Miqueias de Melo Lobo

O Teorema de Posner para PI-álgebras Graduadas *gr*-Primas

CAMPINAS
2015

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

MIQUEIAS DE MELO LOBO

O TEOREMA DE POSNER PARA PI-ÁLGEBRAS GRADUADAS *gr*-PRIMAS

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: Lucio Centrone

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO MIQUEIAS DE MELO LOBO, E ORIENTADA PELO PROF. DR. LUCIO CENTRONE.

Assinatura do Orientador

CAMPINAS

2015

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

L786t

Lobo, Miqueias de Melo, 1990-
O teorema de Posner para PI-álgebras graduadas gr-primas / Miqueias de Melo Lobo. – Campinas, SP : [s.n.], 2015.

Orientador: Lucio Centrone.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Identidade polinomial. 2. Álgebras graduadas. 3. PI-álgebras. I. Centrone, Lucio,1983-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: The Posner's theorem for graded PI-algebras gr-primes
Palavras-chave em inglês:
Polynomial identity
Graded algebras
PI-algebras
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Lucio Centrone [Orientador]
Viviane Ribeiro Tomaz da Silva
Francesco Matucci
Data de defesa: 15-05-2015
Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 15 de maio de 2015 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof.(a). Dr(a). FRANCESCO MATUCCI

Prof.(a). Dr(a). VIVIANE RIBEIRO TOMAZ DA SILVA

Abstract

In this work we study algebras with polynomial identities. More specifically, we study the main structure theorems for graded PI-algebras and including the graded version of Posner's theorem, obtained by Balaba in 2005, which paved the way for several important applications in recent years.

Resumo

Neste trabalho estudamos álgebras com identidades polinomiais. Mais especificamente, estudamos os principais teoremas de estrutura das PI-álgebras graduadas e entre eles a versão graduada do teorema de Posner, obtida por Balaba em 2005, que abriu o caminho para diversas aplicações importantes nos últimos anos.

Sumário

Aos meus pais.

Agradecimentos

Antes de tudo eu agradeço a Deus por, em sua infinita bondade, ter me feito chegar até aqui.

Agradeço à minha querida esposa por ter sido tão compreensiva e motivadora durante esses dois anos de mestrado, aos meus pais e aos meus irmãos pela dedicação e incentivo que sempre me deram.

Não posso esquecer de externar minha gratidão ao meu orientador Professor Dr. Lucio Centrone pela paciência, pela excelente orientação mostrando-se sempre disponível e uma pessoa inspiradora independente de suas muitas ocupações. Nesta mesma linha, sou grato aos membros da banca pelas correções apontadas e também pelas valiosas sugestões que, sem dúvida nenhuma, contribuíram significativamente para o enriquecimento deste trabalho.

Agradeço ao meu grande amigo Ramon Códamo por aceitar o desafio de deixar o Amazonas e vir comigo morar em São Paulo, dando o primeiro passo na direção de tornar-se um algebrista. Também sou grato ao Claudemir Fidelis (UFCG) pelas muitas discussões a respeito de PI-álgebras. Agradeço ainda a todos os meus colegas de mestrado que ajudaram de alguma forma para o meu êxito acadêmico, em especial, aos meus colegas de república Carlos Bassani, Leonardo Soriani e ao Osmar Rogério Reis Severiano (o Murriquinha) por ter se mostrado um amigo nos momentos em que mais precisei e também ao Valter Moitinho pelos bons conselhos (e pelos maus também).

Por fim, meus sinceros agradecimentos à CAPES pelo auxílio financeiro, sem o qual tudo isso se tornaria bem mais difícil.

Introdução

Álgebras com identidades polinomiais representam um importante ramo da teoria de anéis que começa como um campo de estudo bem definido no ano de 1948 com um artigo publicado por Kaplansky no qual se prova que uma álgebra primitiva com identidade polinomial é simples e dimensão finita sobre o seu centro.

Este é um momento oportuno para se dizer o que se entende por "identidade polinomial" em álgebras. Dada uma álgebra A e um polinômio $f(X_1, \ldots, X_n)$ nas variáveis não-comutativas $X_1, \ldots, X_n$, diz-se que f é uma *identidade* de A se $f(a_1, \ldots, a_n) = 0$ para todas as substituições $a_1, \ldots, a_n$ em A. Se f é uma identidade de A, também dizemos que A satisfaz f. Uma PI-álgebra é uma álgebra satisfazendo uma identidade não-nula. Por exemplo, se uma álgebra é comutativa então $ab = ba$ (equivalentemente $ab - ba = 0$) quaisquer que sejam os elementos a e b dessa álgebra. Ou seja, toda álgebra comutativa satisfaz a identidade polinomial $f(X, Y) = XY - YX$.

O objeto de estudo deste trabalho são estas álgebras que satisfazem uma identidade polinomial que, na verdade, são investigadas muito antes de 1948, a saber, desde o início do século passado. De fato, os artigos de Dehn em 1922 ([6]) e Wagner em 1937 ([20]) esclareceram porque, em um plano projetivo, a resolubilidade do Teorema de Desargue é equivalente ao plano satisfazer uma identidade polinomial. Depois de alguns anos, o trabalho de Amitsur e Levitzki acerca de identidades de grau mínimo para a álgebra das matrizes, o trabalho de Kaplansky e o de Posner abriram as portas para um estudo mais detalhado da área em um sentido mais algébrico.

Um dos resultados clássicos (e mais importantes) relacionados à estrutura das PI-álgebras, é o teorema de Posner que afirma que uma PI-álgebra prima A tem uma álgebra de quocientes $Q(A)$ simples e de dimensão finita sobre o seu centro, além disso A e $Q(A)$ satisfazem as mesmas identidades polinomiais.

As questões históricas levantadas acima fazem referência a resultados clássicos das PI-álgebras. Pode-se perguntar: *O que, de destaque, se tem estudado recentemente que esteja relacionado com os teoremas citados acima?* "Álgebras com uma estrutura graduada por grupo" é uma boa resposta. E o que se entende por isso?

Dada uma álgebra A e um grupo multiplicativo G, a álgebra A é dita *graduada por* G (ou G-graduada) se existir uma família $\{A_g \mid g \in G\}$ de subespaços de A para os quais vale que $A = \bigoplus_{g \in G} A_g$ e $A_g A_h \subseteq A_{gh}$, quaisquer que sejam $g, h \in G$.

Nos últimos anos, álgebras com uma estrutura graduada por grupo tornaram-se cada vez mais atraentes. Por exemplo, o problema de Specht, que foi um das questões em aberto mais importantes da PI-teoria, respondido por Kemer no caso em que F é um corpo de característica 0, foi resolvido também para o caso graduado por grupos abelianos finitos graças ao trabalho de

Sviridova e finalmente teve sua solução completa (com graduação por qualquer grupo) graças ao trabalho de Aljadeff e Belov.

O teorema de Posner também possui uma versão graduada e tem tido vastas aplicações. O principal objetivo desta dissertação é estudar o artigo ([2]) no qual Balaba apresenta uma demonstração para tal versão do teorema de Posner.

Para estudar o artigo supracitado foi necessário desenvolver um pouco a teoria básica das PI-álgebras e apresentar os teoremas clássicos de estrutura mais importantes como o teorema de Kaplansky e o teorema de Rowen. Esse é o conteúdo dos dois primeiros capítulos desta dissertação. Os principais resultados encontram-se no último capítulo onde é feito um paralelo com o Capítulo 2 a fim de tornar mais curta, na medida do possível, a apresentação feita alí.

Capítulo 1

Conceitos Básicos e Exemplos

Este primeiro capítulo segue o roteiro dos livros [13] e *Polynomial Identities in Ring Theory* ([17]) de Rowen. Aliás, boa parte das notações utilizadas neste trabalho seguem as notações de Rowen no segundo livro citado acima.

Formalmente, o pré-requisito necessário para a leitura deste trabalho é um conhecimento equivalente ao conteúdo dos Capítulos 3, 4 e 5 do livro *Topics in Algebra* ([10]) o qual é usado como referência padrão. Para nós *anel* significará "anel associativo com unidade 1". Os símbolos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ denotam, respectivamente, o anel dos números inteiros, o corpo dos números racionais, o corpo dos números reais e o corpo dos números complexos.

Para representar o conjunto $\{1, 2, 3, \ldots\}$ reservamos o símbolo $\mathbb{Z}^+$. Além disso, *ideal* significará "ideal bilateral" e $I \lhd R$ é a notação usada para dizer que I é um ideal do anel R. Quando houver necessidade de citar ideais à direita (resp. à esquerda) vamos escrever $I \lhd_r R$ (resp. $I \lhd_l R$). Aqui *módulo* significa "módulo unitário", isto é, sendo M um módulo sobre o anel R, tem-se $1m = m$ para todo $m \in M$, onde 1 é a unidade de R. Para qualquer homomorfismo ψ de módulos ou de anéis, $ker(\psi)$ denota o *núcleo* de ψ, a pré-imagem de 0; ψ é injetivo se $ker(\psi) = (0)$ e um homomorfismo injetivo e sobrejetivo é chamado *isomorfismo*.

Se M e N são R-módulos, $\mathrm{Hom}_R(M, N)$ denota o conjunto dos homomorfismos de módulos de M em N. Aliás, com a soma usual de funções e a multiplicação escalar (i.e., multiplicação por elementos de R) dada por $(rf)(m) = r \cdot f(m)$ com $r \in R, f \in \mathrm{Hom}_R(M, N)$ e $m \in M$, o conjunto $\mathrm{Hom}_R(M, N)$ é um R-módulo. Como é usual, denotamos por $\mathrm{End}_R M$ o conjunto $\mathrm{Hom}_R(M, M)$. Note que $\mathrm{End}_R M$ é um anel cuja multiplicação é dada pela composição de funções.

Um R-módulo é dito ser de *dimensão finita* se é gerado (sobre R) por uma quantidade finita de elementos; a menor quantidade possível de geradores é a *dimensão* do módulo.

Finalizando nossas primeiras convenções, diremos que um conjunto S é *enumerável* se existir uma bijeção $\psi : S \to \mathbb{Z}^+$. Para qualquer conjunto S, o produto cartesiano $S \times \cdots \times S$ tomado n vezes é denotado por $S^{(n)}$ (exceções ficarão claras no contexto); $\subseteq$ denotará a inclusão de conjunto, e $\subset$ denotará a inclusão própria. Com esta última conveção temos que se $I \lhd R$ e $I \subset R$, I é dito um ideal *próprio* de R.

1.1 Álgebra

Definimos nesta seção a estrutura algébrica que desempenha o papel central deste trabalho. Tal estrutura é o que chamamos de *álgebra*.

Definição 1.1.1. *Seja A um módulo sobre um anel comutativo R. Se A está equipado com uma operação binária $*$ de $A \times A$ em A, chamada multiplicação, tal que para quaisquer $x, y, z \in A$ e qualquer $r \in R$ valem as relações*

(1) $(x + y) * z = x * z + y * z$;

(2) $x * (y + z) = x * y + x * z$;

(3) $r(x * y) = (rx) * y = x * (ry)$,

diremos que A é uma **álgebra** *sobre R ou uma R-álgebra.*

Baseado nesta definição é fácil perceber que todo anel é uma $\mathbb{Z}$-álgebra de modo natural pondo, para $n > 0$, $nr = r + \cdots + r$, $(-n)r = (-r) + \cdots + (-r)$ (n parcelas) e $0r = 0$. A noção de álgebra generaliza ambas as noções de anel e módulo.

Convenção 1.1.2. *Sempre que dissermos que A é uma R-álgebra, ficará subentendido que R é um anel comutativo.*

Definição 1.1.3. *Um submódulo S da R-álgebra A é uma* **subálgebra** *de A se for fechado com respeito à multiplicação, i.e., $x, y \in S$ implica que $x * y \in S$.*

Definição 1.1.4. *Seja A uma álgebra sobre R. Um submódulo I de A é um* **ideal à esquerda** *de A se $r * x \in I$ para todo $r \in A$, $x \in I$. De modo similar define-se um* **ideal à direita** *e um* **ideal bilateral** *(ou simplesmente um* **ideal** *que é um ideal à esquerda e à direita simultaneamente. Denota-se $I \lhd A$) da álgebra A.*

Se A_1 e A_2 são álgebras sobre R, um homomorfismo de R-módulos $\psi : A_1 \to A_2$ é dito ser um homomorfismo de álgebras, ou simplesmente um **homomorfismo**, se

$$\psi(x * y) = \psi(x) * \psi(y),\ x, y \in A_1.$$

Um homomorfismo bijetivo é chamado de **isomorfismo**. Quando existe um isomorfismo entre duas álgebras A_1 e A_2 diz-se que elas são isomorfas, e a notação empregada é $A_1 \approx A_2$ (o símbolo $\approx$ é também usado para denotar isomorfismo de grupos, de módulos e de anéis). Um homomorfismo cujo domínio e o contra-domínio são iguais chama-se **endomorfismo**. Um **automorfismo** é um endomorfismo bijetivo. O conjunto de todos os endomorfismos de uma R-álgebra A é denotado por $\mathrm{End}_R A$. Se $I \lhd A$, podemos construir a R-álgebra A/I de modo similar ao que era feito para anéis pondo $(a + I) + (b + I) := (a + b) + I$, $(a + I)(b + I) := (ab) + I$ e $r(a + I) := (ra) + I$ para $a, b \in A$ e $r \in R$. A álgebra assim construida é chamada de **álgebra quociente** (ou álgebra dos resíduos). Vale lembrar que os teoremas usuais acerca de homomorfismos de grupos, módulos e anéis valem também para álgebras. Por exemplo:

Teorema 1.1.5. *Sejam A_1 e A_2 R-álgebras e $\psi : A_1 \to A_2$ um homomorfismo (de álgebras). Então o núcleo de ψ*

$$ker(\psi) = \{x \in A_1 \mid \psi(x) = 0\}$$

é um ideal de A_1 e a álgebra quociente $A_1/ker(\psi)$ é isomorfa à imagem $Im(\psi) = \{\psi(x) \mid x \in A_1\}$ de ψ.

Usualmente a multiplicação de A é denotada por $\cdot$ e escreve-se xy em vez de $x \cdot y$.

Definição 1.1.6. *Seja A uma álgebra. O* **centro** *de A é o conjunto $Z(A) = \{a \in A \mid ab = ba \ \forall\, b \in A\}$. Além do mais, $Z(A)$ é uma subálgebra de A.*

Observe que A pode ser vista como uma álgebra sobre $Z(A)$ de acordo com a Definição 1.1.1. Em outras palavras, o anel A é também um módulo sobre $Z(A)$ de modo natural.

Definição 1.1.7. *Uma R-álgebra é dita ser de* **dimensão finita** *se ela for de dimensão finita como um R-módulo. Denotamos a dimensão de A sobre R por $[A : R]$ e escrevemos $[A : R] < \infty$ quando esta dimensão for finita.*

Definição 1.1.8. *Seja A uma R-álgebra.*

- *A é* **associativa** *se $(xy)z = x(yz)$ para quaisquer $x, y, z \in A$;*
- *A é* **comutativa** *se $xy = yx$ para quaisquer $x, y \in A$;*
- *A é* **unitária** *se A possui uma unidade $1 \neq 0$ com a propriedade $1x = x1 = x$ para todo $x \in A$.*
- *A é uma* **nil álgebra** *se para cada $a \in A$ existe $n \in \mathbb{Z}^+$ tal que $a^n = 0$. O menor número n para o qual vale esta relação é chamado* **índice de nilpotência** *do elemento a.*

Perceba que uma nil álgebra não pode ser unitária e esta mesma observação vale para as duas definições seguintes.

- *A é uma* **nil álgebra de índice limitado** *n se existe $n \in \mathbb{Z}^+$ fixo tal que $a^n = 0$, para todo $a \in A$.*
- *A é* **nilpotente** *se existe um número natural fixo n tal que o produto de quaisquer n elementos de A é igual a zero. O menor número n para o qual isso vale é chamado* **índice de nilpotência da álgebra** *A.*

Exemplo 1.1.9. *O conjunto $M_2(\mathbb{R})$ com a soma e multiplicação usual de matrizes é uma $\mathbb{R}$-álgebra associativa e não-comutativa cujo elemento unidade é a matriz identidade.*

Exemplo 1.1.10. *O conjunto dos números inteiros pares (como soma e multiplicação usuais) é uma $\mathbb{Z}$-álgebra associativa, comutativa e não possui um elemento unidade.*

Exemplo 1.1.11. *O $\mathbb{R}$-espaço vetorial $\mathbb{R}^3$ é uma álgebra não-associativa, não-comutativa e com unidade quando munido da multiplicação conhecida como produto vetorial.*

Exemplo 1.1.12. *O exemplo que apresentamos agora é um pouco mais elaborado e faremos uso do mesmo no Capítulo 3. Seja G um grupo e R um anel comutativo. No conjunto de todas as funções $f : G \to R$ considere o subconjunto formado por todas as combinações lineares finitas sobre R das funções f_g tais que*

$$f_g(h) = \begin{cases} 1 & se \quad h = g \\ 0 & se \quad h \neq g \end{cases}$$

é uma R-álgebra, denotada por $R[G]$, e é chamada **álgebra de grupo** *de G. Dado $g \in G$, o elemento $f_g \in R[G]$ é usualmente denotado por g. A multiplicação em $R[G]$ é dada por*

$$\begin{aligned} (\sum_{g\in G} \alpha_g g)(\sum_{h\in G} \beta_h h) &= \sum_{g,h\in G} \alpha_g\beta_h gh \\ &= \sum_{f\in G} \gamma_f f \end{aligned}$$

onde $\gamma_f = \sum_{gh=f} \alpha_g\beta_h$ e $\alpha_g, \beta_h \in R$.

Convenção 1.1.13. *A menos que seja feita alguma ressalva, o símbolo F denotará um corpo e quando dissermos "A é uma álgebra", sem tornar explícito sobre qual anel estamos tomando a álgebra A, deve ficar subentendido que A é uma álgebra sobre o corpo F.*

Convenção 1.1.14. *A partir de agora, a menos que seja dito o contrário, todas as álgebras que considerarmos são unitárias e associativas.*

Com esta convenção um subespaço vetorial S de uma álgebra A é uma **subálgebra** se a unidade de A pertence a S e $xy \in S$ para todos $x, y \in S$. Seja A uma álgebra e U um subconjunto não-vazio de A. Considere $B(U)$ o subespaço vetorial de A gerado pelo conjunto $\{1, s_1s_2 \dots s_k \mid k \in \mathbb{Z}^+, s_i \in U\}$. Temos que $B(U)$ é fechado por multiplicação e $1 \in B(U)$. Assim, $B(U)$ é uma subálgebra de A, chamada **subálgebra gerada por** U. Além disso, $B(U)$ é a menor subálgebra de A que contém U, ou seja, toda subálgebra de A que contém U deve conter $B(U)$.

1.2 A Álgebra Livre $F\langle X\rangle$

Nosso objeto de estudo são as álgebras que satisfazem uma identidade polinomial (a ideia intuitiva foi dada na Introdução). A fim de que consigamos dar a definição formal do que se entende por álgebra com identidade polinomial, faz-se necessário apresentar cada um dos objetos. Na seção anterior apresentamos o primeiro deles e agora nesta seção faremos uma construção da álgebra de polinômios. Com isto teremos o caminho pronto para falarmos de álgebra com identidade polinomial.

Antes de começarmos a tratar sobre polinômios daremos duas definições importantes ao que segue.

Definição 1.2.1. *Um conjunto não-vazio S, no qual está definida uma operação $*$ de $S \times S$ em S, é um* **semigrupo** *se para quaisquer x, y e z em S a seguinte condição é satisfeita:*

$$(x * y) * z = x * (y * z).$$

Definição 1.2.2. *Um conjunto não-vazio M, no qual está definida uma operação $*$ de $M \times M$ em M, é um* **monóide** *se para quaisquer x, y e z em M as seguintes condições são satisfeitas:*

(i) $(M, *)$ *é um semigrupo;*

(ii) existe em M um elemento denotado por 1 *e chamado elemento neutro tal que* $x*1 = 1*x = x$.

Considere um conjunto não-vazio de símbolos $\mathcal{A} = \{a_i\}_{i \in I}$. O conjunto $\mathcal{A}$ é chamado **alfabeto** e os símbolos $a_i, i \in I$, as **letras** deste alfabeto.

Uma **palavra** em $\mathcal{A}$ é qualquer lista finita de símbolos, i.e., uma palavra w é uma expressão da forma

$$w = a_{i_1} \dots a_{i_n},$$

onde n é qualquer elemento de $\mathbb{Z}^+$, $a_{i_j} \in \mathcal{A}$ com $1 \leqslant j \leqslant n$. O número n é chamado o **comprimento** da palavra w e este número é exatamente a quantidade de letras que w possui. Como uma convenção, vamos considerar a palavra que não possui letras ou, como é habitualmente chamada, **palavra vazia**, de comprimento 0, que será denotada pelo símbolo 1.

Por praticidade, uma palavra com m letras iguais é denotada como

$$\underbrace{a_i a_i \dots a_i}_{m-\text{vezes}} = a_i^m$$

Se $u = a_{i_1} \dots a_{i_n}$ e $v = a_{j_1} \dots a_{j_m}$ são duas palavras, o símbolo uv denota a palavra obtida pela justaposição de u e v, i.e.,

$$uv = a_{i_1} \dots a_{i_n} a_{j_1} \dots a_{j_m}.$$

Para a palavra vazia 1 e qualquer palavra w, convencionamos que $1w = w1 = w$.

O conjunto de todas as palavras em $\mathcal{A}$, denotado por $\mathcal{A}^*$, com a operação

$$\begin{array}{rccl} \bullet : \mathcal{A}^* \times \mathcal{A}^* & \longrightarrow & \mathcal{A}^* \\ (u, v) & \mapsto & u \bullet v = \text{ justaposição de } u \text{ e } v, \end{array}$$

é um monóide cujo elemento neutro é a palavra vazia 1.

Exemplo 1.2.3. *Se tomarmos $\mathcal{A} = \{a, c, s\}$ como alfabeto, $w_1 = as$, $w_2 = casa$, $w_3 = saca$, $w_4 = ssc = s^2c$, $w_5 = a$, $w_6 = c$, $w_7 = s$, $w_8 = aaaaa = a^5$, $w_9 = cccacc = c^3ac^2$, são palavras em $\mathcal{A}^*$. Vale ainda que $w_7 w_4 = s^3 c$, $w_6 w_5 w_7 w_5 = w_2$.*

No processo anterior não fizemos qualquer restrição sobre o alfabeto ser finito ou infinito. Mas por agora, considere o conjunto enumerável $X = \{X_1, X_2, X_3, \dots\}$ como alfabeto. Cada $X_i \in X$ recebe o nome de **variável**.

O conjunto X^* é um monóide e uma palavra h em X^* é chamada de **monômio**. Para facilitar a notação escrevemos (indutivamente) X_i^k para $X_i^{k-1}X_i$; por exemplo, $X_1^3 = X_1X_1X_1$.

Escreve-se $\deg(h)$ para denotar o grau do monômio h, i.e., o comprimento da palavra h. Como vimos acima, $\deg(h_1h_2) = \deg(h_1) + \deg(h_2)$. Seja $\deg_{X_i}(h)$ o número de vezes que a variável X_i aparece em h, então $\deg(h) = \sum_i \deg_{X_i}(h)$. Um monômio h é **linear** em X_i se $\deg_{X_i}(h) = 1$.

Similarmente, podemos definir outro monóide ξ^* no qual consideramos símbolos ξ_i para representar as variáveis, estipulando que $\xi_i\xi_j = \xi_j\xi_i$ para todo i, j.

Claramente todo elemento de ξ^* pode ser escrito unicamente na forma $\xi_{i_1} \cdots \xi_{i_k}$, onde $i_1 \leqslant i_2 \leqslant \ldots \leqslant i_k$; ξ^* é chamado **monóide livre comutativo**.

Observação 1.2.4. *Substituimos o símbolo X por ξ e seus respectivos elementos X_i por ξ_i apenas para não gerar confusão e para estabelecer a notação quando quisermos fazer uma boa distinção entre o monóide livre não-comutativo e o monóide livre comutativo. Além disso, nem sempre nos limitaremos ao uso das letras X_i e ξ_i para denotar variáveis (Vez por outra também usaremos X, Y, Z, X_i, Y_i, Z_i, etc.). E embora estejamos usando os símbolos X e ξ para denotar um conjunto de variáveis, quando as utilizarmos representando variáveis isso ficará claro.*

Definição 1.2.5. *Para o monóide X^*, a F-**álgebra livremente gerada por** X, denotada por $F\langle X\rangle$, é o conjunto $\{\sum_{h\in X^*} \alpha_h h \mid \alpha_h \in F$ e $\alpha_h = 0$ exceto para um número finito de $h\}$, cujas operações são dadas por*

$$\sum \alpha_h h + \sum \beta_h h := \sum(\alpha_h + \beta_h)h, \quad \alpha(\sum \alpha_h h) := \sum(\alpha\alpha_h)h$$

e

$$(\textstyle\sum_{f\in X^*} \alpha_f f)(\sum_{g\in X^*} \beta_g g) := \sum_{h\in X^*}(\sum_{fg=h} \alpha_f\beta_g)h$$

para $\alpha \in F$.

