi_i^0$ é consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$. Da mesma forma, ϕ_i' são consequências de f_1 e f_2, e daí, $\sum_{i=1}^{m'} -\gamma_i' \phi_i' \circ [v_i, x_l]$ é consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$. Em particular, f é consequência de $\mathscr{M} \cup \mathscr{M}_{l-1}$. Por indução, teremos que $\mathscr{M}$ é uma base para as identidades de $M_2(K)$, e isso prova o que queríamos.

Assim, provou-se o seguinte teorema

Teorema 4.4.5. *As identidades $\mathscr{M} = \{(23), (24), (26), f_1, f_2, f_1', f_2'\}$ formam uma base de identidades de $M_2(K)$.*

Vale notar que $\mathscr{M} \subset \Gamma_4(M_2(K)) \cup \Gamma_5(M_2(K)) \cup \Gamma_6(M_2(K))$ e as identidades de Lie $f_1, f_2 \in P_5(\mathfrak{sl}(2, K))$.

§4.5 Base minimal de Identidades de $M_2(K)$

O objetivo é demonstrar o seguinte teorema:

Teorema 4.5.1. *As identidades*

$$s_4(x_1,x_2,x_3,x_4) = \tfrac{1}{2}\sum(-1)^\sigma [x_1,x_{\sigma(2)}]\circ[x_{\sigma(3)},x_{\sigma(4)}] = 0 \tag{27}$$

$$[[x_1,x_2]^2,x_1] = 0 \tag{28}$$

formam uma base minimal das identidades de $M_2(K)$.

Os teoremas provados por Razmyslov mostram que as identidades de $M_2(K)$ são consequências das identidades $\Gamma_4\cup\Gamma_5\cup\Gamma_6$, e as identidades de Lie de $\mathfrak{sl}(2,K)$ são consequências das identidades de $P_5(\mathfrak{sl}(2,K))$. Seja $\mathscr{U}$ a variedade gerada pelas identidades (27) e (28). Claro que $\mathrm{Var}(M_2(K))\subset\mathscr{U}$. Mostraremos que $\Gamma_m(M_2(K)) = \Gamma_m(\mathscr{U}), m = 4,5,6$, e isso é suficiente para concluir que $\mathscr{U} = \mathrm{Var}(M_2(K))$.

Para auxiliar nas demonstrações, vale notar as seguintes observações:

Observação. 1. Em qualquer álgebra associativa A, dados $a,b,x\in A$, vale a relação $[a\circ b,x] = [a,x]\circ b + a\circ[b,x]$. De fato, temos

$$\begin{aligned}[a\circ b,x] &= abx + bax - xab - xba\\ [a,x]\circ b &= axb + bax - xab - bxa\\ a\circ[b,x] &= abx - axb + bxa - xba\end{aligned}$$

e somando as duas últimas, obtemos que é igual a primeira equação e vale a afirmação.

2. Se f é um polinômio que gera um S_n-módulo irredutível, e queremos mostrar que f é consequência de g, então, podemos assumir que os demais S_n-módulos irredutíveis "são nulos". Isso se deve ao seguinte fato: se consideramos o espaço $\Gamma_n/(T(g)\cap\Gamma_n)$, o espaço dos polinômios multilineares próprios de grau n quocientado pelas identidades multilineares próprios que são consequências de g, então nesse espaço, se mostrarmos que f é consequência de polinômios em algum S_n-módulo irredutível M não isomorfo a $(KS_n)f$, então teremos $f\in M\cap(KS_n)f = 0$ (uma vez que ambos são irredutíveis e não isomorfos), ou seja, f é nulo no espaço $\Gamma_n/(\Gamma_n\cap T(g))$, o que implica que $f\in T(g)$, ou seja, f é consequência de g. Informalmente, ao tentarmos mostrar que uma dada identidade f é consequência de (27) ou (28), podemos assumir que os demais S_n-módulos irredutíveis não isomorfos a $(KS_n)f$ são nulos, e então, podemos assumir as suas identidades.