Verifica-se facilmente que o elemento 0 de $F\langle X\rangle$ é $\sum_{h\in X^*} 0h$ e o inverso aditivo $-(\sum \alpha_h h) = \sum(-\alpha_h)h$. Por fim, não é difícil verificar que $F\langle X\rangle$ com as operações acima definidas é de fato uma álgebra e um elemento $f \in F\langle X\rangle$ é chamado **polinômio**. Escrevendo f como $\sum \alpha_h h$, dizemos que α_h é o **coeficiente** de h. Se $\alpha_h \neq 0$, diremos que $\alpha_h h$ é um monômio não-nulo de f ou, simplesmente, que $\alpha_h h$ é um monômio de f.

Escrevemos $F\langle X_{i_1}, \dots, X_{i_k}\rangle$ para denotar a subálgebra de $F\langle X\rangle$ gerada por $1, X_{i_1}, \dots, X_{i_k}$. Quando tomamos o monóide livre comutativo ξ^*, a álgebra comutativa livremente gerada por ξ é denotada por $F[\,\xi\,]$ e a subálgebra de $F[\,\xi\,]$ gerada por $\xi_{i_1}, \dots, \xi_{i_k}$ denotamos por $F[\xi_{i_1}, \dots, \xi_{i_k}]$.

Definição 1.2.6. *Dizemos que X_i **ocorre** em um polinômio f se $\deg_{X_i}(h) > 0$ para algum monômio h de f; para denotar que $X_1, \dots, X_n$ são as únicas variáveis que ocorrem em f escrevemos $f(X_1, \dots, X_n)$.*

Definição 1.2.7. $\deg(f) = \max\{\deg(h) \mid h \text{ é monômio de } f\}$ *é o* **grau** *do polinômio* f*. Um polinômio* f *é* **homogêneo** *em* X_i *se* X_i *tem o mesmo grau em cada monômio de* f*;* f *é* **multi-homogêneo** *se é homogêneo em cada uma de suas variáveis;* f *é* **linear** *em* X_i *se cada monômio de* f *é linear em* X_i*;* f *é* $\boldsymbol{k}$**-linear** *se é linear em cada* X_i *com* $1 \leqslant i \leqslant k$*;* f *é* **multilinear** *se, para cada* i*,* f *é linear em* X_i*.*

Definição 1.2.8. *Seja* $\mathscr{C}$ *uma classe de álgebras e seja* $F\{\Omega\}$ *uma álgebra gerada por um conjunto* Ω*. A álgebra* $F\{\Omega\}$ *é dita uma* **álgebra livre na classe** $\mathscr{C}$**, livremente gerada pelo conjunto** Ω*, se para qualquer álgebra* $R \in \mathscr{C}$*, toda função* $\psi : \Omega \to R$ *pode ser estendida a um único homomorfismo* $\overline{\psi} : F\{\Omega\} \to R$*. A cardinalidade do conjunto* Ω *é o* **posto** *de* $F\{\Omega\}$*.*

Um resultado de grande importância é o fato de a álgebra $F\langle X\rangle$ ser livre na classe das F-álgebras associativas, unitárias. Este é o conteúdo da proposição seguinte.

Proposição 1.2.9. *A álgebra* $F\langle X\rangle$ *é livre na classe* $\mathscr{A}$ *das* F*-álgebras associativas, unitárias.*

Demonstração. Sejam $A \in \mathscr{A}$ e $\sigma : X \to A$ uma função (de conjuntos). Podemos estender σ unicamente a um homomorfismo de monóide $\sigma' : X^* \to A$, pondo $\sigma'(1) = 1$ e $\sigma'(h) = \sigma'(X_{i_1} \dots X_{i_k}) = \sigma'(X_{i_1}) \dots \sigma'(X_{i_k})$. Agora faremos uma extensão de σ'. Defina $\overline{\sigma} : F\langle X\rangle \to A$ por $\overline{\sigma}(\sum \alpha_h h) = \sum \alpha_h \sigma'(h)$. Obviamente $\overline{\sigma}$ estende σ. Por outro lado, se τ é um homomorfismo estendendo σ, então

$$\tau(h) = \tau(X_{i_1} \dots X_{i_k}) = \tau(X_{i_1}) \dots \tau(X_{i_k}) = \sigma(X_{i_1}) \dots \sigma(X_{i_k}) = \sigma'(X_{i_1} \dots X_{i_k})$$

e portanto $\tau(\sum \alpha_h h) = \sum \alpha_h \tau(h) = \sum \alpha_h \sigma'(h) = \overline{\sigma}(\sum \alpha_h h)$. Provando que $\tau = \overline{\sigma}$. □

De modo inteiramente análogo se mostra que a álgebra $F[\,\xi\,]$ é livre na classe $\mathscr{C}$ das álgebras associativas, comutativas, unitárias.

Antes de iniciarmos a próxima seção vale lembrar que $F[\,\xi\,]$ é um domínio de integridade e portanto possui um corpo de frações, o qual denotaremos por $F(\xi)$; o corpo das frações racionais em uma quantidade enumerável de variáveis.

1.3 Identidades

Nesta seção introduzimos as PI-álgebras, propriedades relacionadas e exemplos. De agora em diante fixamos $X = \{X_1, X_2, \dots\}$ como sendo um conjunto enumerável.

Definição 1.3.1. *Se* $f = f(X_1, \dots, X_n) \in F\langle X\rangle$ *e* R *é uma álgebra, seja*

$$f(R) = \{\psi(f) \mid \psi \in \mathrm{Hom}_F(F\langle X\rangle, R)\},$$

isto é, o conjunto $f(R)$ *é gerado pelas imagens de* f *sob todos os homomorfismos de* $F\langle X\rangle$ *em* R*. Seja ainda* $f(R)^+$ *o subgrupo aditivo de* R *gerado por* $f(R)$*.*

Observe que se $g \in f(F\langle X\rangle) = \{\psi(f) \mid \psi \in \mathrm{End}_F F\langle X\rangle\}$ então $g(R) \subseteq f(R)$.

Definição 1.3.2. *Sejam R uma álgebra e $f \in F\langle X\rangle$. Dizemos que f é uma* **identidade** *para R ou que R satisfaz (a identidade) f se $f(R) = 0$. Esta definição é válida tanto para álgebras unitárias como para álgebras sem unidade. Os exemplos abaixo mostram isso.*

Assim f é uma identidade para R se, e somente se, $f \in \bigcap\{ker(\psi) \mid \psi \in \mathrm{Hom}_F(F\langle X\rangle, R)\}$; mais intuitivamente, f é uma identidade se, e somente se, toda avaliação de f em R resulta em 0.

Para qualquer homomorfismo de álgebras $\varphi : F\langle X\rangle \to R$ que leva X_i em r_i, $1 \leqslant i \leqslant n$, escrevemos $f(r_1, \ldots, r_n)$ para denotar $\varphi(f)$.

Em vista da Proposição 1.2.9, temos que $f(R) = \{f(r_1, \ldots, r_n) \mid r_i \in R\}$. Assim, um polinômio f é uma identidade para R se $f(r_1, \ldots, r_n) = 0$ para quaisquer $r_1, \ldots, r_n$ em R. O conjunto de todas as identidades satisfeitas por R é denotado por $Id(R)$ (Note que $Id(R) \lhd F\langle X\rangle$). Já que o polinômio trivial $f = 0$ é uma identidade para qualquer álgebra R, fazemos o seguinte.

Definição 1.3.3. *Quando uma álgebra R satisfaz uma identidade não trivial f, dizemos que R é uma* **PI-álgebra** *ou que R é uma álgebra com identidade polinomial.*

Para $a, b \in R$, $[a, b] = ab - ba$ denota o comutador de Lie de a e b. Vejamos alguns exemplos de PI-álgebras.

Exemplo 1.3.4. *Se R é uma álgebra comutativa, então R é uma PI-álgebra visto que satisfaz a identidade $[X_1, X_2]$.*

Exemplo 1.3.5. *Qualquer álgebra nilpotente R é uma PI-álgebra. De fato, se n é o índice de nilpotência de R então $f = X_1X_2 \cdots X_n$ é uma identidade polinomial para R.*

Exemplo 1.3.6. *Seja R uma álgebra nil de índice limitado. Isto significa que existe algum número inteiro $n \geqslant 1$ tal que $r^n = 0$, para todo $r \in R$. Então claramente $f = X^n$ é uma identidade polinomial para R.*

Definição 1.3.7. *Um polinômio $f(X_1, \ldots, X_n) \in F\langle X\rangle$ é um* **polinômio R-central** *para a álgebra R se $f(R) \neq 0$ e $f(R) \subseteq Z(R)$. Quando o contexto estiver claro diremos apenas que f é central.*

Observação 1.3.8. *Suponha que $g \in f(F\langle X\rangle)^+$. Se f é uma identidade polinomial para R, então g é uma identidade polinomial para R. Se f é central, então g é uma identidade polinomial para R ou g é central. Além do mais $f(X_1, \ldots, X_n)$ é central se, e somente se, $[X_{n+1}, f]$ (mas não f) é uma identidade polinomial para R.*

Segue da observação anterior que o polinômio $f = X$ é central para qualquer álgebra comutativa e o polinômio $[X, Y]^2$ é central para o álgebra $M_2(F)$. A demonstração de que o polinômio $[X, Y]^2$ é central para a álgebra $M_2(F)$ é bem simples e a omitiremos aqui, mas pode ser encontrada

na página 2 do livro [8] ou na página 7 do livro [7].

Dada uma classe de álgebras $\{R_\gamma \mid \gamma \in \Gamma\}$, o produto cartesiano $\prod_{\gamma\in\Gamma} R_\gamma$ com operações definidas componente a componente é uma álgebra e é chamada **produto direto** dos R_γ. Existe uma projeção canônica $\pi_\gamma : \prod R_\alpha \to R_\gamma$ dada por tomar a γ-ésima componente de um elemento de $\prod_{\gamma\in\Gamma} R_\gamma$. O produto direto de cópias de R é chamado **potência direta** de R.

Veremos agora como "transferir" identidades de uma álgebra para outra. Se R_1 e R_2 são álgebras escrevemos $R_1 \leqslant_F R_2$ se toda identidade de R_2 é uma identidade de R_1. Recorde que uma álgebra R' é uma imagem homomorfa da álgebra R se existir um homomorfismo sobrejetor $R \to R'$.

Observação 1.3.9. *(i) Se $R_1 \subseteq R_2$, então $R_1 \leqslant_F R_2$. (ii) Se R_1 é imagem homomorfa de R_2, então $R_1 \leqslant_F R_2$. (iii) Se $R_\gamma \leqslant_F R$ para todo $\gamma \in \Gamma$, então $\prod_{\gamma\in\Gamma} R_\gamma \leqslant_F R$.*

As propriedades descritas na observação acima são fundamentais à PI-teoria e as usaremos com frequência posteriormente (sem mencionar) para transferir informações de uma álgebra à outra. Na verdade o que colocamos aqui em forma de observação é um teorema devido a Birkhoff que caracteriza variedades de álgebras.

1.4 Multilinearização

Para entender melhor as PI-álgebras, examinemos os polinômios multilineares. Estes polinômios estão intimamente relacionados com o grupo simétrico de n símbolos, denotado por S_n, que é o grupo das permutações de $\{1, \ldots, n\}$. Se $\sigma \in S_n$, então σ pode ser escrita como um produto de elementos de ordem 2, chamados **transposições**; se este produto tem comprimento k, escrevemos $(\operatorname{sgn} \sigma)$ significando $(-1)^k$, e sabemos que $(\operatorname{sgn} \sigma)$ independe do produto particular. Escreve-se (ij) para a transposição que troca apenas i e j. Também define-se o grupo alternado $A_n = \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\}$, o qual é um subgrupo normal de índice 2.

Observação 1.4.1. *Todo polinômio multilinear de grau n tem a forma*

$$\sum_{\sigma\in S_n} \alpha_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)}, \quad \textit{onde cada } \alpha_\sigma \in F.$$

Agora examinaremos um importante processo de multilinearização que é aplicado a um dado polinômio $f(X_1, \ldots, X_k)$ a fim de obter um outro cujas propriedades estejam relacionadas às de f. A descrição envolve a avaliação de f na álgebra $F\langle X\rangle$. Dados $h_1, \ldots, h_k, \ldots$ em $F\langle X\rangle$, por $F\langle X\rangle$ ser livre na classe das álgebras associativas (ver a Definição 1.2.8), existe um único homomorfismo $\Psi : F\langle X\rangle \to F\langle X\rangle$ tal que $\Psi(X_i) = h_i$; usamos a notação $f(h_i, \ldots, h_k)$ para o polinômio obtido pelas substituições $X_i \to h_i$, $1 \leqslant i \leqslant k$. Deste modo, $f(X_1, \ldots, X_k)$ pode ser visto como uma função de $F\langle X\rangle^{(k)}$ em $F\langle X\rangle$.

Definição 1.4.2. *Dada qualquer álgebra R e qualquer função $\psi : R^{(k)} \to R$, definimos $\Delta^\psi_{i,k+1} : R^{(k+1)} \to R$ por*

$$\begin{aligned}\Delta^\psi_{i,k+1}(r_1, \ldots, r_{k+1}) = {} & \psi(r_1, \ldots, r_{i-1}, r_i + r_{k+1}, r_{i+1}, \ldots, r_k) \\ & - \psi(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_k) - \psi(r_1, \ldots, r_{i-1}, r_{k+1}, r_{i+1}, \ldots, r_k)\end{aligned}$$

Segue do que foi observado o parágrafo anterior que, quando vemos um polinômio $f(X_1, \ldots, X_k)$ como uma função de $F\langle X\rangle^{(k)}$ em $F\langle X\rangle$, a função $\Delta^f_{i,k+1} : F\langle X\rangle^{(k+1)} \to F\langle X\rangle$ avaliada na $k+1$-upla $(X_1, \ldots, X_{k+1})$ é

$$\begin{aligned}\Delta^f_{i,k+1}(X_1, \ldots, X_{k+1}) = {} & f(X_1, \ldots, X_{i-1}, X_i + X_{k+1}, X_{i+1}, \ldots, X_k) \\ & - f(X_1, \ldots, X_{i-1}, X_i, X_{i+1}, \ldots, X_k) - f(X_1, \ldots, X_{i-1}, X_{k+1}, X_{i+1}, \ldots, X_k)\end{aligned}$$

Por exemplo, se $f(X_1, X_2) : F\langle X\rangle^{(2)} \to F\langle X\rangle$ é tal que $f(X_1, X_2) = X_1^2 X_2$ então

$$\begin{aligned}\Delta^f_{1,3}(X_1, X_2, X_3) &= f(X_1 + X_3, X_2) - f(X_1, X_2) - f(X_3, X_2) \\ &= (X_1 + X_3)^2 X_2 - X_1^2 X_2 - X_3^2 X_2 \\ &= X_1 X_3 X_2 + X_3 X_1 X_2\end{aligned}$$

Agora vamos coletar algumas propriedades importantes para um polinômio $f(X_1, \ldots, X_k)$. Suponha que $\deg_{X_i}(f) > 0$, e seja $g(X_1, \ldots, X_{k+1}) = \Delta^f_{i,k+1}(X_1, \ldots, X_{k+1})$. **(i)** $\deg_{X_i}(g) = \deg_{X_i}(f) - 1$. **(ii)** Se $1 \leqslant j \leqslant k$ e $j \neq i$, então $\deg_{X_j}(g) = \deg_{X_j}(f)$. **(iii)** $g \in f(F\langle X\rangle)^+$. **(iv)** Todos os coeficientes de g são coeficientes de f. **(v)** Se f é homogêneo de grau n em X_i, então $g(X_1, \ldots, X_k, X_i) = (2^n - 2)f(X_1, \ldots, X_k)$ desde que a característica de F não seja 2.

É comum denotar o polinômio $\Delta^f_{i,k+1}(X_1, \ldots, X_{k+1})$ também por $\Delta_{i,k+1}(f)(X_1, \ldots, X_{k+1})$. Suponha que f seja um polinômio cujo termo constante é 0 (i.e., cada monômio de f tem grau > 0). Se $\deg_{X_i}(f(X_1, \ldots, X_k)) = n$, então $\Delta_{i,k+n-1} \cdots \Delta_{i,k+1}(f)$ é um polinômio que é linear nas variáveis $X_i, X_{k+1}, \ldots, X_{k+n-1}$. Para verificar isto basta aplicar indução em n e depois notar que $\deg_{X_{k+1}}(f)$ vai diminuindo quando se aplicam $\Delta_{i,k+2}, \ldots, \Delta_{i,k+n-1}$. Usando este procedimento em cada variável de f, chegaremos em um polinômio multilinear.

Exemplo 1.4.3. *Pelo pequeno teorema de Fermat, o corpo $\mathbb{Z}/3\mathbb{Z}$ satisfaz a identidade $f(X_1) = X_1^3 - X_1$ (bem como a identidade óbvia $[X_1, X_2]$). Linearizemos f passo a passo. Primeiro, tome $f_1(X_1, X_2) = \Delta^f_{1,2} = X_1^2 X_2 + X_1 X_2 X_1 + X_2 X_1^2 + X_2^2 X_1 + X_2 X_1 X_2 + X_1 X_2^2$. E por fim, tome $f_2(X_1, X_2, X_3) = \Delta^{f_1}_{1,3} = X_1 X_3 X_2 + X_3 X_1 X_2 + X_1 X_2 X_3 + X_3 X_2 X_1 + X_2 X_1 X_3 + X_2 X_3 X_1$.*

Definição 1.4.4. *O* **polinômio simétrico em k variáveis** *é $\sum_{\sigma \in S_k} X_{\sigma(1)} \cdots X_{\sigma(k)}$.*

O polinômio $p = \sum_{\sigma \in S_k} X_{\sigma(1)} \cdots X_{\sigma(k)}$ é uma identidade polinomial para todo corpo finito com k elementos. De fato, se F é um corpo com k elementos, então $F - \{0\}$ é um grupo multiplicativo, assim, pelo teorema de Lagrange, $a^{k-1} = 1$ para todo $a \in F - \{0\}$. Consequentemente, $X^k - X$ é uma identidade em F e, como no exemplo anterior, vê-se facilmente que a multilinearização de $X^k - X$ é o polinômio simétrico p.

1.5 Polinômios Normais

Definição 1.5.1. *Um polinômio $f(X_1, \ldots, X_n)$ é* ***k*-alternado**, *$k \leqslant n$, se satisfaz a seguinte condição para cada i, j, com $1 \leqslant i < j \leqslant k$: Para qualquer homomorfismo $\psi : F\langle X\rangle \to F\langle X\rangle$ tal que $\psi(X_i) = \psi(X_j)$ tem-se $\psi(f) = 0$. Em outras palavras, escrever X_i no lugar de X_j produz $f(\ldots, X_i, \ldots, X_i, \ldots) = 0$.*

Definição 1.5.2. *Um polinômio f é* ***k*-normal** *se f é k-linear e k-alternado. Se $f(X_1, \ldots, X_n)$ é n-normal, diremos simplesmente que f é* **normal**.

O polinômio $[X, Y] = XY - YX$ é uma identidade normal de qualquer álgebra comutativa. A alternância e propriedades lineares são análogas à alternância e propriedades lineares do determinante de uma matriz. Consequentemente, é razoável tentarmos acumular informações concernentes a identidades normais imitando parte da teoria de determinantes.

O **polinômio *standard*** de grau n, $St_n(X_1, \ldots, X_n) = \sum_{\sigma \in S_n} (\text{sgn } \sigma) X_{\sigma(1)} \cdots X_{\sigma(n)}$, é o mais simples exemplo de polinômio n-normal (veremos isso depois).

Prossigamos com as observações fáceis de verificar a respeito das identidades k-lineares ou k-normais. Sejam $T_1, \ldots, T_m$ subconjuntos de uma álgebra R e $f(X_1, \ldots, X_m)$ um polinômio, escrevemos $f(T_1 \times \cdots \times T_m)$ para $\{f(x_1, \ldots, x_m) \mid x_i \in T_i\}$. Escrevemos $T^{(i)}$ para $T \times \cdots \times T$, o produto cartesiano tomado i vezes. Assim, $f(R^{(m)})$ é o mesmo que $f(R)$. Também, dados os conjuntos A, B e uma operação binária $* : A \times B \to G$ para algum grupo *aditivo* G, escrevemos $A * B$ para denotar o conjunto dos elementos da forma $\sum_i a_i * b_i$ para adequados a_i em A, b_i em B. Por exemplo, para uma álgebra R, escrevemos $[R, R]$ denotando o conjunto dos objetos da forma $\sum_i [r_{i_1}, r_{i_2}]$. Similarmente, definimos $A^1 = A$ e, indutivamente, $A^{i+1} = A^i A$. Nessa mesma linha, se $A_\gamma \subseteq R$, para cada γ em um conjunto de índices Γ, definimos $\sum_{\gamma \in \Gamma} A_\gamma = \{\text{somas finitas de elementos tomados dos diferentes } A_\gamma\}$. A única exceção a esta regra notacional é que se $A \subseteq R$, escrevemos $R - A$ para denotar $\{r \in R \mid r \notin A\}$.

Observação 1.5.3. *Se $f(X_1, \ldots, X_d)$ é k-linear, $x_1, \ldots, x_k, r_{k+1}, \ldots, r_d$ são elementos de R, e $\alpha_{ij} \in Z(R)$, então*

$$f(\sum_{i=1}^{k} \alpha_{i1} x_i, \ldots, \sum_{i=1}^{k} \alpha_{ik} x_i, r_{k+1}, \ldots, r_d) = \sum_{i_1, \ldots, i_k} \alpha_{i_1 1} \cdots \alpha_{i_k k} f(x_{i_1}, \ldots, x_{i_k}, r_{k+1}, \ldots, r_d).$$

O próximo resultado segue imediadamente desta observação.

Lema 1.5.4. *Se $f(X_1, \ldots, X_d)$ é k-linear, $T_1, \ldots, T_d$ são sobconjuntos de R, então*

$$f(Z(R)T_1 \times \cdots \times Z(R)T_k \times T_{k+1} \times \cdots \times T_d) \subseteq Z(R) f(T_1 \times \cdots \times T_d).$$

Como consequência desse lema temos a proposição abaixo.

Proposição 1.5.5. *Suponha que a álgebra R seja gerada como um $Z(R)$-módulo por um conjunto B. Para checar que um polinômio k-linear $f(X_1, \ldots, X_d)$ é uma identidade de R (resp. é central), é suficiente mostrar que $f(B^{(k)} \times R^{(d-k)}) = 0$ (resp. $0 \neq f(B^{(k)} \times R^{(d-k)}) \subseteq Z(R)$).*

Notemos um caso especial importante. Dizemos que uma álgebra R é uma **extensão central** de uma subálgebra S se $R = Z(R)S$. Sendo assim, a proposição acima diz que uma extensão central de S satisfaz todas as identidades multilineares de S. Observe que se R é uma extensão central de S, então $Z(S) \subseteq Z(R)$. Portanto, se R é uma extensão central de S e S é uma extensão central de R_1, então $R = Z(R)S = Z(R)Z(S)R_1 = Z(R)R_1$, assim R é uma extensão central de R_1.

Proposição 1.5.6. *Se $f(X_1, \ldots, X_d)$ é k-normal e $T \subseteq R$, fechado com a multiplicação, é tal que $Z(R)T$ é uma $Z(R)$-álgebra cuja dimensão é $< k$, então $f(T^{(k)} \times R^{(d-k)}) = 0$.*

Demonstração. Seja $B = \{b_1, \ldots, b_{k-1}\}$ um conjunto que gera T sobre $Z(R)$. Algum elemento de B deve aparecer duas vezes nos primeiros k lugares de qualquer avaliação de $f(B^{(k)} \times R^{(d-k)})$; já que f é k-alternado, temos que $f(B^{(k)} \times R^{(d-k)}) = 0$. Além disso, $T^{(k)} \subseteq (Z(R)B)^{(k)}$. Daí, $f(T^{(k)} \times R^{(d-k)}) \subseteq f((Z(R)B)^{(k)} \times R^{(d-k)}) \subseteq Z(R)f(B^{(k)} \times R^{(d-k)}) = 0$. □

Segue desta proposição que $M_n(F)$ é uma PI-álgebra já que qualquer polinômio (n^2+1)-normal é uma identidade. Em particular, St_{n^2+1} é uma identidade polinomial para $M_n(F)$.