3. Pela teoria de módulos completamente redutíveis, temos $\Gamma_n \simeq \Gamma_n(A)\oplus(\Gamma_n\cap T(A))$, ainda, dado um S_n-módulo irredutível, a quantidade de vezes que ele aparece na decomposição de $\Gamma_n(A)$, somando com a quantidade de vezes que ele aparece como identidades polinomiais (em $\Gamma_n\cap T(A)$), deve resultar na quantidade de vezes que ele aparece em Γ_n.

Lema 4.5.2. $\Gamma_5(\mathscr{U}) = \Gamma_5(M_2(K))$

Demonstração. Utilizaremos a notação e a decomposição de Γ_5 dada na proposição 3.5.11, e basta provarmos que os polinômios que são identidades de $M_2(K)$ são consequências das identidades (27) e (28). Utilizando a proposição 3.6.4, obtemos que os polinômios y_5 e y_9 são identidades de $M_2(K)$, e aplicando o Teorema 3.6.8.(i), segue que y_3 e y_5 são as identidades de Lie de $M_2(K)$ e y_1,y_2,y_4 não

são identidades. Aplicando o Teorema 3.6.8.(ii), segue que y_7 não é identidade de $M_2(K)$ (pois na composição de $\Gamma_n(M_2(K))$ deve entrar um S_n-módulo isomorfo a cada partição $(p+q+r, p+q, p)$ satisfazendo as dadas condições, e sabemos que (as linearizações de) y_2 e y_5 são os geradores dos S_5-módulos irredutíveis correspondentes às partições $(3,2)$ e $(2,2,1)$). Então, basta verificar se y_6 e y_8 são identidades, e, substituindo por matrizes genéricas, vemos que de fato são identidades (provaremos formalmente que ambas são identidades, ao mostrarmos que elas são consequências das identidades (27) e (28)).

Então, mostraremos que y_3, y_5, y_6, y_8, y_9 são consequências de (27) e (28):

y_3**:**

$$\begin{aligned} s_4(x_1^2, x_1, x_2, x_3) &= [x_1^2, x_2] \circ [x_3, x_1] + [x_1^2, x_3] \circ [x_1, x_2] \\ &= ([x_1, x_2] \circ x_1) \circ [x_3, x_1] + ([x_1, x_3] \circ x_1) \circ [x_1, x_2] \\ &= x_1([x_1, x_2][x_3, x_1] + [x_1, x_3][x_1, x_2]) + ([x_3, x_1][x_1, x_2] + [x_1, x_2][x_1, x_3])x_1 \\ &= [x_1, x_2, [x_1, x_3], x_1] \\ &= -[x_2, x_1, x_1, [x_1, x_3]] - \underbrace{[x_2, x_1, [x_1, x_3, x_1]]}_{-[x_1, x_3, x_1, [x_2, x_1]]} = \frac{1}{2} y_3(x_1, x_2, x_3) \end{aligned}$$

y_6 :

$$\begin{aligned} y_6(x_1, x_2) &= [x_2, x_1, x_1] \circ [x_2, x_1] = ([x_2, x_1]x_1 - x_1[x_2, x_1]) \circ [x_2, x_1] \\ &= [x_2, x_1]x_1[x_2, x_1] + [x_2, x_1]^2 x_1 - x_1[x_2, x_1]^2 - [x_2, x_1]x_1[x_2, x_1] = [[x_2, x_1]^2, x_1] \end{aligned}$$

y_8 :

$$s_4([x_1, x_2], x_1, x_2, x_3) = \frac{1}{2} \sum_{\sigma \in S_3} (-1)^\sigma [x_2, x_1, x_{\sigma(1)}] \circ [x_{\sigma(2)}, x_{\sigma(3)}] = y_8(x_1, x_2, x_3)$$

y_9 :

$$\begin{aligned} [s_4(x_1, x_2, x_3, x_4), x_1] &= \left[\frac{1}{4} \sum (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}] \circ [x_{\sigma(3)}, x_{\sigma(4)}], x_1 \right] \\ &= \frac{1}{2} \sum (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}, x_1] \circ [x_{\sigma(3)}, x_{\sigma(4)}] = y_9(x_1, x_2, x_3, x_4) \end{aligned}$$

y_5 : Sabendo que a identidade y_9 é consequência das identidades (27) e (28) e utilizando a observação acima, podemos realizar nossos cálculos módulo o espaço $N = \sum_{i=6}^{9} (KS_5) \operatorname{lin} y_i = (KS_5)[x_1, x_2, x_3] \circ [x_4, x_5]$ (proposição 3.5.11). Nós temos

$$\begin{aligned} 2s_4(x_1 \circ u, x_2, x_3, x_4) &= \sum (-1)^\sigma [x_1 \circ, x_{\sigma(2)}] \circ [x_{\sigma(3)}, x_{\sigma(4)}] \\ &= \sum (-1)^\sigma ([x_1, x_{\sigma(2)}] + [x_1, x_{\sigma(2)}] \circ u + x_1 \circ [u, x_{\sigma(2)}]) \circ [x_{\sigma(3)}, x_{\sigma(4)}] \\ &= \sum (-1)^\sigma (2u[x_1, x_{\sigma(2)}] + [x_1, x_{\sigma(2)}, u] + 2x_1[u, x_{\sigma(2)}] + [u, x_{\sigma(2)}, x_1]) \circ [x_{\sigma(3)}, x_{\sigma(4)}] \\ &\equiv 2 \sum (-1)^\sigma (u[x_1, x_{\sigma(2)}] \circ [x_{\sigma(3)}, x_{\sigma(4)}] + [x_{\sigma(3)}, x_{\sigma(4)}, u][x_1, x_{\sigma(2)}] + \\ &\quad + x_1[u, x_{\sigma(2)}] \circ [x_{\sigma(3)}, x_{\sigma(4)}] + [x_{\sigma(3)}, x_{\sigma(4)}, x_4][u, x_{\sigma(2)}]) \\ &\equiv 2 \sum (-1)^\sigma ([x_{\sigma(3)}, x_{\sigma(4)}, u][x_1, x_{\sigma(2)}] + [x_{\sigma(3)}, x_{\sigma(4)}, x_1][u, x_{\sigma(2)}]) \end{aligned}$$

então, em particular, $2\sum_{i=1}^{4} s_4(x_1, \cdots, x_i \circ u, \cdots, x_4) = 2\sum(-1)^\sigma [x_{\sigma(3)}, x_{\sigma(4)}, u][x_{\sigma(2)}, x_{\sigma(3)}]$, e então, y_5 é consequência de (27) e (28).

□

Observação. Em particular, pela demonstração feita acima, as identidades de Lie de $PL_5(M_2(K))$ são consequências da identidade standard s_4.

Lema 4.5.3. $\Gamma_6(\mathscr{U}) = \Gamma_6(M_2(K))$

Demonstração. Utilizaremos muitas vezes as observações feitas no início desta seção, e iremos procurar quais dos polinômios (ou combinação dos polinômios) na decomposição de Γ_6 (proposição 3.5.12) são identidades de $M_2(K)$, utilizando as matrizes genéricas.

Sabemos que as identidades de Lie de grau 6 são consequências das identidades de Lie de grau 5, e então, qualquer identidade de $M_2(K)$ de Lie de grau 6 será consequência das identidades (27) e (28). Daí, basta verificarmos as identidades multilineares próprias que não são de Lie. Ainda, podemos trabalhar nos espaços quocientados por polinômios de Lie - pois se mostrarmos que um dado polinômio h em é equivalente a um polinômio de Lie em $\Gamma_n(\mathscr{U})$, então h será identidade de $M_2(K)$ se e só se for identidade em $\mathscr{U}$.