1.6 Álgebras com Identidades Polinomiais

Esta seção é destinada aos exemplos que consideramos importantes à sequência deste trabalho. Além dos que apresentamos aqui, existem diversos exemplos interessantes de álgebras que satisfazem identidades polinomiais mas que foram omitidos por conveniência.

Exemplo 1.6.1. *Se R é uma álgebra de dimensão $< k$, então todo polinômio k-normal é uma identidade polinomial para R. De fato, R obviamente tem dimensão $< k$ como $Z(R)$-álgebra, assim aplicamos a Proposição 1.5.6 com $T = R$.*

Exemplo 1.6.2. *Seja R uma álgebra. Um elemento $r \in R$ é* **integral de grau k** *(sobre F) se $r^k = \sum_{i=0}^{k-1} \alpha_i r^i$ para elementos adequados $\alpha_0, \ldots, \alpha_{k-1}$ em F. R é* **integral** *se cada um de seus elementos é integral; R é* **integral de grau limitado** *se cada elemento é integral de grau $\leqslant k$ (tomamos o menor k possível).*

Em 1945 Jacobson provou que toda álgebra integral de grau limitado satisfaz uma identidade polinomial ([11]). Obteremos isso como consequência da proposição seguinte.

Proposição 1.6.3. *Se R é uma álgebra integral de grau $\leqslant k$, então para qualquer polinômio k-normal $f(X_1, \ldots, X_d)$ o polinômio*

$$f([X_1^k, X_2], [X_1^{k-1}, X_2], \ldots, [X_1, X_2], X_{k+1}, \ldots, X_d)$$

é uma identidade em R.

Demonstração. Para qualquer r sabemos que $r^k = \sum_{i=0}^{k-1} \alpha_i r^i$ para α_i adequados em F. Então, para todo s, $[r^k, s] = \sum_{i=1}^{k-1} \alpha_i [r^i, s]$ ($[\alpha_0, s] = 0$ uma vez que $F \subseteq Z(R)$). Portanto, tomando $T = \{[r^i, s] \mid 1 \leqslant i \leqslant k\}$, temos $f(T^{(k)} \times R^{(d-k)}) = 0$. □

Na proposição anterior o conjunto $T = \{[r^i, s] \mid 1 \leqslant i \leqslant k\}$ depende de r e s. Ou seja, para cada x, y em R temos um $T_{xy} = \{[x^i, y] \mid 1 \leqslant i \leqslant k\}$. De posse deste resultado podemos concluir que o polinômio *standard* de grau k, $St_k([X_1^k, X_2], [X_1^{k-1}, X_2], \ldots, [X_1, X_2])$, é uma identidade polinomial para toda álgebra integral de grau $\leqslant k$, provando o resultado de Jacobson.

Exemplo 1.6.4. *Se $UT_n(F)$ é a álgebra das matrizes $n\times n$ triangulares superiores (com a diagonal) sobre F, então $[X_1, X_2][X_3, X_4]\cdots[X_{2n-1}, X_{2n}]$ é uma identidade polinomial para $UT_n(F)$. De fato, se $A, B \in UT_n(F)$, temos que a matriz $C = AB - BA$ tem a diagonal principal nula. Sendo assim, é suficiente mostrarmos que as matrizes triangulares superiores (sem a diagonal) são anuladas pelo polinômio $Y_1 \cdots Y_n$. Denotemos por e_{ij} a matriz que tem 1 na entrada ij e 0 nas demais (estas são chamadas matrizes unidade). As matrizes $A = \sum_{j-i\geqslant 1} \alpha_{ij}e_{ij}$ e $B = \sum_{l-k\geqslant h\geqslant 1} \beta_{kl}e_{kl}$ pertencem a $UT_n(F)$ e possuem a diagonal principal nula. Levando em consideração as regras usuais de multiplicação de matrizes temos*

$$\begin{aligned}(\sum_{j-i\geqslant 1} \alpha_{ij}e_{ij})(\sum_{l-k\geqslant h\geqslant 1} \beta_{kl}e_{kl}) &= \sum_{i,j,k,l} \alpha_{ij}\beta_{kl}e_{ij}e_{kl} \\ &= \sum_{i,j,l} \alpha_{ij}\beta_{jl}e_{il} \\ &= \sum_{l-i\geqslant h+1} \gamma_{il}e_{il}.\end{aligned}$$

A desigualdade no último somatório é justificável: $l - i = \underbrace{(l-j)}_{\geqslant h} + \underbrace{(j-i)}_{\geqslant 1} \geqslant h + 1$.

Exemplo 1.6.5. *Suponha que a característica de F é diferente de 2. Seja*

$$\mathbf{G} = F\langle X\rangle/U,$$

U é o ideal de $F\langle X\rangle$ gerado por todos os $X_iX_j + X_jX_i$. Chamamos $\mathbf{G}$ a **álgebra exterior** *ou* **álgebra de Grassmann**, *e escrevemos e_i para a imagem de X_i em $\mathbf{G}$ via projeção canônica. Escreva $B = \{e_i \mid i \in \mathbb{Z}^+\}$ e $B' = \{e_{i_1}\cdots e_{i_m} \mid 0 \leqslant m < \infty \text{ e } i_1 < \cdots < i_m\}$. Para $m = 0$ escrevemos "1". Cada elemento de $\mathbf{G}$ pode ser escrito unicamente na forma $\sum \alpha_b b$, onde $\alpha_b \in F, b \in B'$ e α_b é diferente de 0 apenas para uma quantidade finita.*

Vamos desenvolver algumas propriedades básicas da álgebra exterior. Se $b = e_{i_1}\cdots e_{i_m}$, escrevemos $\deg(b) = m$. Seja $\mathbf{G}_0$ (resp. $\mathbf{G}_1$) o F-subespaço vetorial de $\mathbf{G}$ gerado por todos os monômios de grau par (resp. ímpar).

Observação 1.6.6. *Se $a \in \mathbf{G}_0$, então $ae_i = e_ia$ para todo e_i. Se $a \in \mathbf{G}_1$, então $ae_i = -e_ia$ para todo e_i. (Para provar essas afirmações, podemos assumir que $a \in B'$ e aplicar indução no comprimento de a.)*

Observação 1.6.7. *$Z(\mathbf{G}) = \mathbf{G}_0$. (Segue da observação anterior, tendo em vista que $a \in Z(\mathbf{G})$ se, e só se, $ae_i = e_ia$ para todo i.)*

Existe algo sutil nesta última observação que fizemos. Afirmamos que todo elemento do centro de $\mathbf{G}$ tem grau par. Isto é verdade porque convencionamos no início na Seção 1.3 que nosso conjunto X de variáveis é enumerável. Mas quando tomamos X com uma quantidade finita de elementos, obviamente, a álgebra $\mathbf{G}$ neste caso tem dimensão finita e a observação deixa de ser verdadeira. De fato, tome $X = \{X_1, X_2, X_3\}$ e seja $F = \mathbb{R}$. O elemento $b = e_1e_2e_3$ de $\mathbf{G} = \mathbb{R}\langle X\rangle/U$ tem grau ímpar (logo pertence a $\mathbf{G}_1$), mas $b \in Z(\mathbf{G})$ já que para todo $a \in \mathbf{G}$, $ab = ba = 0$.

Observação 1.6.8. *Como $Z(\mathbf{G})$-módulo, $\mathbf{G}$ é gerada por $B \cup \{1\}$.*

Proposição 1.6.9. *O polinômio $[X, Y]$ é $\mathbf{G}$-central.*

Demonstração. Pela Proposição 1.5.5, precisamos apenas mostrar que cada i, j, $[e_i, 1] \in Z(\mathbf{G})$ e $[e_i, e_j] \in Z(\mathbf{G})$. Mas $[e_i, 1] = 0$ e $[e_i, e_j] \in \mathbf{G}_0 = Z(\mathbf{G})$. □

Portanto $\mathbf{G}$ é uma PI-álgebra e tem um polinômio central.

1.7 Fatos sobre Polinômios Normais

Tendo visto que os polinômios k-normais são figuras proeminentes nas álgebras de dimensão finita e nas álgebras integrais de grau limitado, gostaríamos de examiná-los mais explicitamente, tendo em vista a Observação 1.4.1. Assuma por toda esta seção que $f(X_1, \ldots, X_d)$ é k-linear. Nosso principal objetivo é encontrar um modo de verificar quando f é k-normal.

Definição 1.7.1. *Se $\sigma \in S_n, n \leqslant k$, definimos $f_{(\sigma,n)}$ como sendo a soma daqueles monômios de f nos quais as variáveis $X_1, \ldots, X_n$ aparecem exatamente nesta ordem $X_{\sigma(1)}, \ldots, X_{\sigma(n)}$ (ignorando as demais variáveis $X_j, j > n$ que ocorrem em f); escrevemos $f_{(n)}$ para denotar $f_{(1,n)}$.*

Exemplo 1.7.2. *Seja $F = \mathbb{R}$ e $f(X_1, X_2, X_3, X_4, X_5) = 13X_4^2X_1X_3X_5X_2 - \sqrt{2}X_3X_5X_2X_4^3X_1$ em $\mathbb{R}\langle X\rangle$. O polinômio f é 3-linear ($k = 3$). Se tomamos $\sigma = (12) \in S_2$ ($n = 2$) devemos analisar as variáveis X_1 e X_2, e elas devem aparecer em $f_{(\sigma,2)}$ exatamente na ordem X_2, X_1. Daí, temos que $f_{(\sigma,2)} = -\sqrt{2}X_3X_5X_2X_4^3X_1$. Agora se tomamos o mesmo polinômio f, $n = 3$ e $\sigma = (12) \in S_3$, devemos analisar as três primeiras variáveis de f e elas devem aparecer em $f_{(\sigma,2)}$ exatamente na ordem X_2, X_1, X_3. Daí, temos que $f_{(\sigma,2)} = 0$.*

Exemplo 1.7.3. *Seja $F = \mathbb{Q}$ e*

$$f(X_1, X_2, X_3, X_4, X_5) = X_3X_4^3X_5^2X_1X_2 - 3X_2X_1X_3X_5X_4^{19} + 4X_4^8X_3X_1X_5X_2$$

em $\mathbb{Q}\langle X\rangle$. Como se pode ver, f é 3-linear. A definição foi dada para $n \leqslant k$ e como $k = 3$, tome, por exemplo, $n = 3$.

$$S_3 = \{\sigma_0 = 1, \sigma_1 = (12), \sigma_2 = (13), \sigma_3 = (23), \sigma_4 = (123), \sigma_5 = (132)\}.$$

Temos que $f_{(1,3)} = 0$, $f_{(\sigma_1,3)} = -3X_2X_1X_3X_5X_4^{19}$, $f_{(\sigma_5,3)} = X_3X_4^3X_5^2X_1X_2 + 4X_4^8X_3X_1X_5X_2$, $f_{(\sigma_3,3)} = 0$, $f_{(\sigma_4,3)} = 0$ e $f_{(\sigma_2,3)} = 0$

Perceba por este último exemplo que $f = \sum_{\sigma_i \in S_3} f_{(\sigma_i,3)}$, $i = 0, 1, 2, 3, 4, 5$. Não há nada de especial com este exemplo. Isso é um fato geral entre os polinômios k-lineares.

Definição 1.7.4. *Para $\sigma \in S_k$, escrevemos $\sigma \circ f$ para denotar*

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(k)}, X_{k+1}, \ldots, X_d)$$

Assuma até o fim desta seção que F é um corpo cuja característica é diferente de 2.

Proposição 1.7.5. *f é k-normal se, e só se, $(ij) \circ f = -f$ para todo $i < j \leqslant k$.*

Demonstração. Se f é k-normal, então (trabalhando nas posições i e j)

$$\begin{aligned}(ij) \circ f + f &= f(\dots, X_j, \dots, X_i, \dots) + f(\dots, X_i, \dots, X_j, \dots) \\ &= f(\dots, X_i + X_j, \dots, X_i + X_j, \dots) - f(\dots, X_i, \dots, X_i, \dots) \\ &\quad - f(\dots, X_j, \dots, X_j, \dots) \\ &= 0\end{aligned}$$

Reciprocamente, suponha que $(ij) \circ f = -f$ para todo $i < j \leqslant k$. Então, escrevendo $f = \sum_{\sigma \in S_k} f_{(\sigma,k)}$, temos $(ij) \circ f_{(\sigma,k)} = -f_{((ij)\sigma,k)}$ para todo $\sigma \in S_k$. Assim, sendo $G = \{\sigma \in S_k \mid \sigma^{-1}(i) < \sigma^{-1}(j)\}$, temos $f = \sum_{\sigma \in G}(f_{(\sigma,k)} + f_{((ij)\sigma,k)}) = \sum_{\sigma \in G}(f_{(\sigma,k)} - (ij) \circ f_{(\sigma,k)})$, implicando $f(\dots, X_i, \dots, X_i, \dots) = 0$. Portanto f, é k-normal pela definição. □

Corolário 1.7.6. *Se $(ii+1) \circ f = -f$ para todo $i < j \leqslant k-1$, então f é k-normal.*

Demonstração. As transposições $(12), (23), (34), \dots$ geram todas as transposições visto que, para $i < j$, $(ij+1) = (ij)(jj+1)(ij)$. E o resultado segue da proposição anterior. □

Estamos prontos para um bom critério de k-normalidade.

Teorema 1.7.7. *(i) f é k-normal se, e só se, para qualquer σ em S_k, $f_{(\sigma,k)} = (\operatorname{sgn} \sigma)\sigma \circ f_{(k)}$.*

(ii) f é k-normal se, e só se, $f = \sum_{\sigma \in S_k}(\operatorname{sgn} \sigma)\sigma \circ f_{(k)}$.

Demonstração. (i) Toda permutação é um produto de transposições. Agora use a relação $(ij) \circ f_{(\sigma,k)} = -f_{((ij)\sigma,k)}$ que apareceu na demonstração da recíproca da Proposição 1.7.5.
(ii) Isto agora tornou-se imediato. □

Corolário 1.7.8. *f é k-normal se, e só se,*

$$f(X_{\sigma(1)}, \dots, X_{\sigma(k)}, X_{k+1}, \dots) = (\operatorname{sgn} \sigma) f(X_1, \dots, X_k, X_{k+1}, \dots)$$

para todo $\sigma \in S_k$.

Demonstração. Segue imediatamente da Proposição 1.7.5. □

Agora usaremos os resultados acima para descrever os dois mais importantes polinômios na PI-teoria.

1.8 Polinômio de Capelli e Polinômio *Standard*

Definimos o k-ésimo **polinômio de Capelli**

$$C_{2k}(X_1, \ldots, X_{2k}) = \sum_{\sigma \in S_k} (\text{sgn } \sigma) X_{\sigma(1)} X_{k+1} X_{\sigma(2)} X_{k+2} \cdots X_{\sigma(k-1)} X_{2k-1} X_{\sigma(k)} X_{2k},$$

O polinômio de Capelli C_{2k} é k-normal com

$$(C_{2k})_{(k)} = X_1 X_{k+1} \cdots X_k X_{2k}$$

e desempenha um papel muito importante entre os polinômios que são k-alternados, como mostra o Lema 1.8.1 abaixo.

A fim de fazer distinção entre as variáveis que são permutadas e as que são mantidas fixas, às vezes escrevemos o polinômio de Capelli como

$$C_{2k}(X; Y) = C_{2k}(X_1, \ldots, X_k; Y_1, \ldots, Y_k) = \sum_{\sigma \in S_k} (\text{sgn } \sigma) X_{\sigma(1)} Y_1 X_{\sigma(2)} Y_2 \cdots X_{\sigma(k)} Y_k.$$

Por exemplo, para $k = 2$, temos

$$C_4 = X_1 Y_1 X_2 Y_2 - X_2 Y_1 X_1 Y_2.$$

Vale notar que $St_k(X_1, \ldots, X_k) = C_{2k}(X_1, \ldots, X_k; 1, \ldots, 1)$.

Em vista da Proposição 1.5.6, o polinômio $C_{2(n^2+1)}$ é também uma identidade polinomial para a álgebra $M_n(F)$. Além disso, pelo item (ii) do Teorema 1.7.7, podemos escrever

$$St_k = \sum_{\sigma \in S_k} (\text{sgn } \sigma)(\sigma \circ h)$$

onde $h = X_1 \cdots X_k$ e

$$C_{2k} = \sum_{\sigma \in S_k} (\text{sgn } \sigma)(\sigma \circ h)$$

onde $h = X_1 X_{k+1} \cdots X_k X_{2k}$.

O polinômio *standard* ofuscou por quase toda a história da PI-teoria o polinômio de Capelli, em vista do teorema de Amitsur-Levitzki, que afirma que St_{2n} é a única identidade polinomial de grau mínimo para a álgebra das matrizes $n \times n$ sobre um anel comutativo. No entanto, como a propriedade de alternância se tornou mais importante ao longo do tempo, o polinômio de Capelli assumiu seu papel de liderança. Hoje é impossível mergulhar profundamente na PI-teoria sem recorrer constantemente ao polinômio de Capelli. Veremos agora e na próxima seção porque o polinômio de Capelli surge tão naturalmente na teoria dos polinômios alternados.

Lema 1.8.1. *Todo polinômio que é k-normal tem a forma*

$$h_0 C_{2k}(X_1, \ldots, X_k, h_1, \ldots, h_k),$$

para monômios adequados $h_0, \ldots, h_k$.

Demonstração. É uma consequência clara do item (ii) do Teorema 1.7.7. □

Olhando este lema mais de perto podemos notar que se C_{2k} é uma identidade em uma álgebra R, então todo polinômio k-normal é também uma identidade para R. Assim, em algum sentido, C_{2k} "gera" os polinômios k-normais.

A seguir, afirmamos algumas propriedades do polinômio *standard*. Mas antes disso convencionamos que $St_0 = 1$.

Proposição 1.8.2. *(i) Se $f(X_1, \ldots, X_m)$ é normal, então $f = \alpha St_m(X_1, \ldots, X_m)$, para algum $\alpha \in F$.*

(ii) $St_{m+1}(X_1, \ldots, X_m) = \sum_{i=1}^{m+1} (-1)^{i+1} X_i St_m(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_m)$. Consequentemente, se St_m é uma identidade polinomial para uma álgebra R, St_{m+1} também é uma identidade para R.

Demonstração. (i) Segue do item (ii) do Teorema 1.7.7.
(ii) O polinômio St_{m+1} pode ser escrito como

$$St_{m+1} = X_1 g_1 + \cdots + X_{m+1} g_{m+1}$$

onde $g_i = g_i(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots X_{m+1})$ é normal. Pelo item (i) desta proposição,

$$g_i = \alpha_i St_m(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots X_{m+1})$$

com $\alpha_i = (-1)^{i+1}$. □

No início desta seção observamos que $C_{2(n^2+1)}$ é uma identidade para a álgebra $M_n(F)$ e consequentemente St_{n^2+1}. Qual seria o grau mínimo para estes polinômios a fim de que isto continue valendo? Para o polinômio de Capelli a resposta é dada na proposição seguinte.

Proposição 1.8.3. *O polinômio de Capelli C_{2n^2} não é uma identidade polinomial para $M_n(F)$, mas é uma identidade polinomial para toda subálgebra de $M_n(F)$ cuja dimensão é menor do que n^2.*

Demonstração. Seja $k = n^2$. Ordenemos as k matrizes unidade e_{ij} da seguinte maneira

$$e_{11} < e_{12} < \cdots < e_{1n} < e_{21} < e_{22} < \cdots < e_{2n} < \cdots < e_{n1} < e_{n2} < \cdots < e_{nn}$$

e escrevamos e_d para a d-ésima matriz unidade ($1 \leqslant d \leqslant n^2$). Considere $C_{2k}(e_1, \ldots, e_k; e_1, \ldots, e_k) = \sum_{\sigma \in S_k} (\text{sgn } \sigma) e_{\sigma(1)} e_1 \cdots e_{\sigma(k)} e_k$. Agora $e_1 e_{\sigma(2)} e_2 = e_{11} e_{\sigma(2)} e_{12}$, que é 0 a não ser que $e_{\sigma(1)} = e_{11}$. Da mesma forma, $e_2 e_{\sigma(3)} e_3 = 0$ a menos que $e_{\sigma(3)} = e_{21}$. Continuando desta maneira, vemos que existe precisamente uma escolha de $e_{\sigma(2)}, \ldots, e_{\sigma(n)}$ tal que $e_1 e_{\sigma(2)} e_2 \cdots e_{\sigma(n)} e_n \neq 0$, e esta escolha determina σ (e força que se tenha $e_{\sigma(1)} = e_{n1}$). Portanto $C_{2k}(e_1, \ldots, e_k; e_1, \ldots, e_k) = \pm e_{nn}$.
Para concluir a proposição, basta usar o Exemplo 1.6.1. □

Já respondemos a pergunta para um caso. A saber, o grau mínimo para o polinômio de Capelli a fim de que este seja uma identidade polinomial para a álgebra $M_n(F)$ é $2(n^2 + 1)$. Para o caso do polinômio *standard*, este é o conteúdo de um famoso teorema devido à Amitsur e Levitzki.

Teorema 1.8.4 (Amitsur-Levitzki)**.** *St_{2n} é uma identidade polinomial para $M_n(R)$, onde R é qualquer álgebra comutativa. Além disso, $M_n(R)$ não satisfaz uma identidade de grau menor do que $2n$.*

Uma prova enxuta para este teorema pode ser encontrada na página 19 do livro *Computational Aspects of Polynomial Identities* ([13]) de Belov & Rowen.

1.9 Polinômios Centrais para a Álgebra de Matrizes

Uma parte fundamental na estrutura das PI-álgebras é a teoria de matrizes. Nesta seção são trazidos fatos clássicos e básicos a respeito da álgebra de matrizes. Bem como a abordagem de Razmyslov para polinômios centrais da álgebra de matrizes.

Seja δ_{ij} o *delta de Kronecker*. Novamente e_{ij} denota uma matriz unidade em $M_n(R)$, onde R é uma álgebra. Claro que cada elemento de $M_n(R)$ pode escrito unicamente na forma $\sum_{i,j}^{n} r_{ij} e_{ij}$ para $r_{ij} \in R$ tomados de maneira adequada; vamos denotar uma tal matriz por (r_{ij}). Recorde que as operações de adição e multiplicação de matrizes são dadas por

$$(r_{ij}) + (s_{ij}) = (r_{ij} + s_{ij}) \text{ e } (r_{ij})(s_{ij}) = (\sum_{k=1}^{n} r_{ik} s_{kj}).$$

Claramente, $e_{ij} e_{kl} = \delta_{jk} e_{il}$ e também $r_{kl} e_{kl} = e_{kk}(r_{ij}) e_{ll}$. Estes fatos são óbvios, mas ajudam a identificar precisamente as entradas das matrizes.

Uma **matriz escalar** é uma matriz da forma $\sum_{i=1}^{n} r e_{ii}$ com $r \in R$. O conjunto das matrizes escalares é uma subálgebra de $M_n(R)$ que pode ser identificada com R pelo isomorfismo $r \mapsto \sum r e_{ii}$, e é o centralizador de $\{e_{ij} \mid 1 \leqslant i, j \leqslant n\}$, i.e, o conjunto das matrizes de $M_n()R$ que comutam com todos os elementos de $\{e_{ij} \mid 1 \leqslant i, j \leqslant n\}$. Em particular, podemos identificar $Z(R)$ com $Z(M_n(R)) = \{\sum z e_{ii} \mid z \in Z(R)\}$. Esta afirmação é importante e caso haja interesse em verificar tal fato, consulte a página 22 do livro [18].

Similarmente, qualquer homomorfismo $\psi : R \to R_1$ estende-se de modo natural a um homomorfismo $\widehat{\psi} : M_n(R) \to M_n(R_1)$ dado por $\widehat{\psi}((r_{ij})) = (\psi(r_{ij}))$.