(4,2) Pelo teorema 3.6.8.(i), temos que todos os S_6-módulos irredutíveis de Lie relativos à partição $(4, 2)$ são identidades de $M_2(K)$, e então, pelo mesmo teorema 3.6.8.(ii), temos que necessariamente existirá exatamente um S_6-módulo irredutível (de polinômios próprios não de Lie) relativo à partição $(4, 2)$ que consistirá apenas de identidades de $M_2(K)$, e exatamente um que não conterá nenhuma identidade de $M_2(K)$. Ainda, novamente pelo teorema 3.6.8, o gerador desse S_6-módulo irredutível de identidades será alguma identidade da forma $az_1+bz_2 = 0$, para algum $a, b \in K$ (não exclui a possibilidade $a = 0$ ou $b = 0$, ou seja, z_1 ou z_2 serem geradores do espaço), pois os dois polinômios, se não identidades, são equivalentes em $\Gamma_6(M_2(K))$. Então, se mostrarmos que, em $\Gamma_6(\mathscr{U})$, z_1 é equivalente a z_2, então obteremos que a única identidade $az_1 + bz_2 = 0$ em $\Gamma_6(M_2(K))$ módulo PL_6 é consequência de (27) e (28).

Temos, linearizando a variável x_2 de (28), e substituindo uma das variáveis obtidas por $[x_2, x_1]$:

$$[[x_2, x_1, x_1] \circ [x_2, x_1], x_1] = [x_2, x_1, x_1, x_1] \circ [x_2, x_1] + [x_2, x_1, x_1] \circ [x_2, x_1, x_1] = 2(z_1 + z_2)$$

e então, o polinômio $z_1 + z_2$ é consequência de (27) e (28), e isso implica (pelos comentários acima) que $z_1 + z_2 = 0$ é a única identidade de $M_2(K)$ (a menos de equivalência) próprio, não de Lie e relativo a partição $(4, 2)$, e essa identidade é consequência de (27) e (28).

(4,1,1) Utilizamos a identidade de grau 5, denotada por y_3 e obtemos

$$\begin{aligned}
&y_3(x_1, x_1 \circ x_2, x_3) = 2([x_1 \circ x_2, x_1, x_1, [x_3, x_1]] - [x_3, x_1, x_1, [x_1 \circ x_2, x_1]]) \\
&= 2([x_1 \circ [x_2, x_1, x_1], [x_3, x_1]] - [x_3, x_1, x_1, x_1 \circ [x_2, x_1]]) \\
&= 2([x_1, [x_3, x_1]] \circ [x_2, x_1, x_1] - [x_3, x_1, x_1, x_1] \circ [x_2, x_1] + \\
&\quad + x_1 \circ ([x_2, x_1, x_1, [x_3, x_1]] - [x_3, x_1, x_1, [x_2, x_1]])) \\
&= -2([x_3, x_1, x_1, x_1] \circ [x_2, x_1] + [x_3, x_1, x_1] \circ [x_2, x_1, x_1]).
\end{aligned}$$

Então, temos

$$y_3(x_1, x_1 \circ x_2, x_3) - y_3(x_1, x_1 \circ x_3, x_2) = 2([x_2, x_1, x_1, x_1] \circ [x_3, x_1] - [x_3, x_1, x_1, x_1] \circ [x_2, x_1])$$
$$= 2(\underbrace{2[x_3, x_1][x_2, x_1, x_1, x_1] - 2[x_2, x_1][x_3, x_1, x_1, x_1]}_{z_3(x_1,x_2,x_3)}) -$$
$$- \underbrace{4([[x_3, x_1], [x_2, x_1, x_1, x_1]] - [[x_2, x_1], [x_3, x_1, x_1, x_1]])}_{\in PL_6}.$$

Logo, a menos de polinômios de Lie, z_3 é consequência de (27) e (28).

(3,3) Temos que os polinômios de Lie correspondentes a essa partição são identidades de $M_2(K)$, pelo teorema 3.6.8, e ainda por esse teorema, segue que necessariamente z_4 não é identidade de $M_2(K)$. Então, nada a fazer aqui.

(3,2,1) Identidade z_5:

$$s_4([x_2, x_1, x_1], x_1, x_2, x_3) = \frac{1}{2}\sum (-1)^\sigma [x_2, x_1, x_1, x_{\sigma(1)}] \circ [x_{\sigma(2)}, x_{\sigma(3)}]$$
$$= \frac{1}{2}\underbrace{\sum (-1)^\sigma [x_2, x_1, x_1, x_{\sigma(1)}][x_{\sigma(2)}, x_{\sigma(3)}]}_{z_5(x_1,x_2,x_3)} + \frac{1}{2}\sum (-1)^\sigma \underbrace{[x_{\sigma(2)}, x_{\sigma(3)}][x_2, x_1, x_1, x_{\sigma(1)}]}_{[x_2,x_1,x_1,x_{\sigma(1)}][x_{\sigma(2)},x_{\sigma(3)}]+[[x_2,x_1,x_1,x_{\sigma(1)}],[x_{\sigma(2)},x_{\sigma(3)}]]}$$
$$= z_5 + w$$

em que $w \in PL_6$. Daí, z_5 pode ser ou pode não ser uma identidade de $M_2(K)$, mas caso seja, será consequência de (27) e (28), pelo mencionado no início da demonstração.

Identidade z_6: todas as identidades de grau 5 de $M_2(K)$ são consequências de (27) e (28), então, podemos utilizá-las livremente: da identidade de Hall $[[x_1, x_2]^2, x_3]$, obtemos (utilizando a relação $[a \circ b, x] = [a, x] \circ b + a \circ [b, x]$):

$$[[x_1, x_2]^2, [x_1, x_3]] = \frac{1}{2}[[x_1, x_2] \circ [x_1, x_2], [x_1, x_3]] = [x_1, x_2, [x_1, x_3]] \circ [x_1, x_2]$$
$$= 2[x_1, x_2]\underbrace{[x_1, x_2, [x_1, x_3]]}_{-[x_3,x_1,[x_2,x_1]]} + [[x_1, x_2, [x_1, x_3]], [x_1, x_2]] = -2z_6 + w$$

em que $w \in PL_6$.

Identidade z_7: considere, na notação da proposição 3.6.4, o S_6-submódulo $N_2+N_3 = (KS_6)[x_1, x_2][x_3, x_4, x_5, x_6]$. As identidades $y_5 = \sum(-1)^\sigma [[x_{\sigma(1)}, x_{\sigma(2)}, x_1], [x_{\sigma(3)}, x_{\sigma(4)}]]$ e $y_9 = \sum(-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}, x_1] \circ [x_{\sigma(3)}, x_{\sigma(4)}]$ são de grau 5. Somando ambas, obtemos a identidade (que será consequência de (27) e (28)):

$$\frac{1}{2}(y_5 + y_9) = \sum (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}, x_1][x_{\sigma(3)}, x_{\sigma(4)}].$$

Substituindo a variável x_4 por $[x_2, x_1]$, obtemos

$$\frac{1}{2}(y_5 + y_9) \equiv \underbrace{\sum (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}, x_1][x_{\sigma(3)}, [x_2, x_1]]}_{z_7(x_1,x_2,x_3)} (\mathrm{mod}\, N_2 + N_3)$$

e segue que z_7 é consequência de (27) e (28), pelas observações iniciais.