Suponha agora que M é um R-módulo livre n-dimensional com base $y_1, \ldots, y_n$; defina a função $\widehat{e}_{ij}$ em $\mathrm{End}_R M$ por $\widehat{e}_{ij}(\sum_{u=1}^n r_u y_u) = r_i y_j$, e para cada $r \in R$ defina a função $\widehat{r}$ em $\mathrm{End}_R M$ por $\widehat{r}(\sum_{u=1}^n r_u y_u) = \sum_{u=1}^n r_u r y_u$. Sendo $\widehat{R} = \{\widehat{r} \mid r \in R\}$, vemos que $\widehat{R} \approx R$ (basta verificar que $\widehat{r+s} = \widehat{r}+\widehat{s}$ e $\widehat{rs} = \widehat{r}\cdot\widehat{s}$ e depois definir $\theta : R \to \widehat{R}$ por $r \mapsto \widehat{r}$) e $\mathrm{End}_R M = \sum_{i,j=1}^n \widehat{R}\widehat{e}_{ij} \approx M_n(\widehat{R}) \approx M_n(R)$. O isomorfismo $\sum_{i,j=1}^n \widehat{R}\widehat{e}_{ij} \approx M_n(\widehat{R})$ é canônico, enquanto $M_n(\widehat{R}) \approx M_n(R)$ segue da observação feita no parágrafo anterior.

Mesmo quando M não é livre existe uma conexão entre $\mathrm{End}_R M$ e $M_n(R)$ a qual é obtida agora para o caso em que R é uma álgebra comutativa.

Seja C uma álgebra comutativa.

Proposição 1.9.1 (Procesi-Small)**.** *Suponha que M seja um módulo de dimensão n sobre C. Então* $\mathrm{End}_C M \leqslant_F M_n(C)$*. Na verdade, como uma C-álgebra,* $\mathrm{End}_C M$ *é uma imagem homomorfa de uma C-subálgebra de $M_n(C)$.*

Demonstração. Seja $\{x_1, \ldots, x_n\}$ um conjunto gerador de M, então $M = \sum_{i=1}^n Cx_i$. Para qualquer $\beta \in \mathrm{End}_C M$ podemos escrever $\beta(x_i) = \sum_{j=1}^n \beta_{ij} x_j$ para $\beta_{ij} \in C$ adequados, visto que $\beta(x_i) = \beta_{i1}x_1 + \beta_{i2}x_2 + \cdots + \beta_{in}x_n$ para cada $i \in \{1, \ldots, n\}$. Agora, seja $R = \{r = (c_{ij}) \in M_n(C) \mid$ para algum $\beta_r \in \mathrm{End}_C M,\ \beta_r(x_i) = \sum_{j=1}^n c_{ij}x_j\}$. Então R é uma subálgebra de $M_n(C)$ e a aplicação natural $r \mapsto \beta_r$ é um homomorfismo sobrejetor de R em $\mathrm{End}_C M$. Portanto $\mathrm{End}_C M \leqslant_F R \leqslant_F M_n(C)$. □

Claro que podemos definir o traço e o determinante para matrizes arbitrárias em $M_n(C)$ de maneira completamente análoga ao caso especial quando C é um corpo. Aqui estão alguns fatos úteis.

Observação 1.9.2. *Para $r = (r_{ij}) \in M_n(C)$,* $\mathrm{tr}(r \cdot e_{kl}) = r_{lk}\ \ 1 \leqslant k, l \leqslant n$*. Assim, se* $\mathrm{tr}(re_{ij}) = 0$ *para todos i, j, então $r = 0$.*

Observação 1.9.3. $[M_n(C), M_n(C)] = (\sum_{i\neq j} Ce_{ij} + \sum_{i=1}^{n-1} C(e_{ii} - e_{i+1,i+1})) = \{$*elementos de traço* $0\}$*, é um C-módulo de dimensão $n^2 - 1$. Uma matriz r em $[M_n(C), M_n(C)]$ é chamada* **matriz traço***. Quando C é o próprio corpo F, $[M_n(F), M_n(F)]$ é um espaço vetorial sobre F e é usualmente denotado por $sl_n(F)$.*

Seja R uma álgebra. Recorde que $f(X_1, \ldots, X_n) \in F\langle X\rangle$ é um polinômio central para R se não tem termo constante, $f(r_1, \ldots, r_n) \in Z(R)$ para quaisquer $r_1, \ldots, r_n \in R$, e $f(X_1, \ldots, X_n)$ não é uma identidade polinomial para R.

Em 1956 Kaplansky deu uma lista de problemas que motivou atividades de pesquisas significativas nas décadas subsequentes. Um de seus problemas era o seguinte.

Problema.(Kaplansky) *Existe um polinômio $f(X_1, \ldots, X_n)$, multi-homogêneo central para a álgebra de matrizes $M_k(F), k > 2$?*

A resposta para o problema de Kaplansky foi dada em 1972-1973 por Formanek e Razmyslov independentemente. Isto foi muito frutífero para a PI-teoria. Uma vez que resultados importantes foram estabelecidos ou suas demonstrações foram simplificadas usando polinômios centrais para as álgebras de matrizes.

Daremos a abordagem de Razmyslov para polinômios centrais com algumas modificações adicionais nas construções concretas. O método de Razmyslov usa a noção de identidade fraca e da transformação de Razmyslov.

Definição 1.9.4. *O polinômio $f(X_1, \ldots, X_n) \in F\langle X\rangle$ é uma* **identidade fraca** *para a álgebra de matrizes $M_k(F)$ se $f(a_1, \ldots, a_n) = 0$ para quaisquer matrizes $a_1, \ldots, a_n \in sl_k(F)$. Uma identidade fraca f é* **essencial** *se f não é uma identidade polinomial para $M_k(F)$.*

Exemplo 1.9.5. *Dada uma matriz $a \in M_2(F)$. Sabemos que se o traço de a é igual a 0, então a^2 é uma matriz escalar e $[a^2, b] = 0$ para todo $b \in M_2(F)$. Consequentemente $[X^2, Y]$ é uma identidade fraca essencial para $M_2(F)$.*

Exemplo 1.9.6. *$sl_n(F)$ é um espaço vetorial de dimensão $n^2 - 1$. Portanto quaisquer n^2 matrizes em $sl_n(F)$ são linearmente dependentes (L.D.) e o polinômio de Capelli*

$$C_{2n^2}(X_1, \ldots, X_{n^2}; Y_1, \ldots, Y_{n^2})$$

se anula quando são substituídos elementos de $sl_n(F)$ nas n^2 variáveis $X_1, \ldots X_{n^2}$ e nas outras variáveis $Y_1, \ldots, Y_{n^2}$ são substituídas matrizes arbitrárias de $M_n(F)$. Consequentemente C_{2n^2} é uma identidade fraca para $M_n(F)$. E é essencial porque a identidade de Capelli de grau mínimo pra $M_n(F)$ é $C_{2(n^2+1)}$ (veja a Proposição 1.8.3).

Lema 1.9.7. *Seja S_n o grupo das simetrias do conjunto $\{0, 1, \ldots, n-2, n\}$. Então*

$$w(X, Y_1, \ldots, Y_{n-1}) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) X^{\sigma(0)} Y_1 X^{\sigma(1)} Y_2 \cdots Y_{n-2} X^{\sigma(n-2)} Y_{n-1} X^{\sigma(n)}$$

é uma identidade fraca para $M_n(F)$ que se anula para todo $a \in sl_n(F)$ e $b_1, \ldots, b_{n-1} \in M_n(F)$.

Demonstração. Pelo teorema de Cayley-Hamilton, para qualquer $a \in M_n(F)$,

$$a^n - \operatorname{tr}(a) a^{n-1} + \cdots + (-1)^n \det(a) I = 0, \qquad \text{onde } I \text{ é a matriz identidade.}$$

Se $\operatorname{tr}(a) = 0$, então $I, a, a^2, \ldots, a^{n-2}, a^n$ são linearmente dependentes e

$$w(a, b_1, \ldots, b_{n-1}) = 0, \quad b_1, \ldots, b_{n-1} \in M_n(F).$$

Por outro lado, se $a = \sum_{p=1}^{n} \gamma_p e_{pp}$, então um cálculo nos dá que

$$w(a, e_{12}, e_{23}, \ldots, e_{n-1,n}) = \Delta(\gamma_1, \ldots, \gamma_n) e_{1n},$$

onde

$$\Delta(\gamma_1,\ldots,\gamma_n) = \begin{vmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ \gamma_1 & \gamma_2 & \gamma_3 & \cdots & \gamma_{n-1} & \gamma_n \\ \gamma_1^2 & \gamma_2^2 & \gamma_3^2 & \cdots & \gamma_{n-1}^2 & \gamma_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \gamma_1^{n-2} & \gamma_2^{n-2} & \gamma_3^{n-2} & \cdots & \gamma_{n-1}^{n-2} & \gamma_n^{n-2} \\ \gamma_1^n & \gamma_2^n & \gamma_3^n & \cdots & \gamma_{n-1}^n & \gamma_n^n \end{vmatrix}$$
$$= (\gamma_1 + \cdots + \gamma_n) \prod_{1\leqslant p<q\leqslant n} (\gamma_q - \gamma_p).$$

Daí $w(a, e_{12}, e_{23}, \ldots, e_{n-1,n}) \neq 0$ se os autovalores de a são dois a dois distintos e seu traço é não-nulo. Portanto $w(X, Y_1, \ldots, Y_{n-1})$ não é uma identidade polinomial "ordinária" para $M_n(F)$. □

Lema 1.9.8. *Se $f(X_1, \ldots, X_m)$ é uma identidade fraca para $M_n(F)$, então*

$$f([X_1, X_{m+1}], [X_2, X_{m+2}], \ldots, [X_m, X_{2m}])$$

é uma identidade ordinária.

Demonstração. Já que $\mathrm{tr}([a, b]) = 0$ para quaisquer $a, b \in M_n(F)$, obtemos que $f(X_1, \ldots, X_m)$ se anula em $M_n(F)$ quando substituímos as variáveis por comutadores. Isto significa que

$$f([X_1, X_{m+1}], [X_2, X_{m+2}], \ldots, [X_m, X_{2m}])$$

é uma identidade polinomial ordinária para a álgebra $M_n(F)$. □

Recordemos algumas propriedades elementares do traço de matrizes.

Lema 1.9.9. *Qualquer matriz em $M_n(F)$ cujo traço é igual a zero é uma soma de $n^2 - 1$ comutadores.*

Demonstração. Considere a base de $sl_n(F)$ consistindo dos elementos e_{ij}, $i \neq j$, e $e_{11} - e_{ii}$, $i = 2, \ldots, n$. As igualdades

$$e_{ij} = [e_{ij}, e_{jj}], i \neq j, \quad \text{e} \quad [e_{1i}, e_{i1}] = e_{11} - e_{ii}$$

nos dão que os elementos da base são comutadores. E uma vez que $\alpha[r, s] = [\alpha r, s], \alpha \in F$, o lema segue imediatamente. □

Lema 1.9.10. *Definindo uma forma bilinear simétrica no espaço vetorial $V = M_n(F)$ por*

$$\langle a, b\rangle = \mathrm{tr}(ab), \quad a, b \in M_n(F).$$

Esta forma é não-degenerada, i.e., $\langle u, V\rangle = 0$ implica $u = 0$

Demonstração. O lema segue do fato de que sempre podemos multiplicar a matriz não-nula $u \in M_n(F)$ por uma matriz adequada $a \in M_n(F)$ a fim de obter $\mathrm{tr}(ua) \neq 0$. □

Agora introduzimos a transformação de Razmyslov e provaremos o seu lema. Estas foram as principais ferramentas utilizadas por Razmyslov na construção de seus polinômios centrais.

Definição 1.9.11. *Seja $f(X, Y_1, \ldots, Y_m)$ um polinômio em $F\langle X, Y_1, \ldots, Y_m\rangle$ que é linear na variável X. Escrevendo f na forma $f = \sum g_i X h_i$, onde $g_i, h_i \in F\langle Y_1, \ldots, Y_m\rangle$, a* **transformação de Razmyslov** *de f é o polinômio*

$$f^*(X, Y_1, \ldots, Y_m) = \sum h_i X g_i.$$

Exemplo 1.9.12. *Se $f(X, Y_1, Y_2) = [XY_1 + Y_1X, Y_2] = 1\cdot X\cdot Y_1Y_2 + Y_1\cdot X\cdot Y_2 - Y_2\cdot X\cdot Y_1 - Y_2Y_1\cdot X\cdot 1$, então*

$$\begin{aligned} f^*(X, Y_1, Y_2) &= Y_1Y_2 \cdot X \cdot 1 + Y_2 \cdot X \cdot Y_1 - Y_1 \cdot X \cdot Y_2 - 1 \cdot X \cdot Y_2Y_1 \\ &= [Y_2, X]Y_1 + Y_1[Y_2, X]. \end{aligned}$$

Teorema 1.9.13 (Lema de Razmyslov)**.** *Sejam $f = f(X, Y_1, \ldots, Y_m) \in F\langle X, Y_1 \ldots, Y_m\rangle$ um polinômio homogêneo de grau 1 em X e $f^* = f^*(X, Y_1, \ldots, Y_m)$ o polinômio obtido pela transformação de Razmyslov. Vale que:*

(i) Se f é uma identidade polinomial para $M_n(F)$, então f^* é também uma identidade polinomial para $M_n(F)$.

(ii) Se f é uma identidade fraca para $M_n(F)$, então f^* é uma identidade fraca ou a avaliação de f^* em $sl_n(F)$ resulta apenas em matrizes escalares.

(iii) Se f é uma identidade fraca essencial de $M_n(F)$ tal que

$$f([X, Z], Y_1, \ldots, Y_m)$$

é uma identidade polinomial para $M_n(F)$, então f^* é um polinômio central para $M_n(F)$.

Demonstração. (i) Seja

$$f = \sum g_i X h_i, \quad g_i, h_i \in F\langle Y_1, \ldots, Y_m\rangle.$$

Então, pelo Lema 1.9.10, o traço é não-degenerado e f é uma identidade polinomial para $M_n(F)$ se, e somente se, $\mathrm{tr}(fZ) = 0$ é uma identidade traço (i.e., se anula em $M_n(F)$). Já que $\mathrm{tr}(uv) = \mathrm{tr}(vu)$, obtemos

$$\begin{aligned} \mathrm{tr}(f(X, Y_1, \ldots, Y_m)Z) &= \mathrm{tr}(fZ) \\ &= \sum \mathrm{tr}(g_i X h_i Z) \\ &= \sum \mathrm{tr}(h_i Z g_i X) \\ &= \mathrm{tr}(f^*(Z, Y_1, \ldots, Y_m)X). \end{aligned}$$

Consequentemente $f(X, Y_1, \ldots, Y_m)$ é uma identidade polinomial para $M_n(F)$ se, e somente se, $\mathrm{tr}(f^*(Z, Y_1, \ldots, Y_m)X)$ é uma identidade traço que, novamente pelo Lema 1.9.10, é equivalente ao

fato de que $f^*(Z, Y_1, \ldots, Y_m)$ é uma identidade polinomial.

(ii) Seja

$$f(X, Y_1, \ldots, Y_m) = \sum g_i(Y_1, \ldots, Y_m) X h_i(Y_1, \ldots, Y_m)$$

uma identidade fraca para $M_n(F)$. Em f substituímos X por $[X, Z]$, cada Y_j por uma soma $\sum[Y_{jk}, Z_{jk}]$ de $n^2 - 1$ comutadores $[Y_{jk}, Z_{jk}]$, $k = 1, \ldots, n^2 - 1$, e obtemos

$$\tilde{f} = f\left([X, Z], \sum_{k=1}^{n^2-1} [Y_{1k}, Z_{1k}], \ldots, \sum_{k=1}^{n^2-1} [Y_{mk}, Z_{mk}]\right)$$

é uma identidade polinomial para $M_n(F)$. Como

$$\tilde{f} = \sum \tilde{g_i}[X, Z]\tilde{h_i} = \sum(\tilde{g_i} X Z \tilde{h_i} - \tilde{g_i} Z X \tilde{h_i}),$$

onde

$$\tilde{g_i} = g_i\Big(\sum[Y_{1k}, Z_{1k}], \ldots, \sum[Y_{mk}, Z_{mk}]\Big),$$

$$\tilde{h_i} = h_i\Big(\sum[Y_{1k}, Z_{1k}], \ldots, \sum[Y_{mk}, Z_{mk}]\Big),$$

pelo item (i) obtemos que

$$\begin{aligned}
\tilde{f^*} &= \sum(Z\tilde{h_i} X \tilde{g_i} - \tilde{h_i} X \tilde{g_i} Z) \\
&= \Big[Z, \sum \tilde{h_i} X \tilde{g_i}\Big] \\
&= \Big[Z, f^*\Big(X, \sum[Y_{1k}, Z_{1k}], \ldots, \sum[Y_{mk}, Z_{mk}]\Big)\Big]
\end{aligned}$$

é também uma identidade polinomial para $M_n(F)$. Aplicando o Lema 1.9.9 obtemos que

$$[Z, f^*(X, Y_1, \ldots, Y_m)]$$

se anula quando são substituídos elementos de $sl_n(F)$ nas variáveis $Y_1, \ldots, Y_m$ e nas variáveis X, Z são substituídos elementos de $M_n(F)$. Consequentemente $f^*(X, Y_1, \ldots, Y_m)$ se anula, ou quando são subtituídas matrizes traço $n \times n$ nas variáveis $Y_1, \ldots, Y_m$ e qualquer matriz em X o resultado é uma matriz escalar. (Se a identidade fraca f é multilinear, é suficiente subtituir Y_j por $[Y_j, Z_j]$. Foi necessário a soma a fim de tratar o caso de um corpo arbitrário.)

(iii) Seja f uma identidade fraca essencial para $M_n(F)$ tal que $f([X, Z], Y_1, \ldots, Y_m)$ é uma identidade polinomial. Como no item (ii),

$$f^*([X, Z], Y_1, \ldots, Y_m) = [Z, f^*(X, Y_1, \ldots, Y_m)]$$

é uma identidade polinomial. Consequentemente $f^*(X, Y_1, \ldots, Y_m)$ avaliado em $M_n(F)$ assume valores escalares (i.e. matrizes escalares). Já que f não é uma identidade polinomial, concluímos que $f^*(r, r_1, \ldots, r_m) \neq 0$ para certos $r, r_1, \ldots, r_m \in M_n(F)$ e isto significa que f^* é um polinômio central não-trivial. □

Teorema 1.9.14 (Razmyslov). *Sejam $C_{2n^2}(X_1,\ldots,X_{n^2};Y_1,\ldots,Y_{n^2})$ o polinômio de Capelli e*

$$\begin{aligned} f &= f(X,Z_1,\ldots,Z_{2n^2-2},Y_1,\ldots,Y_{n^2}) \\ &= C_{2n^2}(X,[Z_1,Z_2],\ldots,[Z_{2n^2-3},Z_{2n^2-2}];Y_1,\ldots,Y_{n^2}). \end{aligned}$$

A transformação de Razmyslov f^* aplicada a f é um polinômio multilinear central para $M_n(F)$ sobre qualquer corpo F.

Demonstração. Pelo Exemplo 1.9.6, a identidade de Capelli C_{2n^2} é uma identidade fraca para $M_n(F)$ e C_{2n^2} se anula quando substituímos elementos de $sl_n(F)$ nas n^2 variáveis $X_1,\ldots,X_{n^2}$ e nas outras variáveis $Y_1,\ldots,Y_{n^2}$ são substituídas matrizes arbitrárias de $M_n(F)$. Já que os comutadores de elementos de $M_n(F)$ são elementos de $sl_n(F)$, f é também uma identidade fraca que se anula quando substituímos X por elementos de $sl_n(F)$ e $Y_1,\ldots,Y_{n^2}$ e $Z_1,\ldots,Z_{2n^2-2}$ são substituídas por matrizes quaisquer. Consequentemente,

$$f([X,Z],Z_1,\ldots,Z_{2n^2-2},Y_1,\ldots,Y_{n^2})$$

é uma identidade polinomial. A fim de aplicar o Lema de Razmyslov, é suficiente mostrar que

$$f(X,Z_1,\ldots,Z_{2n^2-2},Y_1,\ldots,Y_{n^2})$$

não se anula em $M_n(F)$. Pela Proposição 1.8.3, $C_{2n^2}(X_1,\ldots,X_{n^2};Y_1,\ldots,Y_{n^2})$ não é uma identidade polinomial de $M_n(F)$. Já que C_{2n^2} é anti-simétrico nas variáveis X_i's, então não se anula se substituirmos $X_1,\ldots,X_{n^2}$ por elementos de qualquer base $\{r_1,\ldots,r_{n^2}\}$ de $M_n(F)$ e $Y_1,\ldots,Y_{n^2}$ por $s_1,\ldots,s_{n^2}$ adequados. Fixe a base

$$\{r_1,\ldots,r_{n^2}\}=\{e_{11},e_{11}-e_{ii},e_{jk}\mid i=2,\ldots,n,\quad j\neq k,\quad j,k=1,\ldots,n\},$$

onde denotamos e_{11} por r_1 e os outros elementos por $r_2,\ldots,r_{n^2}$. Então

$$C_{2n^2}(r_1,\ldots,r_{n^2};s_1,\ldots,s_{n^2})\neq 0.$$

Uma vez que $r_2,\ldots,r_{n^2}$ são comutadores, $r_u=[a_u,b_u]$, $u=2,\ldots,n^2$, daí tem-se

$$C_{2n^2}(r_1,\ldots,r_{n^2};s_1,\ldots,s_{n^2})=f(r_1,[a_2,b_2],\ldots,[a_{n^2},b_{n^2}],s_1,\ldots,s_{n^2})\neq 0,$$

e isto completa a demonstração. □

A fim de obter polinômios centrais pelo método de Razmyslov, precisamos de uma identidade fraca essencial $w(X_1,\ldots,X_m)$ para $M_n(F)$. Então $w(X_1,\ldots,X_m)$ não é uma identidade polinomial e $w([Y_1,Z_1],\ldots,[Y_m,Z_m])$ é. Consequentemente existe um u (se necessário, considerando uma linearização de w) tal que $f=w([Y_1,Z_1],\ldots,[Y_u,Z_u],X_{u+1},X_{u+2}\ldots,X_m)$ não se anula em $M_n(F)$ e

$$w([Y_1,Z_1],\ldots,[Y_u,Z_u],[Y_{u+1},Z_{u+1}],X_{u+2}\ldots,X_m)$$

é uma identidade polinomial. Então, aplicando a transformação de Razmyslov a f com respeito a X_{u+1} obtemos um polinômio central.

Exemplo 1.9.15. *Pelo Exemplo 1.9.5,*

$$w(X,Y) = [X^2, Y]$$

é uma identidade fraca essencial para $M_2(F)$*. Sua linearização*

$$w_1(X,Y,Z) = [XZ + ZX, Y] = XZY + ZXY - YXZ - YZX$$

é também uma identidade fraca. Substituindo em $w_1(X, Y, [Z_1, Z_2])$ *elementos adequados de* $M_2(F)$*, obtemos que*

$$f(X,Y,Z_1,Z_2) = w_1(X,Y,[Z_1,Z_2])$$

não é uma identidade ordinária para $M_2(F)$*. Por exemplo,*

$$w_1(e_{11} + e_{22}, e_{22}, [e_{11}, e_{12}]) = 2[e_{12}, e_{22}] = 2e_{12} \neq 0.$$

Por outro lado, $w_1([X,V], Y, [Z_1, Z_2])$ *é uma identidade polinomial (*V *é uma variável). Consequentemente a transformação de Razmyslov* f^* *com respeito a* X *aplicada em* $f(X, Y, Z_1, Z_2)$ *é um polinômio central. Expressamos* f *na forma*

$$f = [X[Z_1,Z_2] + X, Y] = X[Z_1,Z_2]Y + [Z_1,Z_2]XY - YX[Z_1,Z_2] - Y[Z_1,Z_2]X$$

e o polinômio central obtido é

$$\begin{aligned} g(X,Y,Z_1,Z_2) = f^* &= [Z_1,Z_2]YX + YX[Z_1,Z_2] - [Z_1,Z_2]XY - XY[Z_1,Z_2] \\ &= [Z_1,Z_2][Y,X] + [Y,X][Z_1,Z_2]. \end{aligned}$$

Se fizermos $Z_2 = X$ *e* $Z_1 = Y$*, obtemos*

$$g(X,Y,Y,X) = 2[X,Y]^2$$

o qual sabemos ser um polinômio central para $M_2(F)$*.*

Finalizamos esta seção enunciando um lema que será útil na demonstração de um teorema de vido a Rowen que aparece no capítulo seguinte.

Lema 1.9.16. *Se* f *é um polinômio central de* $M_n(F)$*, então* f *é uma identidade polinomial de* $M_{n-1}(F)$*.*

Capítulo 2

Teoremas de Estrutura de PI-álgebras

Neste capítulo estão os principais teoremas de estrutura que serão utilizados posteriormente. A fim de que o texto não se torne rígido, apresentamos alguns resultados básicos (porém importantes) como, por exemplo, o Lema de Schur, etc.