(3,1,1,1) Identidade z_{10}: considere a identidade de grau 5

$$h(x_1,x_2,x_3,x_4,x_5)=\sum(-1)^\sigma[x_{\sigma(1)},x_{\sigma(2)},x_5,[x_{\sigma(3)},x_{\sigma(4)}]]$$

(é identidade, pois é próprio e antissimétrico em 4 variáveis, c.f. demonstração da proposição 3.6.4), e é consequência de (27) e (28) (pois toda identidade de grau 5 é consequência de (27) e (28)). Então, substituindo a variável x_5 por x_1^2, obtemos

$$\begin{aligned}&\frac{1}{2}\sum(-1)^\sigma[[x_{\sigma(1)},x_{\sigma(2)},x_1\circ x_1],[x_{\sigma(3)},x_{\sigma(4)}]]=\sum(-1)^\sigma[[x_{\sigma(1)},x_{\sigma(2)},x_1]\circ x_1,[x_{\sigma(3)},x_{\sigma(4)}]]\\&=\underbrace{\sum(-1)^\sigma[[x_{\sigma(1)},x_{\sigma(2)},x_1,[x_{\sigma(3)},x_{\sigma(4)}]]\circ x_1}_{h(x_1,x_2,x_3,x_4,x_1)\circ x_1}+\sum(-1)^\sigma[x_{\sigma(1)},x_{\sigma(2)},x_1]\circ[x_1,[x_{\sigma(3)},x_{\sigma(4)}]\end{aligned}$$

e daí z_{10} é consequência de (27) e (28).

Identidade z_8: considere o espaço $N_4=(KS_6)[x_1,x_2,x_3][x_4,x_5,x_6]$. Então

$$\begin{aligned}[s_4(x_1,x_2,x_3,x_4),x_1,x_1]=&\frac{1}{2}\left(\underbrace{\sum(-1)^\sigma[x_{\sigma(1)},x_{\sigma(2)}]\circ[x_{\sigma(3)},x_{\sigma(4)},x_1,x_1]}_{z_8}\right)+\\&+\frac{1}{2}\left(\sum(-1)^\sigma\underbrace{[x_{\sigma(1)},x_{\sigma(2)},x_1]\circ[x_{\sigma(3)},x_{\sigma(4)},x_1]}_{\in N_4}\right)\end{aligned}$$

e então, pelos comentários no início desta demonstração, z_8 é consequência de (27) e (28).

Identidade z_9: considere o espaço $N_4=(KS_6)[x_1,x_2,x_3][x_4,x_5,x_6]$. Então

$$\sum(-1)^\sigma s_4(x_1,x_{\sigma(2)},[x_{\sigma(3)},x_1],[x_{\sigma(4)},x_1])\equiv z_9(x_1,x_2,x_3,x_4)(\mathrm{mod}\,N_4)$$

e daí, do mesmo modo, z_9 é consequência de (27) e (28).

(2,2,2) Será utilizada a mesma ideia da partição $(4,2)$ aqui: mostraremos que z_{11} é equivalente a z_{12}. Considere o espaço $N_4=KS_6[x_1,x_2,x_3][x_4,x_5,x_6]$ (que contém o S_6-módulo irredutível gerado por (linearização de) z_{12}). Então

$$\begin{aligned}s_4([x_1,x_2],[x_3,x_4],x_5,x_6)&=[x_1,x_2,[x_3,x_4]]\circ[x_5,x_6]\\&=[x_5,x_6][x_1,x_2,[x_3,x_4]]-[[x_5,x_6],[x_1,x_2,[x_3,x_4]]]\end{aligned}$$

e então, a menos de polinômios de Lie, fazendo uma soma adequada, temos que z_{11} é equivalente a z_{12} em $\mathscr{U}$.

(2,2,1,1) Claro que z_{13} é consequência de s_4.

Identidade z_{14}: segue de $[s_4(x_1,x_2,x_3,x_4),[x_2,x_1]]$, utilizando $s_4=\frac{1}{4}\sum(-1)^\sigma[x_{\sigma(1)},x_{\sigma(2)}]\circ[x_{\sigma(3)},x_{\sigma(4)}]$ e a relação $[a\circ b,x]=a\circ[b,x]+[a,x]\circ b$.

(2,1,1,1,1) Considere a identidade de grau 5 (toda identidade de grau 5 é consequência de (27) e (28)):

$$g(x_1,x_2,x_3,x_4,x_5)=\sum(-1)^\sigma[x_{\sigma(1)},x_{\sigma(2)}][x_{\sigma(3)},x_{\sigma(4)},x_5].$$

Claro que esse polinômio é uma identidade de $M_2(K)$, pois é próprio e antissimétrico em 4 variáveis, c.f. argumento da proposição 3.6.4. Substituindo a variável x_5 por $[x_{\sigma(5)}, x_1]$ e somando com respeito a $\sigma \in S_5$ obtemos z_{15}, formalmente:

$$\sum_{\sigma \in S_5} (-1)^\sigma f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}, [x_{\sigma(5)}, x_1]) = (n-1)! z_{15}$$

(1,1,1,1,1,1) Temos que s_6 é consequência de s_4.

□

Com isso, como $\operatorname{car} K = 0$, todas as identidades de $M_2(K)$ seguem de $\Gamma_m(M_2(K))$, e ainda, podemos nos restringir para $m = 4, 5, 6$. Ainda, as identidades dessa restrição seguem de (27) e (28), pelo que foi provado agora, e isso prova o teorema. Uma base de identidades para o caso de característica $p > 0$, $p \neq 2$, foi encontrada por Koshlukov em 2001 (sendo essa base minimal para $p \neq 3$), vide [41].

Bibliografia

[1] Amitsur, S. A. "The identities of PI-rings." Proceedings of the American Mathematical Society 4.1 (1953): 27-34.

[2] Amitsur, S. A. "Algebras over infinite fields." Proceedings of the American Mathematical Society 7.1 (1956): 35-48.

[3] Amitsur, S. A. "A generalization of Hilbert's Nullstellensatz." Proceedings of the American Mathematical Society 8.4 (1957): 649-656.

[4] Atiyah, M. F., and I. G. Macdonald. Introduction to commutative algebra. Vol. 2. Reading: Addison-Wesley, 1969.

[5] Bahturin, Yu. A. Identical relations in Lie algebras. Utrecht: VNU Science Press, 1987.

[6] Bergman, G. M. "A ring primitive on the right but not on the left." Proceedings of the American Mathematical Society 15.3 (1964): 473-475.

[7] Cameron, P. J. Introduction to algebra. Oxford University Press, 1998.

[8] Curtis, C. W., and I. Reiner. Representation theory of finite groups and associative algebras. Vol. 356. AMS Bookstore, 1962.

[9] Drensky, V. S. Free algebras and PI-algebras: graduate course in algebra. Singapore: Springer, 2000.

[10] Drensky, V. S. "Representations of the symmetric group and varieties of linear algebras." Matematicheskii Sbornik 157.1 (1981): 98-115.

[11] Drensky, V. S. "A minimal basis of identities for a second-order matrix algebra over a field of characteristic 0." Algebra and Logic 20.3 (1981): 188-194.

[12] Dubnov, J., and V. Ivanov. "Sur l'abaissement du degré des polynômes en affineurs", CR (Doklady) Acad. Sci. USSR 41 (1943): 96-98.

[13] Endler, O. Teoria dos corpos. Instituto nacional de matemática pura e aplicada (IMPA), 2005.

[14] Garcia, A., and Y. Lequain. Elementos de álgebra. Instituto de Matematica Pura e Aplicada, 2008.

[15] Giambruno, A., and M. Zaicev. Polynomial identities and asymptotic methods. Vol. 122. AMS Bookstore, 2005.

[16] Iltyakov, A. "On finite basis of identities of Lie algebra representations." Nova J. Algebra Geom. 1 (1992), no. 3, pp. 207-259.

[17] Kaplansky, I. "Rings with a polynomial identity." Bulletin of American Mathematical Society, vol. 54 (1948), pp. 575-580.