Os dois principais resultados que aparecem neste capítulo são o Teorema de Kaplansky, considerado por muitos o ponto de partida da teoria de PI-álgebras, e o famoso Teorema de Posner que diz respeito às álgebras primas satisfazendo uma identidade polinomial.

Formalmente, seguiremos o roteiro do livro [8] procurando manter um equilíbrio entre [9] e [17].

Antes de começar faremos a seguinte convenção: neste capítulo o efeito de uma aplicação f em x, usualmente denotado por $f(x)$, será denotado por fx. Apenas quando quisermos enfatizar manteremos a notação usual. Além disso, vamos escrever a composição de funções ψ e φ simplesmente por $\psi\varphi$.

2.1 Densidade

Sejam R uma álgebra e M um R-módulo. Então $\mathrm{End}_R M$ é uma álgebra. Claro que $M^{(n)}$ é um R-módulo com operações dadas componente a componente.

Suponha que $\Phi : (\mathrm{End}_R M)^{(n)} \to \mathrm{Hom}_R(M^{(n)}, M)$ é uma função que associa cada n-upla $(f_1, \ldots, f_n)$ a um homomorfismo de R-módulos f definido por $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} f_i x_i$. Escreva $\pi_i : M^{(n)} \to M$ para a projeção sobre a i-ésima componente e $\theta_i : M \to M^{(n)}$ para a aplicação $\theta_i x = (0, \ldots, 0, x, 0, \ldots, 0)$ onde x aparece na i-ésima componente. Então $\Phi(f_1, \ldots, f_n) = \sum f_i \pi_i$. Definindo $\Psi : \mathrm{Hom}_R(M^{(n)}, M) \to (\mathrm{End}_R M)^{(n)}$ por $\Psi f = (f\theta_1, \ldots, f\theta_n)$, vemos que $\Phi\Psi f = \sum f\theta_i\pi_i = f \sum \theta\pi_i = f$ e $\Psi\Phi(f_1, \ldots, f_n) = \Psi \sum f_i\pi_i = (f_1, \ldots, f_n)$. Portanto $\Phi = \Psi^{-1}$ e Ψ, Φ são ambos isomorfismos. Em resumo, $(\mathrm{End}_R M)^{(n)} \approx \mathrm{Hom}_R(M^{(n)}, M)$. Vale notar que $(\mathrm{End}_R M)^{(n)} \approx \mathrm{End}_R M^{(n)}$. Basta definir uma função $\Omega : (\mathrm{End}_R M)^{(n)} \to \mathrm{End}_R M^{(n)}$ que associa cada n-upla $(f_1, \ldots, f_n)$ a um homomorfismo $f \in \mathrm{End}_R M^{(n)}$ definido por $f(x_1, \ldots, x_n) = (f_1 x_1, \ldots, f_n x_n)$. A função $\Lambda : \mathrm{End}_R M^{(n)} \to (\mathrm{End}_R M)^{(n)}$ que associa cada $g \in (\mathrm{End}_R M)^{(n)}$ à n-upla $(\pi_1 g\theta_1, \ldots, \pi_n g\theta_n)$ é a inversa de Ω e além disso Ω e Λ são homomorfismos de anéis.

Diz-se que um R-módulo M é **irredutível** (ou simples) se $RM \neq (0)$ e M não possui outros submódulos além dos triviais (0) e M; assim M é irredutível se, e só se, $Ry = M$ para cada

$y \neq 0$ em M. Por exemplo, $\mathbb{Z}_3$ é irredutível como $\mathbb{Z}$-módulo. Claro que M pode ser visto como $\mathrm{End}_R M$-módulo com a multiplicação escalar definida de modo natural.

Lema 2.1.1 (Lema de Schur)**.** *(i) Se M_1, M_2 são R-módulos irredutíveis, então todo $\psi \neq 0$ em $\mathrm{Hom}_R(M_1, M_2)$ é um isomorfismo.*

(ii) Se M é irredutível, então $\mathrm{End}_R M$ é um anel de divisão.

Demonstração. (i) Dado $\psi \neq 0$ em $\mathrm{Hom}_R(M_1, M_2)$, $\psi(M_1)$ é um submódulo não-nulo de M_2; como M_2 é irredutível, $\psi(M_1) = M_2$. Do mesmo modo $ker(\psi)$ é um submódulo próprio de M_1 e a irredutibilidade de M_1 implica que $ker(\psi) = (0)$, provando que ψ é um isomorfismo.
(ii) Se $\varphi \neq 0$ em $\mathrm{End}_R(M)$, então φ é um isomorfismo pelo item (i), e não é difícil checar que $\varphi^{-1} \in \mathrm{End}_R M$. □

Diferente do uso comum, atribuiremos o termo **espaço vetorial** a um módulo sobre um anel de divisão. Assim, se M é um R-módulo irredutível, M é também um espaço vetorial sobre $D = \mathrm{End}_R M$.

Definição 2.1.2. *Sejam D um anel de divisão qualquer, V um D-espaço vetorial e S um subconjunto não-vazio de $\mathrm{End}_D V$. O conjunto S é* **denso** *em $\mathrm{End}_D V$ se para qualquer quantidade finita de vetores D-independentes $v_1, \ldots, v_n$ e vetores arbitrários $w_1, \ldots, w_n \in V$, existir $s \in S$ (dependendo de $w_1, \ldots, w_n$) tal que*

$$sv_i = w_i, \;\; i = 1, \ldots, n.$$

Observação 2.1.3. *Se $[V : D]$, a dimensão de V sobre D, é igual a $n < \infty$, então $\mathrm{End}_D V$ é o único conjunto denso em $\mathrm{End}_D V$.*

De fato, por absurdo, seja $S \subset \mathrm{End}_D V$ denso em $\mathrm{End}_D V$ e seja $f \in \mathrm{End}_D V$. Sejam $v_1, \ldots, v_n \in V$, D-independentes ($\{v_1, \ldots, v_n\}$ forma uma base de V) e $w_i = f(v_i)$, $i = 1, \ldots, n$. Como S é denso, existe $s \in S$ tal que $sv_i = w_i$. Consequentemente, já que f e s coincidem em uma base, $f = s \in S$, i.e., $\mathrm{End}_D V \subseteq S$ (Absurdo). Portanto S não é denso.

Observação 2.1.4. *Seja M um R-módulo e H um subconjunto de M. Definimos o* **aniquilador** *de H em R como sendo o conjunto $\mathrm{Ann}_R H = \{r \in R \mid rH = (0)\}$. Existe um homomorfismo natural $\psi : R \to \mathrm{End}_{\mathbb{Z}} M$ que associa r a ψ_r, onde $\psi_r : m \mapsto rm$ para todo $m \in M$; $\psi_r = 0$ se, e só se, $rM = (0)$, portanto $ker(\psi) = \mathrm{Ann}_R M$. Assim, $R/ker(\psi)$ é uma álgebra isomorfa a alguma subálgebra de $\mathrm{End}_{\mathbb{Z}} M$.*

O módulo M é um grupo abeliano e $\mathrm{End}_{\mathbb{Z}} M$ denota o conjunto dos endomorfismos de M visto como um grupo. A notação mais frequente para este conjunto é $E(M)$ e é esta que usaremos a partir de agora (o mesmo vale para um anel).

Dizemos que M é um R-módulo **fiel** quando $\mathrm{Ann}_R M = (0)$. Assim, se M é fiel podemos considerar $R \subseteq E(M)$.

O próximo resultado é devido a Jacobson e é conhecido como Teorema da Densidade.

Teorema 2.1.5 (Teorema da Densidade)**.** *Suponha que M é um R-módulo fiel e irredutível e seja $D = \mathrm{End}_R M$. Se $x_1, \ldots, x_n$ são elementos D-independentes de M (n qualquer) e $y_1, \ldots, y_n$ são elementos arbitrários de M, então, para r em R conveniente, $rx_i = y_i$ para todo i, $1 \leqslant i \leqslant n$.*

Demonstração. Faremos indução em n. Para $n = 1$, dado $x \neq 0$ em M, temos que $Rx = M$. Logo, dado qualquer $y \in M$, existe $r_y \in R$ tal que $r_y x = y$. Assuma que o teorema valha para $n - 1$. Então, vendo $(x_1, \ldots, x_{n-1})$ como elementos do R-módulo $M^{(n-1)}$, temos que $M^{(n-1)} = R(x_1, \ldots, x_{n-1})$.

Afirmação: Existe $r_n \in R$ tal que $r_n x_n \neq 0$ e $r_n x_i = 0$ para todo $i \neq n$.

De fato, caso contrário, i.e., negando a *Afirmação* temos que, como M é fiel, para cada $r \in R - \{0\}$ existe $i \neq n$ tal que $rx_i \neq 0$. Em outras palavras, a aplicação $\psi : R(x_1, \ldots, x_{n-1}) \to M$ dada por $\psi(r(x_1, \ldots, x_{n-1})) = rx_n$ é um homomorfismo de R-módulos bem definido, implicando que $\psi \in \mathrm{Hom}_R(M^{(n-1)}; M) \approx (\mathrm{End}_R M)^{(n-1)} = D^{(n-1)}$. O isomorfismo anterior nos permite escrever ψ como $(d_1, \ldots, d_{n-1}) \in D^{(n-1)}$, daí temos que $x_n = \psi(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{n-1} d_i x_i$, contradizendo o que havíamos assumido sobre a D-independência de $x_1, \ldots, x_n$.

A *Afirmação* está portanto estabelecida e, por simetria, para cada j existe r_j com $r_j x_j \neq 0$ e $r_j x_i = 0$ para todo $i \neq j$. Uma vez que M é irredutível, temos que existe t_j tal que $t_j(r_j x_j) = y_j$. Seja $r = \sum_{j=1}^{n} t_j r_j$. Então, para cada i, $rx_i = t_i r_i x_i = y_i$. □

Existem outras formas de afirmar o Teorema da Densidade. Faremos isso no corolário abaixo.

Corolário 2.1.6. *Suponha que M é um R-módulo fiel e irredutível, $n \in \mathbb{Z}^+$, e $x_1, \ldots, x_n \in M$ são arbitrários. Seja $D = \mathrm{End}_R M$, e suponha que V é um D-subespaço de dimensão finita de M que **não** contém x_1. Então existem elementos $d_1 = 1, d_2, \ldots, d_n$ em D satisfazendo a seguinte propriedade:*

Para cada $y \in M$ existe $r \in R$ tal que $rV = 0$ e $rx_i = d_i y$, $1 \leqslant i \leqslant n$.

Demonstração. Seja W o D-subespaço de M gerado por V e $\{x_1, \ldots, x_n\}$. Tome uma base de V e estenda (sobre D) à uma base $w_1, \ldots, w_k$ de W de modo que $w_1 = x_1$. Escreva $x_i = \sum_{j=1}^{k} d_{ij} w_j$ para d_{ij} em D, e ponha $d_i = d_{i1}$, $1 \leqslant i \leqslant n$. Assim $d_1 = 1$. Pelo Teorema da Densidade, existe $r \in R$ tal que $rx_1 = d_1 y$ e $rw_j = 0$, $2 \leqslant j \leqslant k$. Portanto, para cada i, $rx_i = \sum_{j=1}^{k} d_{ij}(rw_j) = d_i y$. □

Corolário 2.1.7. *Suponha que R possui um módulo fiel e irredutível M. Seja $D = \mathrm{End}_R M$. Então uma das seguintes afirmações vale:*

(i) *$[M : D] = n < \infty$ para algum $n \in \mathbb{Z}^+$, em cujo caso $R \approx M_n(D)$.*

(ii) *Para todo $n \in \mathbb{Z}^+$, existe uma subálgebra de R que tem $M_n(D)$ como imagem homomorfa.*

Demonstração. (i) Se $[M : D] = n$, escolha uma base $\{w_1, \ldots, w_n\}$ de M sobre D. Dado $\psi \in \mathrm{End}_D M$, pelo Teorema da Densidade, existe $r \in R$ tal que $rw_i = \psi(w_i)$ para todo i e isto implica que a função

$$\begin{array}{rccccccc} \Psi : & R & \longrightarrow & \mathrm{End}_D M & & & & \\ & r & \mapsto & \widehat{r} & : & M & \to & M \\ & & & & & w_i & \mapsto & rw_i \end{array}$$

é um homomorfismo sobrejetor de anéis. E se r é tal que $0 = \Psi(r) = \widehat{r}$, então $r = 0$, pois M é fiel. Portanto $R \approx \mathrm{End}_D M \approx M_n(D)$.
(ii) Se $[M : D]$ não é finita, dado qualquer $n \in \mathbb{Z}^+$ e elementos D-independentes $x_1, \ldots, x_n$ em M, seja $V = Dx_1 + \cdots + Dx_n$ e $R' = \{r \in R \mid rV \subseteq V\}$. Claro que $R' \neq \varnothing$, pois $0, 1 \in R'$. Pelo Teorema da Densidade, qualquer transformação D-linear de V em V pode ser induzida por um elemento de R. Portanto, existe um homomorfismo natural sobrejetor h de R' em $\mathrm{End}_D V$. □

A recíproca do Teorema da Densidade é também verdadeira (e óbvia). Isto é, se M é um espaço vetorial sobre um anel de divisão D e R é um subanel denso em $\mathrm{End}_D M$, então M é um R-módulo fiel e irredutível. De fato, como um anel de transformações lineares em M, R tem M como módulo fiel e se N é um R-submódulo não-nulo de M, dado $n \neq 0$ em N e $m \in M$, existe $r \in R$ tal que $m = rn \in N$. Daí $M \subseteq N$. Portanto, M é irredutível como R-módulo.

Definição 2.1.8. *Um anel R é dito* **artiniano** *(à esquerda) se qualquer família de ideais à esquerda tem um elemento minimal.*

Exemplo 2.1.9. *O anel $\mathbb{Z}/n\mathbb{Z}$ é artiniano, bem como, para todo $k \in \mathbb{Z}^+$, $F[x]/(x^k)$ é artiniano.*

Observação 2.1.10. *Um anel é artiniano se, e só se, qualquer cadeia decrescente de ideais à esquerda de R, $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$ torna-se estacionária, i.e., a partir de algum índice todos os I_j's são iguais.*

Observação 2.1.11. *Se R é uma álgebra de dimensão finita sobre um corpo, então R é artiniana como álgebra. Ser artiniano como álgebra* **não** *implica ser artiniano como anel. Considere a $\mathbb{Q}$-álgebra $R = \mathbb{Q}e_{12}$, onde e_{12} é a matriz unidade 2×2 que possui 1 na entrada $(1, 2)$ e zero nas demais. Se considerarmos R como um anel, a cadeia de ideais $(2\mathbb{Z})e_{12} \supseteq (4\mathbb{Z})e_{12} \supseteq (8\mathbb{Z})e_{12} \supseteq \cdots$ não estaciona. Já como álgebra, R é artiniana.*

Para qualquer $x \in \mathbb{R}$, denotamos por $[\,x\,]$ o maior inteiro de x, i.e., o maior número inteiro menor do que ou igual a x. Por exemplo, $[1/2] = 0$, $[0,999\ldots] = 1$ e $[\,\pi\,] = [3,14\ldots] = 3$.

Proposição 2.1.12. *Se R tem um módulo fiel e irredutível M, com $D = \mathrm{End}_R M$, e se R satisfaz uma identidade polinomial f de grau d, então $[M : D] \leqslant [d/2]$, assim $R \approx M_{[M:D]}(D)$.*

Demonstração. Suponha que $[M : D] > [d/2]$. Pelo corolário anterior, para algum $n > [d/2]$, tem-se que $R \approx M_n(D)$ ou $M_n(D)$ é imagem homomorfa de uma subálgebra de R. Em qualquer caso f é uma identidade polinomial de $M_n(D)$. Mas isso é impossível pois, pelo Teorema 1.8.4 (Amitsur-Levitzki), $M_n(D)$ não satisfaz identidade de grau menor do que $2n$. Portanto $[M : D] \leqslant [d/2]$. □

Um anel é **primitivo** se possui um módulo fiel irredutível. Todo corpo F é um F-módulo fiel e irredutível e, portanto, é um exemplo óbvio de anel primitivo.

Exemplo 2.1.13. *Seja F um corpo. O conjunto $L = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \;\middle|\; a, b \in F \right\}$ é um ideal à esquerda de $M_2(F)$ que é um $M_2(F)$-módulo irredutível. Além disso, se $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in M_2(F)$ é tal que*

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} a & a \\ b & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

então, tomando $a = 0$ *e* $b = 1$*, temos que* $s = u = 0$ *e para* $a = 1, b = 0$ *obtemos* $r = t = 0$*. Daí,* L *é um* $M_2(F)$*-módulo fiel. Logo* $M_2(F)$ *é primitivo.*

Um anel R é dito **primo** se $aRb = 0,\ a, b \in R$, implicar que $a = 0$ ou $b = 0$. O anel $\mathbb{Z}$ é um exemplo imediado de anel primo. Da definição segue que o centro de um anel primo, é um domínio de integridade e portanto possui um corpo de frações. Usaremos isto quando formos falar de localização central.

Observação 2.1.14. *Um anel* R *é primo se, e só se uma das condições vale:*

(1) $\mathrm{Ann}_R L = (0)$ *para todo* $(0) \neq L \lhd_l R$*.*

(2) *para* I, J *ideais de* R *com* $IJ = (0)$ *tem-se* $I = (0)$ *ou* $J = (0)$ *(equivalentemente,* $IJ \neq (0)$ *para quaisquer ideais não-nulos* I, J *de* R*).*

Teorema 2.1.15 (Goldie)**.** *Se um anel* R *é primitivo, então é primo.*

Demonstração. Sejam M um R-módulo fiel e irredutível e I, J ideais não-nulos de R. Então JM é um submódulo não-nulo de M, implicando que $JM = M$; assim $I(JM) = IM \neq (0)$, portanto $IJ \neq (0)$. O item 2 da observação anterior garante que R é primo. □

Seja R qualquer anel e $E(R)$, como antes, o anel dos endomorfismos de R visto como um grupo aditivo. Se $a \in R$, definimos $T_a : R \to R$ por $T_a x = xa$ e $L_a : R \to R$ por $L_a x = ax$. Para quaisquer $a, b \in R$, as aplicações T_a, L_b estão em $E(R)$. Seja $B(R)$ o subanel de $E(R)$ gerado por todos os T_a e L_b de R para $a, b \in R$. $B(R)$ é chamado **anel de multiplicação** de R.

Claramente R é um módulo sobre $B(R)$. Seja I um $B(R)$-submódulo de R. Veremos que $I \lhd R$. Dados $x \in I$, $y \in R$, como $T_y, L_y \in B(R)$ e I é um submódulo de $B(R)$, temos que $xy = T_y x \in I$ e $yx = L_y x \in I$. Em resumo, os $B(R)$-submódulos de R são meramente os ideais de R. Portanto, R é irredutível como $B(R)$-módulo se, e só se, R simples.

Definição 2.1.16. *Seja* M *um* R*-módulo. O* **comutador** *de* R *em* M *é o conjunto* $\{\psi \in E(R) \mid L_b\psi = \psi L_b$ *para todo* $b \in R\}$*.*

Note que o comutador de R em M é, na verdade, o anel $\mathrm{End}_R M$. Nestes termos, o Lema de Schur diz que o comutador de um R-módulo irredutível é um anel de divisão.

Definição 2.1.17. *O* **centróide** *de* R*, denotado por* $C(R)$*, é o conjunto dos elementos de* $E(R)$ *que comutam com cada elemento de* $B(R)$*.*

Perceba que para qualquer R-módulo M vale que $C(R) \subseteq \mathrm{End}_R M$.

Lema 2.1.18. *Se* $R^2 = R$*, então* $C(R)$ *é comutativo.*

Demonstração. Suponha que $\sigma, \tau \in C(R)$. Para quaisquer $x, y \in R$ temos

$$\sigma(xy) = \sigma(L_x y) = L_x(\sigma y) = x(\sigma y) \quad (*)$$

e

$$\begin{aligned}(\tau\sigma)(xy) &= \tau(\sigma(xy)) = \tau(x(\sigma y)) = \tau(T_{\sigma y}x) = T_{\sigma y}(\tau x)\\ &= (\tau x)(\sigma y) = \sigma((\tau x)y) = \sigma(T_y(\tau x)) = \sigma((T_y\tau)x)\\ &= \sigma((\tau T_y)x) = \sigma(\tau(xy)) = (\sigma\tau)(xy)\end{aligned}$$

Portanto $(\tau\sigma - \sigma\tau)(xy) = 0$. Como $R^2 = R$, dado $u \in R$, $u = \sum x_i y_i$ consequentemente $(\tau\sigma - \sigma\tau)u = (\tau\sigma - \sigma\tau)(\sum x_i y_i) = \sum(\tau\sigma - \sigma\tau)(x_i y_i) = 0$. Isto nos dá que $(\tau\sigma - \sigma\tau) = 0$ e o resultado segue. □

Definição 2.1.19. *O* **radical de Jacobson** *de um anel R, denotado por* $\mathrm{Jac}(R)$*, é a interseção de todos os ideais de R à esquerda que são maximais.*

Como um exemplo, calculemos $\mathrm{Jac}(\mathbb{Z}_4)$. O anel $\mathbb{Z}_4$ é comutativo, assim todo ideal à esquerda é bilateral. Segue do Teorema da Correspondência para Anéis que os ideais maximais de $\mathbb{Z}_4$ são precisamente os ideais maximais de $\mathbb{Z}$ que contém $4\mathbb{Z}$. O único ideal de $\mathbb{Z}$ com esta propriedade é $\mathfrak{m} = 2\mathbb{Z}$ que por sua vez está em correspondência com ideal $\mathfrak{n} = \{\overline{0}, \overline{2}\}$ de $\mathbb{Z}_4$. Logo $\mathrm{Jac}(\mathbb{Z}_4) = \mathfrak{n}$.

Nem sempre se define o radical de Jacobson de um anel R em termo de seus ideais maximais. Em alguns livros como [9] e [12] o radical de Jacobson de R é definido em termo de elementos quase-regulares (não os definiremos aqui). O ponto importante é que $\mathrm{Jac}(R)$ é um ideal bilateral de R, quer seja definido em termo de ideais à esquerda maximais ou em termo de elementos quase-regulares (entre outras caracterizações).

Definição 2.1.20. *Um anel R tal que* $\mathrm{Jac}(R) = (0)$ *chama-se* **semissimples**.

O exemplo mais trivial de um anel semissimples é um corpo. Pelo que fizemos anteriormente, $\mathbb{Z}_4$ não é semissimples.

Definição 2.1.21. *Um anel R é dito* **simples** *se $R^2 \neq (0)$ e seus únicos ideais são os triviais* (0) *e R.*

Exemplo 2.1.22. *O anel $M_2(F)$ é simples. Mais geralmente, $M_n(F)$ é um anel simples.*

Como $\mathrm{Jac}(R)$ é um ideal de R e não contém 1, se R é um anel simples teremos que $\mathrm{Jac}(R) = (0)$. Em outras palavras, todo anel simples é semissimples.

Definição 2.1.23. *Uma álgebra R é dita* **central** *se $Z(R) = F$.*

Para o caso de um anel simples, o Lema 2.1.18 acima pode ser melhorado. Isto é, pode ser revelado algo interessante a respeito do centróide de R. Vejamos:

Seja R um anel simples. Para começar, $R^2 = R$ e, pelo que acabamos de provar, $C(R)$ é comutativo. Além do mais, simplicidade sendo equivalente à irredutibilidade de R como um $B(R)$-módulo, pelo Lema de Schur $\mathrm{End}_{B(R)}R = C(R)$ deve ser um anel de divisão. Combinando esses dois, temos que o centróide de um anel simples é um corpo. R é de modo natural uma álgebra sobre este corpo (segue da relação $(*)$ no lema anterior), consequentemente todo anel simples é

uma álgebra simples sobre seu centróide.

Seja $Z'(R) \subseteq C(R)$ tal que $Z'(R) \approx Z(R)$. Dado $\sigma \in C(R)$; para qualquer $r \in R$, $\sigma(r1) = \sigma(L_r 1) = L_r(\sigma 1) = r(\sigma 1)$. Seja $a = \sigma 1$, temos mostrado que $\sigma r = ra$. Similarmente, $\sigma r = \sigma(1r) = \sigma(T_r 1) = T_r(\sigma 1) = ar$ daí $ar = ra$. Portanto $a \in Z(R)$ e L_a é o seu correspondente em $Z'(R)$. Já que $\sigma r = ar = ra$ temos que $(\sigma - L_a)r = 0$. Contudo, $C(R)$ é um corpo, $(\sigma - L_a) \in C(R)$ e R é uma álgebra sobre $C(R)$; estes juntos nos dão que $\sigma - L_a = 0$. Logo $\sigma = L_a \in Z'(R)$. Mostramos que $Z'(R) = C(R)$. Em particular, $Z(R)$ é um corpo. Este é o conteúdo do

Teorema 2.1.24. *Se R é um anel simples, então $C(R)$ é um corpo e R é uma álgebra sobre $C(R)$. Além disso, $Z(R) \approx C(R)$.*

Agora estamos em condições de enunciar o teorema de Wedderburn-Artin cuja prova pode ser encontrada nas páginas 33, 34 e 48 do livro [9].