[18] Hall, M. "A basis for free Lie rings and higher commutators in free groups." Proceedings of the American Mathematical Society 1.5 (1950): 575-581.

[19] Nagata, M. "On the nilpotency of nil-algebras." Journal of the Mathematical Society of Japan 4.3-4 (1952): 296-301.

[20] Herstein, I. N. "Noncommutative rings, Carus Math." Monographs, Math. Assoc. of America (1968).

[21] Herstein, I. N. Topics in algebra. Wiley. com, 2006.

[22] Higman, G., and P. Hall. "On a conjecture of Nagata." Mathematical Proceedings of the Cambridge Philosophical Society. Vol. 52. No. 01. Cambridge University Press, 1956.

[23] Hoffman, K., and R. Kunze. "Linear Algebra". 1971.

[24] Jacobson, Nathan. Structure of rings. AMS Bookstore, 1956.

[25] Lambek, J. Lectures on rings and modules. Vol. 283. AMS Bookstore, 2009.

[26] Levitzki, J. "A Theorem of Polynomial Identities." Proceedings of the American Mathematical Society 1.3 (1950): 334-341.

[27] Northcott, D. G. Multilinear algebra. Cambridge: Cambridge University Press, 1984.

[28] Razmyslov, Ju P. "On a problem of Kaplansky." Izvestiya: Mathematics 7.3 (1973): 479-496.

[29] Razmyslov, Yu P. "On Lie algebras satisfying the Engel condition." Algebra and Logic 10.1 (1971): 21-29.

[30] Razmyslov, Yu P. "An example of unsolvable just non-cross varieties of groups." Algebra and Logic 11.2 (1972): 108-120.

[31] Razmyslov, Yu P. "Finite basing of the identities of a matrix algebra of second order over a field of characteristic zero." Algebra and Logic 12.1 (1973): 47-63.

[32] Rotman, J. J. Advanced modern algebra. AMS Bookstore, 2002.

[33] San Martin, L. A. "Algebras de Lie." Editorial UNICAMP, Campinas, SP (1999).

[34] Santos, J. P. O. "Teoria dos Números." Rio de Janeiro: IMPA (2009).

[35] Serre, J.-P. "Linear representations of finite groups." New York (1977).

[36] Van der Waerden, B. L. "Modern algebra, vol. I." Ungar: New York (1949).

Leitura extra:

[37] Baer, R. "Radical ideals." American Journal of Mathematics 65.4 (1943): 537-568.

[38] Braun, A. "The nilpotency of the radical in a finitely generated PI ring." Journal of Algebra 89.2 (1984): 375-396.

[39] Filippov, V. T. "Varieties of Mal'tsev algebras." Algebra and Logic 20.3 (1981): 200-210.

[40] Kemer, A. R. "Capelli identities and nilpotency of the radical of finitely generated PI-algebra." Dokl. Akad. Nauk SSSR. Vol. 255. No. 4. 1980.

[41] Koshlukov, P. "Basis of the Identities of the Matrix Algebra of Order Two over a Field of Characteristic $p \neq 2$." Journal of Algebra 241.1 (2001): 410-434.

[42] Razmyslov, Yu P. "The Jacobson radical in PI-algebras." Algebra and Logic 13.3 (1974): 192-204.

[43] Specht, W. "Gesetze in Ringen. I." Mathematische Zeitschrift 52.1 (1950): 557-589.

[44] Vaughan-Lee, M. R. "Varieties of Lie algebras." The Quarterly Journal of Mathematics 21.3 (1970): 297-308.

Dissertações:

[45] Freitas, J. A. O. Identidades polinomiais para a álgebra das matrizes de ordem dois sobre corpos de característica zero. 2006. 107p. Dissertação (Mestre) - Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2006.

[46] Silva, D. D. P. Álgebras graduadas e identidades polinomiais graduadas. 2007. 79f. Dissertação (Mestre) - Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2007

Índice