Teorema 2.1.25 (Wedderburn-Artin, Wedderburn)**.** *Seja R um anel. Então*

(1) *R é artiniano simples se, e só se, $R \approx M_n(D)$ para algum anel de divisão D e $n \geqslant 1$.*

(2) *R é artiniano semissimples se, e só se, $R = I_1 \oplus \cdots \oplus I_k$, onde $I_1, \ldots, I_k$ são anéis artinianos simples e são todos ideais minimais de R.*

2.2 O Teorema de Kaplansky

Os próximos resultados fazem uso de propriedades básicas do produto tensorial de álgebras as quais admitimos conhecidas pelo bem da clareza do texto. Mas um tratamento muito bem dado sobre produto tensorial de álgebras (que satisfaz meu gosto pessoal) pode ser encontrado nas páginas 59 à 65 do livro [17].

Lembre-se que, dado um anel de divisão D, um subcorpo maximal de D é um subcorpo de D que não está contido em nenhum outro subcorpo de D. A existência de um subcorpo maximal é garantida pelo Lema de Zorn. Se K é um subcorpo maximal de um anel de divisão D, então $C_D(K) = \{a \in D \mid ak = ka, \text{ para todo } k \in K\}$, o **centralizador de K em D**, deve coincidir com K (uma prova para esta afirmação pode ser encontrada na página 94 do livro [9]). Esta propriedade na verdade é uma caracterização para subcorpos maximais (é um "se, e só se"). Claro que a definição anterior pode ser dada em um âmbito um pouco mais geral, a saber: Seja R uma anel e S um subconjunto não-vazio de R. O centralizador de S em R é o conjunto $C_R(S) = \{r \in R \mid rs = sr, \text{ para todo } s \in S\}$.

Observação 2.2.1. (1) *$C_R(S)$ é um subanel de R;* (2) *$C_R(R) = Z(R)$;* (3) *$C_R(S) \supseteq Z(R)$;* (4) *Se $R = D$ é um anel de divisão, então $C_D(S)$ é um subanel de divisão de D.*

Lema 2.2.2. *Seja D um anel de divisão cujo centro denotaremos por Z e seja K um subcorpo maximal de D (claro que $Z \subseteq K$). Então $D \otimes_Z K$ é um anel denso em* $\mathrm{End}_K D$.

Demonstração. Para cada $d \in D$, denote por $L_d : D \to D$ a multiplicação à esquerda por d e denote $D_l = \{L_d \mid d \in D\}$. Então $L : D \to D_l \subseteq \mathrm{End}_Z(D)$, tal que $L(d) = L_d$, é um

homomorfismo de Z-álgebras. Também, para cada $k \in K$, denote por $T_k : D \to D$ a multiplicação à direita por k e denote $K_r = \{T_k \mid k \in K\}$. Então, já que K é comutativo, a aplicação $T : K \to K_r \subseteq \mathrm{End}_Z(D)$ tal que $T(k) = T_k$, é também um homomorfismo de Z-álgebras. Uma vez que as multiplicações à esquerda e à direita comutam, segue que a aplicação $D \otimes_Z K \to D_l K_r$ definida por $\sum d_i \otimes k_i \mapsto \sum L_{d_i} T_{k_i}$, está bem definida e é um homomorfismo sobrejetor de Z-álgebras. Isto torna D um $D \otimes_Z K$-módulo com respeito à multiplicação $(\sum d_i \otimes k_i)x = \sum L_{d_i} T_{k_i} x$, para $x, d_i \in D,\ k_i \in K$.

- D é um $D \otimes_Z K$-módulo irredutível.
  De fato, já que para todo $x \neq 0$ em D temos que $Dx = D$, segue que $(D \otimes_Z K)x = D$.

- D é um $D \otimes_Z K$-módulo fiel.
  Todo elemento de $D \otimes_Z K$ pode ser escrito da forma $\sum d_i \otimes k_i$ com todos os k_i's linearmente independentes sobre Z, precisamos apenas mostrar que $\sum_{i=1}^{n} d_i D k_i = 0$ para alguns elementos $k_1, \ldots, k_n \in K$ linearmente independentes sobre Z, então $d_1 = \cdots = d_n = 0$. Provamos isso por indução em n. O caso $n = 1$ é claro. Suponha que o resultado seja válido para $n - 1$ e suponha por contradição que nem todos os d_i's são zero. Seja $d_n \neq 0$. Multiplicando $\sum d_i D k_i$ pela esquerda por d_n^{-1}, podemos assumir que $d_n = 1$. Para todos $x, y \in D$, temos

  $$x(\sum_{i=1}^{n} d_i y k_i) = 0 \quad \text{e} \quad \sum_{i=1}^{n} d_i x y k_i = 0.$$

  Subtraindo estas igualdades obtemos

  $$\sum_{i=1}^{n-1} (x d_i - d_i x) y k_i = 0,$$

  para todo $x \in D$. Assim, pela hipótese de indução, $d_i x = x d_i$ para todo i e para todo $x \in D$. Isto diz que $d_1, \ldots, d_n \in Z$. Da igualdade $\sum_{i=1}^{n-1} d_i k_i = \sum_{i=1}^{n} d_i 1 k_i = 0$ obtemos que $k_1, \ldots, k_n$ são linearmente dependentes sobre Z, uma contradição. Isto prova que D é um $D \otimes_Z K$-módulo fiel.

Portanto $D \otimes_Z K$ é um anel primitivo com módulo irredutível D. Pelo Teorema da Densidade, com a finalidade de completar a prova, é suficiente mostrar que o anel comutador $\mathrm{End}_{D \otimes_Z K}(D)$ é isomorfo a K. Para ver isso, seja $\alpha \in \mathrm{End}_{D \otimes_Z K}(D)$. Para todo $x \in D$, temos que $\alpha(x) = x\alpha(1)$, já que α comuta com a multiplicação à esquerda por D. Também, se $x \in K$, então $x\alpha(1) = \alpha(x \cdot 1) = \alpha(1 \cdot x) = \alpha(1)x$, já que α comuta com multiplicação à direita por K. Consequentemente $\alpha(1) \in D$ centraliza K e, já que K é subcorpo maximal de D, obtemos $\alpha(1) \in K$. Portanto α é a multiplicação à direita por $\alpha(1)$, a saber, $\alpha = T_{\alpha(1)} \in K_r$ e pela ação definida de $D \otimes_Z K$ em D, isto diz que $\mathrm{End}_{D \otimes_Z K}(D) \approx K$. □

No caso em que R é uma álgebra simples central de dimensão finita, sabemos que $[R : Z(R)] = n^2$ e dizemos que n é o **grau da álgebra** R (ver o Teorema 4.2.2 do livro [9]).

Teorema 2.2.3 (Kaplansky)**.** *Seja R uma álgebra primitiva satisfazendo uma identidade polinomial de grau d. Então R é uma álgebra simples central de dimensão finita e $[R : Z(R)] \leqslant [d/2]^2$.*

Demonstração. Seja f uma identidade polinomial de grau d satisfeita por R e assuma que f é multilinear. Sendo R primitiva, possui um R-módulo fiel e irredutível V com anel comutador D. Aplicando a Proposição 2.1.12 temos que $R \approx M_n(D)$, onde $n = [V : D]$. Escreva $Z = Z(R)$.

Já que $M_n(D)$ satisfaz f e D é um subanel, D também satisfaz f. Além do mais, se K é um subcorpo maximal de D, levando em consideração que f é multilinear e K é comutativo, obtemos que $D \otimes_Z K$ ainda satisfaz f. Como, pelo lema anterior, $D \otimes_Z K$ tem um módulo fiel e irredutível com anel comutador K, pela primeira parte desta demonstração obtemos que $D \otimes_Z K \approx M_m(K)$, para algum $m \geqslant 1$. O resultado disso é que

$$R \subseteq R \otimes_Z K \approx M_n(D) \otimes_Z K \approx M_n(D \otimes_Z K) \approx M_n(M_m(K)) \approx M_{nm}(K).$$

Como f é multilinear, $R \otimes_Z K \approx M_{nm}(K)$ ainda satisfaz f. Lembre que $M_{nm}(K)$ não satisfaz identidades de grau menor que $2nm$ (Amitsur-Levitzki), daí obtemos que $nm \leqslant d/2$. Agora, $[R : Z] = [R \otimes_Z K : K] = (nm)^2 \leqslant [d/2]^2$ e a demonstração está completa. □

Se R é uma álgebra, por extensão dos escalares, obtemos uma nova álgebra sobre F cujas identidades são satisfeitas por R.

Seja A uma álgebra comutativa e considere a F-álgebra $R \otimes_F A$. Algumas identidades polinomiais de R podem ainda se anularem em $R \otimes_F A$. Daremos um nome especial.

Definição 2.2.4. *Seja f uma identidade para a álgebra R. Dizemos que f é uma* **identidade estável** *para R se para qualquer álgebra comutativa A, f é ainda uma identidade para $R \otimes_F A$.*

Agora enunciaremos um resultado que é usado como ponte na demonstração no Lema 2.2.6 e cuja demonstração pode ser encontrada na página 10 do livro [8].

Lema 2.2.5. *Se F é um corpo infinito e R é uma F-álgebra, então toda identidade polinomial de R é estável.*

Lembre que um ideal à esquerda (à direita, bilateral) I de um anel R é **nilpotente** se existe $n \in \mathbb{Z}^+$ tal que $a_1 \cdots a_n = 0$ para quaisquer $a_1, \ldots, a_n \in I$ (de outra forma, I é nilpotente se existe $n \in \mathbb{Z}^+$ tal que $I^n = (0)$). Semelhantemente, um elemento $a \in R$ é **nilpotente** se existe $n \in \mathbb{Z}^+$ tal que $a^n = 0$; um ideal I é dito ser um **nil ideal** se todos os seus elementos são nilpotentes.

O próximo passo é relacionar as identidades de uma álgebra simples de dimensão finita às identidades de matrizes. Fazemos isso no lema seguinte.

Lema 2.2.6. *Seja R uma álgebra simples central de dimensão n^2 sobre seu centro F. Então $R \leqslant M_n(F)$ e $M_n(F) \leqslant R$ (ou em outra notação: $Id(R) = Id(M_n(F))$). Além do mais, f é um polinômio central de $M_n(F)$ se, e só se, f é um polinômio central de R.*

Demonstração. A álgebra R tem dimensão n^2 sobre seu centro que é o corpo F. Segue da Observação 2.1.11 que R é artiniano como álgebra. Pelo Teorema 2.1.25 (Wedderburn-Artin), $R \approx M_t(D)$, para alguma álgebra de divisão D, central e de dimensão finita sobre F (Lembre que podemos identificar $Z(D)$ com $Z(M_t(D)) \approx Z(R) = F$. Veja isso na Seção 1.9. Por isso D é central). Se F é finito, D é uma álgebra de divisão finita e, pelo teorema de Wedderburn (*Todo anel de divisão finito é um corpo* - confira o Teorema 3.1.1 do livro [9]), D é um corpo. Consequentemente $D = F$,

visto que D é central sobre F. Segue que $R \approx M_t(F)$ e o lema está provado para este caso.

Suponha que F é infinito e seja K um subcorpo maximal de D. Pelo Lema 2.2.2, $D \otimes_F K \approx M_m(K)$ para algum m. Consequentemente $R \otimes_F K \approx M_{tm}(K)$. Como feito acima, comparando as dimensões, vemos que $R \otimes_F K \approx M_n(K)$. Já que F é infinito, pelo Lema 2.2.5 toda identidade polinomial de R é estável. Consequentemente R e $M_n(F)$ têm as mesmas identidades e os mesmos polinômios centrais. □

Um anel é **semiprimo** se não contém ideais nilpotentes não-nulos. Note que se I é um ideal à direita, nilpotente e não-nulo de um anel simiprimo R, então RI é um ideal nilpotente não-nulo de R, mas isso não é permitido. Portanto um anel semiprimo não possui ideais à direita ou à esquerda nilpotentes não-nulos.

Teorema 2.2.7. *Se R é uma PI-álgebra semiprima, então R não tem nil ideais não-nulos.*

Demonstração. Seja f um polinômio multilinear satisfeito por R e suponha que R possui um nil ideal não-nulo N. Já que $f(N) = 0$, então também $f(N)N = (0)$. Seja $g \in F\langle X\rangle$ um polinômio multilinear de grau mínimo com a propriedade que $g(I)I = (0)$, para algum ideal à direita não-nulo $I \subseteq N$. Acharemos uma contradição provando que $I^2 = (0)$, uma vez que isso não é possível em uma álgebra semiprima.

Suponha que existe $a \in I$ tal que $a^2I = (0)$. Podemos assumir que o monômio $X_1 \cdots X_n$ aparece em g com coeficiênte não-nulo e escreva g na forma

$$g(X_1, \ldots, X_n) = h(X_1, \ldots, X_{n-1})X_n + h'(X_1, \ldots, X_n)$$

onde X_n nunca aparece como a última variável em todo monômio de h'. Já que $a^2I = (0)$ vemos que, para quaisquer $r_1, \ldots, r_n \in I$,

$$g(ar_1, \ldots, ar_{n-1}, a) = h(ar_1, \ldots, ar_{n-1})a.$$

Lembre que $aI \subseteq I$ e $g(I)I = (0)$, obtemos que

$$h(ar_1, \ldots, ar_{n-1})aI = g(ar_1, \ldots, ar_{n-1}, a)I \subseteq g(I)I = (0),$$

para todos $r_1, \ldots, r_n \in I$. Assim, $h(aI)aI = (0)$. Mas então, h é um polinômio multilinear não-nulo com grau menor que o de g e é tal que $h(aI)aI = (0)$ onde aI é um ideal de R à direita contido em N. Pela minimalidade do grau de g, aI é nulo. O que provamos foi que se $a \in I$ é tal que $a^2I = (0)$, então $aI = (0)$. Mas se b é qualquer elemento de I, b é nilpotente, digamos que $b^k = 0$; consequentemente $b^kI = (0)$. Já que $(b^{k-1})^2 = 0$, pelo que já fizemos acima, $b^{k-1}I = (0)$ e, por indução, obtemos finalmente que $bI = (0)$. Isto diz que $I^2 = (0)$ e, sendo R semiprimo, concluimos que $I = (0)$. □

Teorema 2.2.8. *Se R não possui nil ideais não-nulos, então a álgebra dos polinômios $R[X]$ é semissimples.*

Demonstração. Sejam $J = \mathrm{Jac}(R[X])$ e I o ideal de R consistindo dos coeficientes líderes dos polinômios de J. Provaremos que I é um nil ideal e já que por hipótese R não possui nil ideais não-nulos, isto implicará que $I = (0)$ e portanto, $J = 0$

Seja $f = f(X) = \sum_{i=0}^{n} a_i X^i \in J$ não-nulo. Como $Xf \in J$, o elemento $1 - Xf$ é invertível em $R[X]$ e seja $g \in R[X]$ tal que $(1 - Xf)g = 1$. Afirmamos que, para todo $m \geqslant 1$,

$$g = X^m f^m g + \sum_{i=0}^{m-1} X^i f^i. \tag{2.2.1}$$

Provaremos por indução em m. Já que $(1 - Xf)g = 1$, então $g = Xfg + 1$ e o caso $m = 1$ está provado. Suponha que a fórmula acima valha para $m - 1$. Então temos

$$g = X^{m-1} f^{m-1} g + \sum_{i=0}^{m-2} X^i f^i = X^{m-1} f^{m-1}(Xfg + 1) + \sum_{i=0}^{m-2} X^i f^i = X^m f^m g + \sum_{i=0}^{m-1} X^i f^i$$

e a afirmação está provada.

Escreva $g = \sum_{i=0}^{r} b^i X^i$ e tome $m > r$. Lembre que $f = \sum_{i=0}^{n} a_i X^i \in J$ e igualando em (2.2.1) o coeficiente de $X^{m+nm+i}, 1 \leqslant i \leqslant r$, obtemos $0 = a_n^m b_i$. Segue que $a_n^m g = 0$ e , já que g é invertível em $R[X]$, obtemos $a_n^m = 0$ e o coeficiente líder de f é nilpotente. Portanto I é um nil ideal e a demonstração do teorema está completa. □

Lembre que, dada uma coleção de álgebras $\{R_\gamma \mid \gamma \in \Gamma\}$, dizemos que uma álgebra R é um **produto subdireto** das álgebras $R_\gamma, \gamma \in \Gamma$, se R pode ser mergulhada (i.e., existe um homomorfismo injetivo) na álgebra $\prod_{\gamma\in\Gamma} R_\gamma$ de modo que $\pi_\gamma(R) = R_\gamma$ para todo $\gamma \in \Gamma$ onde $\pi_\gamma : R \to R_\gamma$ é a γ-ésima projeção sobre R_γ. Na verdade, se $\{I_\gamma \mid \gamma \in \Gamma\}$ é uma coleção de ideais de R, então R é um produto subdireto das álgebras $R/I_\gamma, \gamma \in \Gamma$, se e só se, $\bigcap_{\gamma\in\Gamma} I_\gamma = (0)$. Por exemplo, o radical de Jacobson da uma álgebra R é a interseção dos ideais primitivos de R (lembre que $I \lhd_l R$ é **primitivo** se $I = \mathrm{Ann}_R(M)$ para algum R-módulo irredutível M), segue que uma álgebra semissimples é um produto subdireto de álgebras primitivas.

O próximo resultado é devido a Rowen e é uma importante aplicação da existência de polinômios centrais para a álgebras das matrizes.

Teorema 2.2.9 (Rowen)**.** *Seja R uma PI-álgebra semiprima. Se I é um ideal não-nulo de R, então $I \cap Z(R) \neq (0)$.*

Demonstração. Seja f uma identidade de R de grau d. Suponha primeiro que R é semissimples. Então R é um produto subdireto de álgebras primitivas $R_\gamma, \gamma \in \Gamma$. Cada R_γ ainda satisfaz f consequentemente, pelo Teorema 2.2.3 (Kaplansky), é uma álgebra simples de dimensão $n_\gamma^2 \leqslant [d/2]^2$ sobre seu centro. Seja I_γ a imagem de I pela projeção canônica $R \to R_\gamma$. Já que R_γ é simples, então, das duas uma, ou $I_\gamma = R_\gamma$ ou $I_\gamma = (0)$. Considere o conjunto $\Gamma' = \{\gamma \in \Gamma \mid I_\gamma = R_\gamma\}$. Como I_γ é um ideal não-nulo de R_γ, temos que $\Gamma' \neq \varnothing$ e seja n_0^2 a maior dimensão de uma álgebra simples central R_γ com $\gamma \in \Gamma'$. Seja h_{n_0} um polinômio central para as matrizes $n_0 \times n_0$. Pelo Lema 2.2.6 para cada álgebra R_γ com $[R_\gamma : Z(R_\gamma)] = n_0^2$,

$$0 \neq h_{n_0}(I_\gamma) = h_{n_0}(R_\gamma) \subseteq Z(R_\gamma).$$

Para qualquer outra álgebra R_γ de dimensão menor sobre seu centro, pelo Lemas 1.9.16 e 2.2.6, devemos ter que $h_{n_0}(I_\gamma) = 0$. O resultado disso é que $0 \neq h_{n_0}(I) \subseteq I \cap Z(R)$ e o teorema está provado para o caso em que R é uma álgebra semissimples.

Agora seja R qualquer álgebra semiprima. Pelo Teorema 2.2.7, R não possui nil ideais não-nulos e, portanto, pelo Teorema 2.2.8, o anel dos polinômios $R[X]$ é semissimples. Já que $I[X]$ é um ideal não-nulo de $R[X]$, pela primeira parte desta demonstração temos que $(0) \neq I[X] \cap Z(R[X]) = I[X] \cap Z(R)[X] = (I \cap Z(R))[X]$. Portanto $I \cap Z(R) \neq (0)$. □

Uma consequência imediata deste teorema é o corolário abaixo.

Corolário 2.2.10. *Se R é uma PI-álgebra semiprima e $Z(R)$ é um corpo, então R é uma álgebra simples central de dimensão finita.*

Demonstração. Se I é um ideal não-nulo de R, pelo teorema anterior $I \cap Z(R) \neq (0)$. Como $Z(R)$ é um corpo, I contém um elemento invertível e, portanto, $I = R$. Isto mostra que R é simples. Agora aplicamos o Teorema de Kaplansky. □

2.3 Localização Central

O processo pelo qual se constrói o anel $\mathbb{Q}$ a partir de $\mathbb{Z}$ (e depois mergulha $\mathbb{Z}$ em $\mathbb{Q}$) se estende facilmente em um contexto um pouco mais geral. O procedimento é chamado **localização central** e é definido como segue.

Seja R uma F-álgebra, novamente denote o centro de R por Z e seja $S \subseteq Z - \{0\}$ um monóide (multiplicativo). A menos que seja feita referência contrária, quando usarmos a letra S nesta seção fica implícito que S é um monóide multiplicativo contido em $Z - \{0\}$.

No produto cartesiano $R \times S = \{(r, s) \mid r \in R, s \in S\}$ defina a relação $\sim$ dada por $(r_1, s_1) \sim (r_2, s_2)$ se, e só se, $(r_1 s_2 - r_2 s_1)s = 0$ para algum $s \in S$; não é difícil verificar que $\sim$ é uma *relação de equivalência* em $R \times S$. Denotamos por rs^{-1} a classe de equivalência do elemento (r, s) e o conjunto de todas as classes de equivalência é denotado por R_S. É possível definir operações em R_S e torná-lo uma álgebra sobre F. Fazemos assim: para todos $\alpha \in F$, $r_i \in R$ e $s_i \in S$,

$$r_1 s_1^{-1} + r_2 s_2^{-1} := (r_1 s_2 + r_2 s_1)(s_1 s_2)^{-1}, \qquad (r_1 s_1^{-1})(r_2 s_2^{-1}) := (r_1 r_2)(s_1 s_2)^{-1}$$

$$\alpha(r_1 s_1^{-1}) := (\alpha r_1) s_1^{-1}.$$

As operações acima estão bem definidas e a verificação não é mais difícil que a da construção usual de $\mathbb{Q}$ a partir de $\mathbb{Z}$. Note que a unidade multiplicativa de R_S é $1 \cdot 1^{-1}$, e o elemento "zero" é $0 \cdot 1^{-1}$.

Observação 2.3.1. *Existe um homomorfismo canônico $\omega_S : R \to R_S$ dado por $r \mapsto r1^{-1}$ e $ker(\omega_S) = \{r \in R \mid rs = 0$ para algum $s \in S\}$. Para todo $s \in S$, $s1^{-1}$ tem um inverso $1s^{-1}$.*

Proposição 2.3.2. *Dada uma álgebra R' e um homomorfismo $\omega : R \to R'$ tal que $\omega(s)$ é invertível em R' para todo $s \in S$, temos um único homomorfismo $\psi_\omega : R_S \to R'$ tal que $\psi_\omega(r1^{-1}) = \omega(r)$ para todo $r \in R$. Então $ker(\psi_\omega) = \{rs^{-1} \mid r \in ker(\omega)\}$.*

Demonstração. Qualquer homomorfismo satisfaz $\psi_\omega(rs^{-1})\psi_\omega(s1^{-1}) = \psi_\omega(r1^{-1}) = \omega(r)$, implicando que $\psi_\omega(rs^{-1}) = \omega(r)\omega(s)^{-1}$ e esta aplicação é de fato um homomorfismo. Além do mais, $ker(\psi_\omega) = \{rs^{-1} \mid \omega(r) = 0\}$. □

Dizemos que um elemento $z \in Z$ é **regular** se $\mathrm{Ann}_R z = (0)$; S é regular se todo elemento de S é regular. Se S é regular, então $ker(\omega_S) = (0)$, e portanto podemos considerar a inclusão $R \subseteq R_S$.

Olhemos um pouco para $Z(R_S)$. Para fazer isso, adotemos a convenção que, para qualquer subconjunto $A \subseteq R$, A_S denota $\{as^{-1} \mid a \in A, s \in S\}$.

Proposição 2.3.3. *$Z_S \subseteq Z(R_S)$ e temos que a igualdade se S é regular.*

Demonstração. Suponha que $z_1 s_1^{-1} \in Z_S$ para $z_1 \in Z, s_1 \in S$. Para todo $rs^{-1} \in R_S$, temos $(z_1 s_1^{-1})(rs^{-1}) = (z_1 r)(s_1 s)^{-1} = (rz_1)(ss_1)^{-1} = (rs^{-1})(z_1 s_1^{-1})$, provando que $z_1 s^{-1} \in Z(R_S)$.

Agora suponha que S é regular e tome $r_1 s_1^{-1} \in Z(R_S)$. Para todo r em R, $0 = [r1^{-1}, r_1 s_1^{-1}] = [r, r_1]s_1^{-1}$, assim $[r, r_1] = 0$ e isto prova que $r_1 \in Z$; portanto $r_1 s_1^{-1} \in Z_S$. □

Proposição 2.3.4. *Se R é primo (resp. semiprimo) com S regular, então R_S é primo (resp. semiprimo).*

Demonstração. Se $r_1 s_1^{-1} R_S r_2 s_2^{-1} = (0)$, então $r_1 R r_2 = (0)$ e assim $r_1 = 0$ ou $r_2 = 0$. (A demonstração para semiprimo é análoga, basta tomar $r_1 = r_2$ e $s_1 = s_2$.) □

Se $r_1 s_1^{-1}, \ldots, r_k s_k^{-1}$ são elementos de R_S então tomando $s = s_1 \cdots s_k$ e $x_j = r_j s_1 \cdots s_{j-1} s_{j+1} \cdots s_k$, $1 \leqslant j \leqslant k$, temos $r_j s_j^{-1} = x_j s^{-1}, 1 \leqslant j \leqslant k$. *Assim podemos sempre assumir que um dado número finito de elementos de R_S têm o mesmo denominador.* Usaremos esta observação sem fazer menção.

Definição 2.3.5. *Para $S = \{$elementos regulares de $Z\}$, R_S é chamada a* **álgebra de quocientes centrais de** *R, e escrevemos $Q_Z(R)$. Quando estiver claro abusaremos da notação e escreveremos apenas $Q(R)$.*

Suponha que S é dado. Escreva $R1^{-1}$ para denotar o conjunto $\{r1^{-1} \mid r \in R\} = \omega_S(R)$, uma imagem homomorfa de R.

Lema 2.3.6. *Se f é um polinômio multilinear, então $f(R_S) = f(R)_S$.*

Demonstração. Segue da Observação 1.5.3. □

Proposição 2.3.7. *Toda identidade multilinear de R é também uma identidade de R_S. Se S é regular, então toda identidade multilinear de R_S é uma identidade de R.*

Demonstração. As identidades de R são identidades de $R1^{-1}$. E as identidades multilineares de $R1^{-1}$ são identidades de R_S. E o resultado segue. Agora, se S é regular então $R \subseteq R_S$, assim $R \leqslant R_S$. □

Finalizamos este tratamento básico a respeito de localização de álgebras provando um resultado bastante útil.

Proposição 2.3.8. $R_S \approx R \otimes_Z Z_S$.

Demonstração. Defina $\psi : R \times Z_S \to R_S$ por $\psi(r, zs^{-1}) = rs^{-1}$ para $r \in R, z \in Z, s \in S$. Então ψ induz um homorfismo sobrejetor $\widehat{\psi} : R \otimes Z_S \to R_S$. Mas qualquer elemento de $R \otimes Z_S$ tem a forma $r \otimes 1s^{-1}$ para $r \in R$ adequado e $s \in S$. Se $r \otimes 1s^{-1} \in ker(\psi)$, então $rs^{-1} = 0$ implicando que $s_1 r = 0$ para algum $s_1 \in S$; portanto $0 = rs_1 \otimes (s_1 s)^{-1} = r \otimes s^{-1}$, provando que ψ é um isomorfismo. □

Como já observamos antes, quando R é um anel primo o seu centro Z é um domínio de integridade e portanto possui um corpo de frações K (na proposição anterior $K = Z_S$). Em outras palavras, quando R é primo, $R \otimes_Z K$. Usualmente escreve-se $a \otimes z^{-1}$ como az^{-1}. Note que quando R é uma PI-álgebra prima o item 2 da Observação 2.1.14 implica que R é uma PI-álgebra semiprima. Logo, pelo Teorema 2.2.9, $Z(R) \neq (0)$.

Teorema 2.3.9 (Posner)**.** *Seja R uma álgebra prima satisfazendo uma identidade polinomial de grau d. Então a localização central R_Z de R é uma álgebra simples central de dimensão $n^2 \leqslant [d/2]^2$ sobre seu centro K. Além disso, R e $M_n(K)$ satisfazem as mesmas identidades polinomiais.*

Demonstração. Suponha primeiro que Z é infinito. Pelo que foi observado acima, a localização central R_Z é ainda uma álgebra prima já que todo elemento $z \in Z - \{0\}$ é regular. Além do mais, $R_Z \approx R \otimes_Z K$, onde K é o corpo de frações de Z, satisfaz as mesmas identidades que R, sendo Z infinito. Pode-se verificar rapidamente que na verdade K é o centro de R_Z e, sendo um corpo, pelo Corolário 2.2.10, R_Z é uma álgebra simples central de dimensão finita. No caso em que Z é finito, então $Z = K$ e aplica-se o Corolário 2.2.10. Já que, pelo Lema 2.2.6, R_Z e $M_n(K)$ satisfazem as mesmas identidades polinomiais, temos que R e $M_n(K)$ satisfazem as mesmas identidades polinomiais. Pelo Teorema 2.2.3 (Kaplansky) temos também $n^2 \leqslant [d/2]^2$. □

A formulação do Teorema de Posner dada acima é uma combinação da formulação original e as consequências acima da existência de polinômios centrais para matrizes.

Capítulo 3

Álgebras Graduadas e o Teorema de Posner

Veremos que todo anel pode ser graduado, sendo assim a grosso modo o que vamos fazer é generalizar as ideias do capítulo anterior. Normalmente, quando se trabalha de um ponto de vista mais geral, nem todas as propriedades boas da estrutura com a qual se está trabalhando são preservadas e o Capítulo 2 foi escrito com o intuito de fazer comparativos com este. Seguiremos o roteiro dos livros [14] e [15] e buscamos apresentar demonstrações para os principais teoremas de estrutura agora para anéis (álgebras) graduados. Como de costume, faremos algumas convenções e começamos dizendo que para nós $(G, *)$ denota um grupo com elemento neutro "e". As demais convenções serão feitas no corpo do texto.

3.1 Definições e Propriedades Básicas

Um grupo abeliano $(H, +)$ é dito **graduado do tipo** G (ou G-graduado) se existe uma família $\{H_g\}_{g\in G}$ de subgrupos de H tal que

$$H = \bigoplus_{g\in G} H_g.$$

Exemplo 3.1.1. *Com a soma usual de matrizes o conjunto $H = M_2(\mathbb{Q})$ é um grupo abeliano. Este grupo é $\mathbb{Z}_4$-graduado, onde $H_{\overline{0}} = \mathbb{Q}e_{11}$, $H_{\overline{1}} = \mathbb{Q}e_{12}$, $H_{\overline{2}} = \mathbb{Q}e_{21}$ e $H_{\overline{3}} = \mathbb{Q}e_{22}$ e os e_{ij}'s são as matrizes unidade.*

A notação utilizada acima representa a *soma direta interna* de uma família de subgrupos de H. Para maiores detalhes acerca de soma direta interna, externa, etc, consulte a página 21 do livro [16].

Todo anel é um grupo abeliano com a soma, sendo assim a definição de anel graduado deve conter a definição de grupo abeliano graduado e uma certa compatibilidade com a estrutura de anel. Vamos à definição formal.

Definição 3.1.2. *Um anel R é dito* **G-graduado** *(ou graduado do tipo G) se*

$$R = \bigoplus_{g \in G} R_g,$$

onde $\{R_g \mid g \in G\}$ é uma família de subgrupos aditivos de R e $R_g R_h \subseteq R_{g*h}$ para todos $g, h \in G$.

Entendemos por $R_g R_h$ o conjunto de todas as somas finitas de elementos da forma $r_g r'_h$ com $r_g \in R_g$ e $r'_h \in R_h$.

Para um anel G-graduado R é comum tomar G como sendo um grupo multiplicativo. Daí a relação $R_g R_h \subseteq R_{g*h}$, $g, h \in G$, passa a ser escrita $R_g R_h \subseteq R_{gh}$. Quando trabalha-se com grupo aditivo, esta última relação é escrita $R_g R_h \subseteq R_{g+h}$.

Os elementos do conjunto $h(R) := \bigcup_{g \in G} R_g$ são chamados elementos **homogêneos** do anel R, um elemento não-nulo $r \in R_g$ é chamado **homogêneo de grau** g e escreve-se $\deg r = g$ para denotar isso.

Qualquer elemento não-nulo $r \in R$ é escrito de modo único como uma soma de elementos homogêneos,

$$r = \sum_{g \in G} r_g$$

onde $r_g \in R_g$ é não-nulo apenas para uma quantidade finita de índices $g \in G$. Os elementos não-nulos r_g nesta decomposição são as **componentes homogêneas** de r.

Proposição 3.1.3. *Para um anel G-graduado $R = \bigoplus_{g \in G} R_g$ as seguinte afirmações são verdadeiras:*

(1) $1 \in R_e$*;*

(2) *se $r \in R_g$ e existe r^{-1}, então $r^{-1} \in R_{g^{-1}}$.*

Demonstração. (1) Sabemos que R_e é um subanel de R. Seja $1 = \sum_{g \in G} r_g$ a decomposição homogênea de $1 \in R$. Tome $h \in G$ e $t_h \in R_h$, então $t_h = 1t_h = \sum_{g \in G} r_g t_h$ e $r_g t_h \in R_{gh}$. Consequentemente, como t_h se escreve de modo único em R, $r_g t_h = 0$ vale para todo $g \neq e$ em G. Segue que $r_g t = 0$ para todo $g \neq e$ em G e para todo $t \in R$. Tomando $t = 1$, $r_g = r_g 1 = 0$ para todo $g \neq e$.

Qualquer que seja $t_h \in R_h$, $t_h = 1t_h = (\sum_{g \in G} r_g)t_h = r_e t_h$. De maneira análoga se prova que $t_h r_e = t_h$ para todo $t_h \in R_h$. Portanto, $r_e = 1$.

(2) Assuma que $r \in R_h$ e é invertível em R. Se $r^{-1} = \sum_{g \in G} s_g$ com $s_g \in R_g$, então $1 = rr^{-1} = r(\sum_{g \in G} s_g)$. Uma vez que $1 \in R_e$ e $rs_g \in R_{hg}$, temos que $rs_g = 0$ para qualquer $g \neq h^{-1}$. Como r é invertível obtemos que $s_g = 0$ para $g \neq h^{-1}$, portanto $r^{-1} = s_{h^{-1}} \in R_{h^{-1}}$. □

Claramente, R_e é um subanel de R e R_g é um R_e-R_e-bimódulo para todo $g \in G$. De fato, como $R_e R_e \subseteq R_{ee} = R_e$, o grupo aditivo R_e é também fechado para o produto de seus elementos. E para todo $g \in G$, $R_g R_e \subseteq R_{ge} = R_g$ e $R_e R_g \subseteq R_g$ daí o grupo aditivo R_g é um R_e-R_e-bimódulo. Vale lembrar que se A e B são anéis, afirmar que M é um *A-B-bimódulo* significa que M é um A-módulo à esquerda, é um B-módulo à direita e vale que $a(mb) = (am)b$ para qualquer $a \in A$, $m \in M$ e $b \in B$. Como exemplo temos que qualquer R-módulo à esquerda é um R-$\mathbb{Z}$-bimódulo.

Definição 3.1.4. *Seja $R = \bigoplus_{g\in G} R_g$ um anel G-graduado. Um subanel S de R é dito* **graduado** *do tipo G se $S = \bigoplus_{g\in G}(R_g \cap S)$. Equivalentemente, S é graduado se para todo elemento $s \in S$ as suas componentes homogêneas (como elementos de R) estão em S.*

A partir de agora tomaremos graduação por grupos multiplicativos e quando considerarmos grupos com outra operação isto ficará claro.

Exemplos de Anéis Graduados

(1) Todo anel R pode ser considerado como um anel graduado do tipo G, para qualquer grupo G, pondo $R_e = R$ e $R_g = (0)$ para todo $g \neq e$ em G. Tal graduação é chamada **trivial** e o anel R é dito G-graduado trivialmente.

(2) Seja G um grupo e R um anel. O anel de grupo $A = R[G]$ é graduado do tipo G onde $A_g = R \cdot g$ para todo $g \in G$.

(3) Seja R um anel comutativo. O anel $R[x]$ dos polinômios em uma variável x comutativa sobre R é um anel $\mathbb{Z}$-graduado, com $R_k = Rx^k$ quando $k \geqslant 0$ e $R_k = (0)$ quando $k < 0$.
$R_kR_n \subseteq R_{k+n}$ e $R[x] = \bigoplus_{k\in\mathbb{Z}} R_k$.

(4) O corpo $\mathbb{C}$ dos números complexos é um anel $\mathbb{Z}_2$-graduado. Onde $\mathbb{C}_{\overline{0}} = \mathbb{R}$ e $\mathbb{C}_{\overline{1}} = i\mathbb{R}$, além disso $\mathbb{C}_{\overline{0}}\mathbb{C}_{\overline{1}} \subseteq \mathbb{C}_{\overline{0}+\overline{1}} = \mathbb{C}_{\overline{1}}$ e $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$.

(5) O anel $R = M_n(A)$ das matrizes sobre um anel A com unidade, é $\mathbb{Z}$-graduado.

$$R_k = \begin{cases} \displaystyle\sum_{i=1}^{n-k} e_{i,i+k}A & \text{se} \quad 0 \leqslant k < n \qquad \text{(I)} \\ \displaystyle\sum_{i=1-k}^{n} e_{i,i+k}A & \text{se} \quad -n < k < 0 \quad \text{(II)} \\ (0) & \text{se} \quad |k| \geqslant n \qquad \text{(III)} \end{cases}$$

Observe que quando $n = 1$, o conjunto $R = M_n(A)$ é o próprio A e a graduação é a trivial. De fato, para $n = 1$, temos apenas duas possibilidades. Primeiro: $k = 0$, neste caso R_k se enquadra em (I). Segundo: $k \neq 0$, daí R_k se encaixa no caso (III). Este exemplo torna-se mais interessante quando $n > 1$. Faremos para o caso $n = 3$ e depois mostraremos como ficam os R_k's no caso geral.

Suponha $n = 3$. Para k em $\{0, 1, 2\}$, i.e., $0 \leqslant k < 3$, o conjunto R_k está no caso (I). Mais especificamente, temos

$$R_0 = \sum_{i=1}^{3-0} e_{i,i+0}A = \sum_{i=1}^{3} e_{i,i}A = e_{11}A + e_{22}A + e_{33}A = \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \end{pmatrix},$$

$$R_1 = \sum_{i=1}^{3-1} e_{i,i+1}A = \sum_{i=1}^{2} e_{i,i+1}A = e_{12}A + e_{23}A = \begin{pmatrix} 0 & A & 0 \\ 0 & 0 & A \\ 0 & 0 & 0 \end{pmatrix}$$

e

$$R_2 = \sum_{i=1}^{3-2} e_{i,i+2}A = \sum_{i=1}^{1} e_{i,i+2}A = e_{13}A = \begin{pmatrix} 0 & 0 & A \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Para k em $\{-1,-2\}$, i.e., $-3 < k < 0$, o conjunto R_k está no caso (II). Mais especificamente, temos

$$R_{-1} = \sum_{i=1-(-1)}^{3} e_{i,i+(-1)}A = \sum_{i=2}^{3} e_{i,i-1}A = e_{21}A + e_{32}A = \begin{pmatrix} 0 & 0 & 0 \\ A & 0 & 0 \\ 0 & A & 0 \end{pmatrix}$$

e

$$R_{-2} = \sum_{i=1-(-2)}^{3} e_{i,i+(-2)}A = \sum_{i=3}^{3} e_{i,i-2}A = e_{31}A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ A & 0 & 0 \end{pmatrix}$$

Para $k \in \mathbb{Z}$ tal que $|k| \geqslant 3$, o conjunto R_k está no caso (III).

Podemos agora afirmar que, para $n \in \{1,2,3,\cdots\}$, os grupos aditivos R_k assumem as formas

$$\cdots \quad , \quad R_{-1} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ A & 0 & 0 & \dots & 0 & 0 \\ 0 & A & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & A & 0 \end{pmatrix}, \qquad R_0 = \begin{pmatrix} A & 0 & 0 & \dots & 0 & 0 \\ 0 & A & 0 & \dots & 0 & 0 \\ 0 & 0 & A & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & A & 0 \\ 0 & 0 & 0 & \dots & 0 & A \end{pmatrix},$$

$$R_1 = \begin{pmatrix} 0 & A & 0 & \dots & 0 & 0 \\ 0 & 0 & A & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & A \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}, \quad \cdots$$

(6) Seja $R = \bigoplus_{g \in G} R_g$ um anel G-graduado e fixe $\overline{g} = (g_1, \dots, g_n) \in G^{(n)}$. Para cada $h \in G$ associamos o seguinte subgrupo aditivo de $M_n(R)$:

$$M_n(R)_h(\overline{g}) = \begin{pmatrix} R_{g_1hg_1^{-1}} & R_{g_1hg_2^{-1}} & \dots & R_{g_1hg_n^{-1}} \\ R_{g_2hg_1^{-1}} & R_{g_2hg_2^{-1}} & \dots & R_{g_2hg_n^{-1}} \\ \vdots & \vdots & \ddots & \vdots \\ R_{g_nhg_1^{-1}} & R_{g_nhg_2^{-1}} & \dots & R_{g_nhg_n^{-1}} \end{pmatrix}.$$

Verifica-se rapidamente que o anel $M_n(R)$ equipado com a graduação do tipo G dada por $\bigoplus_{h\in G} M_n(R)_h(\overline{g})$ é um anel graduado, o qual denotamos por $M_n(R)(\overline{g})$, que contém R como subanel graduado. Uma matriz unidade e_{ij} tem grau $g_i^{-1}g_j$, pois, para $h = g_i^{-1}g_j$, as entradas ij das matrizes de $M_n(R)_{g_i^{-1}g_j}(\overline{g})$ são tomadas em $R_{g_ihg_j^{-1}} = R_{g_ig_i^{-1}g_jg_j^{-1}} = R_e$ e $1 \in R_e$. Se $\overline{g} = (e, \dots, e)$, então escrevemos $M_n(R)$ para denotar o anel $M_n(R)(\overline{g})$ quando não houver ambiguidade se $M_n(R)$ é graduado ou não.

Podemos graduar um mesmo anel de maneiras diferentes. Um ponto interessante é que, dependendo da graduação dada a um certo anel R, seus elementos podem ficar mais manejáveis. Para tornar esta afirmação mais clara, considere o anel $\mathbb{R}[x]$ com a $\mathbb{Z}$-graduação dada no exemplo **(3)** e considere-o também com a $\mathbb{Z}_2$-graduação dada por $\mathbb{R}[x] = A_{\overline{0}} \oplus A_{\overline{1}}$, onde

$$A_{\overline{0}} = \mathbb{R} + \mathbb{R}x^2 + \mathbb{R}x^4 + \cdots \quad \text{e} \quad A_{\overline{1}} = \mathbb{R}x + \mathbb{R}x^3 + \mathbb{R}x^5 + \cdots.$$

Se tomamos $\mathbb{R}[x]$ como um anel $\mathbb{Z}$-graduado, o elemento $1 + x^2$ não é homogêneo. Por outro lado, considerando $\mathbb{R}[x]$ com a $\mathbb{Z}_2$-graduação dada acima, $1 + x^2$ é homogêneo de grau $\overline{0}$.

Definição 3.1.5. *Um ideal I de um anel G-graduado R é um* **ideal graduado** *do tipo G se $I = \bigoplus_{g\in G}(I \cap R_g)$.*

Exemplo 3.1.6. *Seja F um corpo e $R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \;\middle|\; a, b \in F \right\} = R_{\overline{0}} \oplus R_{\overline{1}}$ um anel $\mathbb{Z}_2$-graduado, onde*

$$R_{\overline{0}} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in F \right\}, \quad R_{\overline{1}} = \left\{ \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} \;\middle|\; b \in F \right\}.$$

Facilmente se verifica que $I = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \;\middle|\; x \in F \right\}$ é um ideal graduado não-trivial de R.

Para qualquer ideal I de R (à direita, à esquerda ou bilateral), denotamos por I_{gr} o maior ideal G-graduado contido em I.

Seja R um anel G-graduado e $S \subseteq h(R) \cap Z(R)$ é um monóide multiplicativo. Podemos definir uma graduação em R_S pondo $(R_S)_g = \{as^{-1} \mid s \in S, a \in h(R)$ tais que $g = \deg a(\deg s)^{-1}\}$. Com efeito, se $xs^{-1}, yt^{-1} \in (R_S)_g$ então $g = \deg x(\deg s)^{-1} = \deg y(\deg t)^{-1}$ e isto implica que

$(\deg st)g = \deg xt = \deg ys$. Como $xs^{-1} + yt^{-1} = (xt + ys)(st)^{-1}$, segue da última relação obtida que $\deg(xt + ys) = (\deg st)g$. Consequentemente,

$$\begin{aligned} \deg(xt + ys)(st)^{-1} &= \deg(xt + ys)(\deg st)^{-1} \\ &= (\deg st)g(\deg st)^{-1} \\ &= \deg g. \end{aligned}$$

Portanto $(R_S)_g$ é um subgrupo aditivo de R_S, para cada $g \in G$. De modo similar pode-se verificar que $(R_S)_g(R_S)_h \subseteq (R_S)_{gh}$. Agora ficou claro que $R_S = \sum_{g\in G}(R_S)_g$. O denominador comum produz que a soma é direta. E isto demonstra o que queríamos.

Definição 3.1.7. *Seja R um anel G-graduado. Um R-módulo à esquerda M é um* **módulo G-graduado** *se*

$$M = \bigoplus_{g\in G} M_g,$$

onde $\{M_g \mid g \in G\}$ é uma família de subgrupos do grupo abeliano M tal que $R_hM_g \subseteq M_{hg}$ para quaisquer $g, h \in G$.

Os elementos do conjunto $h(M) = \bigcup_{g\in G} M_g$ são chamados **elementos homogêneos** do módulo M, e qualquer elemento não-nulo $m = \sum_{g\in G} m_g \in M$ se expressa de modo único como uma soma de componentes homogêneas m_g, onde $m_g \neq 0$ apenas para uma quantidade finita de elementos g. Se $m \neq 0$ pertence a M_g, para algum $g \in G$, dizemos que g é o **grau** de m e escrevemos: $\deg m = g$. Segue da Proposição 3.1.3 que, para cada $g \in G$, M_g é um R_e-módulo.

Definição 3.1.8. *Sejam R e S anéis G-graduados. Um grupo abeliano M é um R-S-bimódulo* **graduado** *se $M = \bigoplus_{g\in G} M_g$ é um R-S-bimódulo tal que a estrutura de R-módulo à esquerda é graduada e a estrutura de S-módulo à direira é graduada, i.e., para $h, g, k \in G$ temos $R_hM_gS_k \subseteq M_{hgk}$.*

A partir de agora todos os anéis graduados e módulos graduados são G-graduados por definição. Assim, a frase "X é um módulo graduado" significa que X é um R-módulo à esquerda G-graduado, onde R é um anel G-graduado, a menos que seja feita alguma menção contrária.

Definição 3.1.9. *Um submódulo N de um módulo graduado M é um* **submódulo graduado** *se*

$$N = \bigoplus_{g\in G} N_g,$$

onde $N_g = N \cap M_g$. Equivalentemente, N é graduado se para todo elemento $n \in N$ as suas componentes homogêneas (como elemento de M) estão em N.

Exemplo 3.1.10. *Seja M um módulo graduado e N um submódulo de M. Seja $(N)_g$ o submódulo de M gerado por $N \cap h(M)$. Seja K um submódulo de N e assuma que K é um submódulo graduado de M que contém $(N)_g$. Dado $u \in K$, $u = \sum_{g\in G} n_g$ onde $n_g \in K \cap M_g$. Como $K \subseteq N$ e $M_g \subseteq h(M)$, temos que $n_g \in N \cap h(M)$. Portanto $u \in (N)_g$. Em outras palavras, $(N)_g$ é maximal entre os submódulos de N que são submódulos graduados de M.*

Uma graduação em um módulo M induz uma graduação no módulo quociente M/N, onde N é um submódulo graduado de M. Basta por $(M/N)_g = \{m + N \mid m \in M_g\}$. De fato, se $u \in M$ temos que $u = \sum_{g\in G} u_g$ onde $u_g \in M_g$ para cada $g \in G$. Então $u + N = \sum_{g\in G}(u_g + N)$. Portanto $M/N = \sum_{g\in G}(M/N)_g$. Finalmente, suponha que $\sum_g(u_g + N) = 0 + N$ em M/N, onde $u_g \in M_g$ para cada $g \in G$. Então $\sum_{g\in G} u_g \in N$. Os u_g são as componente homogêneas de $\sum u_g$ e uma vez que N é graduado, temos que $u_g \in N$. Consequentemente, $u_g + N = 0 + N$ para todo $g \in G$. Logo $M/N = \bigoplus_{g\in G}(M/N)_g$. Além disso, $R_h \cdot (M/N)_g = (R_h M_g + N)/N \subseteq (M_{hg} + N)/N \subseteq (M/N)_{hg}$. O módulo M/N é chamado **quociente graduado de** M **por** N.

Sejam R e R' anéis graduados. Um homomorfismo de anéis f é graduado se $f(R_g) \subseteq R'_g$ para todo $g \in G$. Do mesmo modo são definidos isomorfismos, endomorfismo e automorfismos G-graduados.

Definição 3.1.11. *Uma aplicação R-linear $f : M \to N$ de módulos graduados é um* **homomorfismo graduado de grau** *g se $f(M_h) \subseteq N_{hg}$ para todo $h \in G$. Quando $g = e$, dizemos f é um* **homomorfismo graduado**.

Os homomorfismos graduados de grau g formam um subgrupo aditivo de $\mathrm{Hom}_R(M, N)$ o qual será denotado por $\mathrm{HOM}_R(M, N)_g$. É claro que o conjunto $\bigoplus_{g\in G} \mathrm{HOM}_R(M, N)_g$ é um grupo abeliano (aliás, G-graduado) o qual é denotado por $\mathrm{HOM}_R(M, N)$. Quando $N = M$ obtemos o anel G-graduado

$$\mathrm{END}_R(M) = \bigoplus_{g\in G} \mathrm{HOM}_R(M, M)_g$$

o qual é chamado **anel graduado de endomorfismos** de um R-módulo M. Escreveremos $\mathrm{END}_R(M)_g$ para denotar $\mathrm{HOM}_R(M, M)_g$. A composição de um homomorfismo de grau g com um homomorfismo de grau h é um homomorfismo de grau hg.

Para qualquer homomorfismo $f : M \to N$ homogêneo (i.e., homomorfismos pertencentes a $\bigcup_{g\in G} \mathrm{HOM}_R(M, N)_g$), os submódulos $ker(f) \subseteq M$ and $Im(f)$ são graduados. Se $N \subseteq M$ são módulos graduados, então o epimorfismo canônico $\pi : M \to M/N$ é homogêneo de grau e.

Lema 3.1.12. *Sejam M e N módulos graduados. O grupo $\mathrm{HOM}_R(M, N)$ consiste de todos os $f \in \mathrm{Hom}_R(M, N)$ para os quais existe um subconjunto finito de G, digamos W, tal que*

$$(*) \quad f(M_g) \subseteq \sum_{h\in W} N_{gh}, \quad \textit{para todo } g \in G.$$

Demonstração. Suponha que $f \in \mathrm{HOM}_R(M, N)$. Como $\mathrm{HOM}_R(M, N) = \bigoplus_{g\in G} \mathrm{HOM}_R(M, N)_g$, existem $g_1, \ldots, g_n \in G$ tais que $f = f_{g_1} + \cdots + f_{g_n}$ e $f_{g_i} \in \mathrm{HOM}(M, N)_{g_i}$, $i = 1, \ldots, n$. Portanto f satisfaz a relação $(*)$. Reciprocamente, suponha que $f \in \mathrm{Hom}_R(M, N)$ satisfaz $(*)$ para algum conjunto finito $X \subseteq G$. Olhando para um m_g em M_g, por $(*)$ segue que $f(m_g) = \sum_{h\in X} n_{g,gh}$ para únicos $n_{g,gh} \in N_{gh}$, $h \in X$. Para qualquer $h \in X$ defina $f_h(m_g) = n_{g,gh}$. Temos que $f_h \in \mathrm{HOM}_R(M, N)_h$ e $f = \sum_{h\in X} f_h$. Assim $f \in \mathrm{HOM}_R(M, N)$. □

Corolário 3.1.13. *Temos que* $\mathrm{HOM}_R(M,N) = \mathrm{Hom}_R(M,N)$ *em cada um dos casos seguintes:*

(1) *O grupo* G *é finito.*

(2) M *(sem graduação) é finitamente gerado.*

Demonstração. (1) Seque imediatamente do lema acima. (2) Suponha que M (sem graduação) é gerado por $m_1, \ldots, m_r$. Não é muito restritivo supor que $m_1, \ldots, m_r$ são homogêneos e não-nulos, de grau $h_1, \ldots, h_r$ respectivamente. Considere $f \in \mathrm{Hom}_R(M,N)$, então: para $i = 1, \ldots, r$, $f(m_i) = \sum_{j=1}^{t_i} n_{g_{ij}}$ com $n_{g_{ij}} \in N_{g_{ij}}, g_{ij} \in G$. Para cada i, $1 \leqslant i \leqslant r$ pomos: $W_i = \{h_i^{-1}g_{i1}, h_i^{-1}g_{i2}, \ldots, h_i^{-1}g_{it_1}\}$ e $W = \bigcup_{i=1}^{r} W_i$. Agora verificaremos que $f(M_g) \subseteq \sum_{k\in W} N_{gk}$ para todo $g \in G$. Para $m_g \in M_g$ podemos escrever: $m_g = \sum_{i=1}^{r} r_i m_i$ com $r_i \in h(R)$ e, $\deg r_i = gh_i^{-1}$. Portanto segue que $f(m_g) = \sum_{i=1}^{r} r_i f(m_i) = \sum_{i=1}^{r}\sum_{j=1}^{t_i} r_i n_{g_{ij}}$. Contudo $\deg r_i n_{g_{ij}} = gh_i^{-1}g_{ij}$ e portanto: $r_i N_{g_{ij}} \in N_{gk}$ onde $k = h_i^{-1}g_{ij} \in W$ para todo $1 \leqslant i \leqslant r$. □

Se M não é finitamente gerado pode acontecer de $\mathrm{HOM}_R(M,N) \neq \mathrm{Hom}_R(M,N)$ (confira a página 11 do livro [14]). Em geral a inclusão de $\mathrm{HOM}_R(M,N)$ em $\mathrm{Hom}_R(M,N)$ é própria.

Inspirados pelo exemplo **(6)** dado acima, provaremos o lema seguinte.

Lema 3.1.14. *Seja* M *um módulo graduado. Assuma que* M *possui uma base homogênea finita* $e_1, \ldots, e_n$ *e digamos que* $\deg e_i = g_i$. *Então* $\mathrm{END}_R(M) \approx M_n(R)(\overline{g})$ *onde* $\overline{g} = (g_1, \ldots, g_n)$.

Demonstração. Se $f \in \mathrm{END}_R(M)_h, h \in G$, então $f(M_g) \subseteq M_{gh}$ para todo $g \in G$. Consequentemente $f(e_i) \in M_{g_i h}$ para $i = 1, \ldots, n$. Assim podemos escrever $f(e_i) = \sum_{j=1}^{n} a_{ij}e_j$ com $\deg a_{ij} = g_i h g_j^{-1}$. A matriz (a_{ij}) associada a f está em $M_n(R)_h(\overline{g})$. □

Definição 3.1.15. *Um anel graduado* R *é dito* **fortemente graduado** *quando* $R_s R_h = R_{sh}$ *para quaisquer* $s, h \in G$.

Proposição 3.1.16. *Um anel graduado* R *é fortemente graduado se, e somente se,* $R_e = R_g R_{g^{-1}}$ *para todo* $g \in G$.

Demonstração. Supondo R fortemente graduado, a relação desejada é trivial visto que $R_g R_{g^{-1}} = R_{gg^{-1}} = R_e$. Para provar a condição necessária devemos verificar apenas que $R_{sh} \subseteq R_s R_h$, pois a inclusão contrária segue de R ser graduado. Como $1 \in R_e$ e R é graduado, temos que $R_{sh} = R_{esh} = R_e R_{sh} = R_s R_{s^{-1}} R_{sh} \subseteq R_s R_{s^{-1}sh} = R_s R_{eh} = R_s R_h$. □

3.2 Análogos Graduados da Teoria Clássica

Agora consideramos a conexão entre as noções clássicas e teoremas da teoria de anéis e seus análogos graduados que usaremos neste trabalho.

A partir de agora, seguindo a prática comum, a forma análoga graduada de uma definição

clássica será acompanhada pelo prefixo "gr-". Assim, por exemplo, um **módulo gr-irredutível** (ou gr-simples) significa um módulo graduado que não contém submódulos graduados não triviais.

Surge uma pergunta natural e importante na teoria de anéis graduados: Que propriedades de anéis e módulos graduados são equivalentes às correspondentes "gr-propriedades" e sob quais condições valem tais equivalências? No estudo desta pergunta é sempre útil considerar um anel de grupo $R[G]$ com a graduação canônica. Como pode ser imediatamente verificado, existe um isomorfismo estrutural entre os ideais (unilaterais) de um anel R e os ideais graduados (unilaterais) do anel $R[G]$ preservando inclusão, somas e produtos. Em particular, isto implica que se P é uma propriedade de anéis expressiva em termos de ideais unilaterais (por exemplo, primalidade, semiprimalidade, regularidade, primitividade, redutibilidade completa, etc.) e gr-P é seu análogo graduado natural, então o anel R possui a propriedade P se, e somente se, o anel $R[G]$ possui a propriedade gr-P.

Definição 3.2.1. *Um anel graduado que não possui divisores de zero homogêneos é um* **domínio graduado**. *Um anel graduado no qual todo elemento homogêneo não-nulo possui um inverso é chamado* **anel de divisão graduado**. *Um anel de divisão graduado e comutativo é chamado* **corpo graduado**.

Exemplo 3.2.2. *O anel $A = M_2(\mathbb{R}) = A_{\overline{0}} \oplus A_{\overline{1}}$ é um anel de divisão $\mathbb{Z}_2$-graduado, onde*

$$A_{\overline{0}} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}, \quad A_{\overline{1}} = \left\{ \begin{pmatrix} b & -a \\ -a & -b \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

Já mostramos anteriormente que $\mathbb{C}$ é $\mathbb{Z}_2$-graduado e, portanto, é um exemplo de corpo graduado. Todavia nem todo corpo graduado é um corpo no sentido clássico que já conhecemos. A definição de corpo graduado diz respeito apenas aos elementos homogêneos serem invertíveis e, não necessariamente, todos os elementos serem invertíveis. A seguir temos um exemplo de corpo graduado que não é corpo.

Exemplo 3.2.3. *Seja F um corpo de característica 0. Sobre o grupo abeliano $(\mathbb{Z}_2, +)$ considere o anel de grupo $F[\mathbb{Z}_2] = K$. Claro que K é um anel comutativo cujo elemento unidade é $1_F\overline{0}$, onde 1_F é a unidade do corpo F. Denotemos a unidade de K por 1_K. Tomando $K_{\overline{0}} = F\overline{0}$ e $K_{\overline{1}} = F\overline{1}$ nota-se que K é $\mathbb{Z}_2$-graduado, i.e., $K = K_{\overline{0}} \oplus K_{\overline{1}}$ e e vale a compatibilidade com a estrutura de anel. Além disso, se α é um elemento não-nulo de F, então $\alpha\overline{0} \neq 0$ em K e $1_K = 1_F\overline{0} = \alpha\overline{0} \cdot \alpha^{-1}\overline{0}$. Analogamente, para $\beta\overline{1} \neq 0$, tem-se $1_K = 1_F\overline{0} = 1_F(\overline{1} + \overline{1}) = \beta\overline{1} \cdot \beta^{-1}\overline{1}$. Portanto, todo elemento não-nulo em $h(K)$ é invertível. Segue da definição que K é um corpo graduado. Mas o elemento $u = \frac{1}{2}\overline{0} + \frac{1}{2}\overline{1}$ é idempotente [De fato, $u^2 = (\frac{1}{2}\overline{0} + \frac{1}{2}\overline{1})(\frac{1}{2}\overline{0} + \frac{1}{2}\overline{1}) = \frac{1}{4}\overline{0} + \frac{1}{4}\overline{1} + \frac{1}{4}\overline{1} + \frac{1}{4}\overline{0} = \frac{1}{2}\overline{0} + \frac{1}{2}\overline{1} = u$]. Logo não existe $v \in K$ tal que $uv = 1_K$, do contrário teríamos $1_K = uv = u^2v = u1_K = u$.*

Definição 3.2.4. *Um gr-módulo M sobre um anel de divisão graduado D é chamado* **espaço vetorial graduado**.

Se D é um anel de divisão graduado, o subconjunto $H = \{h \in G \mid D_h \neq (0)\}$ é um subgrupo de G. Se M é um D-módulo graduado, e $M_g \neq (0)$, $D_hM_g = M_{hg}$ para todo $h \in H$.

A menos que seja feita menção contrária, a partir de agora D denota um anel de divisão graduado.

Definição 3.2.5. *Seja V um D-espaço vetorial graduado. Um conjunto $\{v_1, \ldots, v_n\} \subseteq h(V)$ é* ***D-independente*** *(ou os elementos $v_1, \ldots, v_n \in h(V)$ são D-independentes) se, sempre que $\sum d_i v_i = 0$, $d_i \in h(D)$, implicar que $d_1 = \cdots = d_n = 0$. Um conjunto $X \subseteq h(V)$ é D-independente se todo subconjunto finito de X for D-independente.*

Da mesma forma, se $\{v_1, \ldots, v_n\} \subseteq h(V)$ não é ***D*-independente**, então existem d_i's em $h(D)$, não todos nulos, tais que $\sum d_i v_i = 0$.

Quando V é um D-espaço vetorial graduado, um conjunto $\{v_1, \ldots, v_n\} \subseteq V_g$ é D-independente se, e só se, $\{v_1, \ldots, v_n\}$ é D_e-independente. De fato, a implicação ($\Rightarrow$) é imediata pois $D_e \subseteq D$. Agora se $\sum d_i v_i = 0$, então podemos assumir que todos os d_i's pertencem a D_h, para algum $h \in G$. Se $d_1 \neq 0$, então $\sum d_1^{-1} d_i v_i = 0$ e $d_1^{-1} d_i \in D_e$ ($d_1 \in D_h$ e pelo item (2) da Proposição 3.1.3, $d_1^{-1} \in D_{h^{-1}}$; segue que $d_1^{-1} d_i \in D_{h^{-1}} D_h \subseteq D_e$).

A proposição seguinte assegura a existência de uma base para um D-espaço vetorial graduado. A demonstração deste fato não exige grandes rasgos de imaginação e basicamente usa a mesma estratégia que a versão não graduada.

Proposição 3.2.6. *Se $V \neq (0)$ é um D-espaço vetorial graduado, então V possui uma base formada por elementos homogêneos, também chamada de* **base homogênea**. *Além disso, duas quaisquer bases homogêneas de V têm a mesma cardinalidade.*

Demonstração. Já que $V \neq (0)$, existe um elemento homogêneo não-nulo $v_g \in V$ para algum $g \in G$. Assim, se $dv_g = 0$ para algum $d \in D$, $d = \sum_{h \in G} d_h$, $d_h \in D_h$, temos que $d_h v_g = 0$ para todo $h \in G$, e, uma vez que D é um anel de divisão graduado, isto implica que $d_h = 0$, para todo $h \in G$. Consequentemente, $d = 0$. Pelo Lema de Zorn (como no caso não graduado) obtemos que V tem uma base homogênea. Usando o mesmo argumento que no caso não graduado podemos concluir que duas quaisquer bases homogêneas têm a mesma cardinalidade. □

Um tratamento um pouco mais geral a respeito do que provamos, bem como transitividade de módulos, etc, pode ser encontrado na Seção 1 de [19].

Definição 3.2.7. *Um anel graduado não trivial cujos únicos ideais graduados são (0) e R é chamado* **gr-simples**.

Todo corpo graduado que é um corpo no sentido clássico é gr-simples. Mas existem corpos graduados que não são gr-simples.

Definição 3.2.8. *Um módulo graduado M é dito* ***g*-fiel** *se, para qualquer $m \in h(M)$ não-nulo, existe $r \in h(R)$ tal que $0 \neq rm \in M_g$. Dizemos que M é* **gr-fiel** *se for g-fiel para todo $g \in G$.*

Definição 3.2.9. *Um anel R graduado é dito* **gr-primitivo** *se possuir um módulo graduado gr-irredutível M tal que $\mathrm{Ann}_R(M) = (0)$. Em outras palavras, R é gr-primitivo se possuir um módulo graduado que é gr-fiel e gr-irredutível. Dizemos que $I \subseteq R$ é um* **ideal gr-primitivo** *se R/I é um anel gr-primitivo. Se um R-módulo M é gr-irredutível, então $R/\mathrm{Ann}_R(M)$ é gr-primitivo e $\mathrm{Ann}_R(M)$ é um ideal gr-primitivo.*

Provaremos agora versão graduada do Lema de Schur.

Lema 3.2.10 (gr-Lema de Schur)**.** *Se M é um módulo gr-irredutível, então* $\mathrm{END}_R(M)$ *é um anel de divisão graduado.*

Demonstração. Como o módulo M é gr-irredutível, para qualquer $m \neq 0$ em $h(M)$, temos que $Rm = M$. Em outras palavras, M é finitamente gerado. Pelo item (2) do Corolário 3.1.13, temos que

$$\underbrace{\mathrm{END}_R(M) = \mathrm{End}_R M}_{(*)}$$

Seja $\psi \neq 0$ em $h(\mathrm{END}_R(M))$. Existe $g \in G$ tal que $\psi \in \mathrm{END}_R(M)_g = \{f \in \mathrm{End}_R(M) \mid f(M_h) \subseteq M_{hg} \text{ para todo } h \in G\}$. Da igualdade $(*)$ segue que $\psi(M)$ é um submódulo de M. Veremos que $\psi(M)$ é G-graduado. Antes disso note que $\psi(M) = \sum_{h\in G} \psi(M_h)$. Seja $u \in \sum_{h\in G} \psi(M_h)$, como $\psi(M_h) \subseteq M_{hg}$ para todo $h \in G$, segue que $u = \sum_{h\in G} n_{hg}$. Supondo $u = 0$, temos $0 = u = \sum_{h\in G} n_{hg} = \sum_{h\in G} \psi(m_h) = \psi(v)$ onde $m_h \in M_h, v \in M$. Logo $v \in ker(\psi)$ e, como já observamos antes, $ker(\psi)$ é um gr-submódulo de M. Já que M é gr-irredutível e $\psi \neq 0$, resulta que $ker(\psi) = (0)$ daí $v = 0$. Pela unicidade da escrita do $0 = v$, concluimos que $m_h = 0$ para todo $h \in G$ e isso nos garante que $n_{hg} = 0$ para todo $h \in G$. Logo, temos concluido duas coisas: ψ é injetiva e a soma $\sum_{h\in G} \psi(M_h)$ é direta. Para finalizar, $R_h\psi(M_k) \subseteq R_h M_{kg} \subseteq M_{hkg}$. Logo $\psi(M)$ é graduado e, como M é gr-irreditível, temos $\psi(M) = M$. Portanto, ψ é invertível. □

Observe que se M é um módulo gr-irredutível de dimensão finita sobre R (digamos que $\dim_R M = n$), segue do lema anterior e do Lema 3.1.14 que $D = \mathrm{END}_R(M) = \mathrm{End}_R(M) \approx M_n(R)(\overline{g}) = M_n(R)(g_1, \ldots, g_n)$ para algum $\overline{g} = (g_1, \ldots . g_n) \in G^{(n)}$.

O próximo teorema é a versão graduada do Teorema da Densidade de Jacobson. A demonstração segue os passos da versão não graduada apresentada no capítulo anterior.

Definição 3.2.11. *Seja M um D-módulo graduado. Um subanel R de* $\mathrm{END}_D(M)$ *é* **gr-denso** *em* $\mathrm{END}_D(M)$ *se, para qualquer conjunto D-independente $\{m_1, \ldots, m_n\} \subseteq h(M)$ e qualquer conjunto $\{y_1, \ldots, y_n\} \subseteq M$, existe $r \in R$ (dependendo de $\{y_1, \ldots, y_n\}$) tal que $rm_i = y_i$ para $i = 1, \ldots, n$.*

Teorema 3.2.12 (gr-Teorema da Densidade)**.** *Para um anel graduado R as seguintes afirmações são equivalentes:*

(1) *R é gr-primitivo;*

(2) *R é gr-denso em* $\mathrm{END}_D(M)$ *para algum anel de divisão graduado D e um D-módulo graduado M.*

Demonstração. Provaremos a implicação não-trivial, i.e., (1) ⇒ (2). Por R ser gr-primitivo, possui um módulo M que é gr-fiel e gr-irredutível. Pelo lema anterior (gr-Lema de Schur), $\mathrm{END}_R(M) = \mathrm{End}_R(M) = D$ é um anel de divisão graduado.

Como no caso não graduado, a demonstração será feita por indução em n (a quantidade de elementos homogêneos D-independentes tomados). Para $n = 1$ e $m \neq 0$ em $h(M)$, Rm é um

submódulo graduado de M, daí $Rm = M$. Logo para qualquer $y \in M$ existe $r_y \in R$ tal que $r_y m = y$. Agora assuma que a afirmação seja verdadeira $n-1$. Considere $\{m_1, \ldots, m_n\} \subseteq h(M)$, $(m_1, \ldots, m_n) \in M^{(n)}$. Temos que $R(m_1, \ldots, m_{n-1})$ é um R-módulo graduado, pois é gerado por elementos homomogêneos e, pela hipótese de indução, isso implica que $R(m_1, \ldots, m_{n-1}) = M^{(n-1)}$.

Provemos que existe $r_n \in R$ tal que $r_n m_n \neq 0$ e $r_n m_i = 0$ para todo $i \neq n$. Com efeito, raciocinando por contradição, o gr-homomorfismo de gr-módulos $\psi : R(m_1, \ldots, m_{n-1}) \to M$ dado por $\psi(r(m_1, \ldots, m_{n-1})) = rm_n$ está bem definido, implicando que $\psi \in \mathrm{HOM}(M^{(n-1)}, M) \approx (\mathrm{END}_R(M))^{(n-1)} = D^{(n-1)}$. Esse isomorfismo nos permite escrever ψ como $(d_1, \ldots, d_{n-1}) \in D^{(n-1)}$, daí temos que $m_n = \psi(m_1, \ldots, m_{n-1}) = \sum_{i=1}^{n-1} d_i m_i$ e isso contradiz o que havíamos assumido sobre a D-independência de $m_1, \ldots, m_n$.

Com os mesmos argumentos do caso não graduado temos a densidade de R em $\mathrm{END}_D(M)$. □

Como no caso não-graduado o teorema seguinte ocorre.

Teorema 3.2.13. *Seja R um anel gr-primitivo. Então uma das seguintes afirmações vale:*

(1) *R é isomorfo a $M_n(D)(\overline{g})$ para algum $\overline{g} = (g_1, \ldots, g_n) \in G^{(n)}$ e algum anel de divisão graduado D.*

(2) *Para cada $m \in \mathbb{Z}^+$ existe um subanel graduado S_m de R que tem $M_m(D)(\overline{g})$ como imagem homomorfa.*

Demonstração. Seja M um R-módulo gr-fiel e gr-irredutível do anel R. Pelo Lema 3.2.10 (gr-Lema de Schur) $\mathrm{END}_R(M) = D$ é um anel de divisão graduado. Além disso, M é um gr-espaço vetorial sobre D.

(1) Se $[M : D] = n < \infty$ para algum $n \in \mathbb{Z}^+$, podemos escolher uma base homogênea $\{w_1, \ldots, w_n\}$ de M sobre D. Dado $\psi \in \mathrm{END}_D(M)$, segue do teorema anterior (gr-Teorema da Densidade) que existe $r \in R$ tal que $rw_i = \psi(w_i)$ e isto implica que o gr-homomorfismo de anéis

$$\begin{array}{rccccc} \Psi: & R & \longrightarrow & \mathrm{END}_D(M) & & \\ & r & \mapsto & \widehat{r} & : & \begin{array}{ccc} M & \to & M \\ w_i & \mapsto & rw_i \end{array} \end{array}$$

é sobrejetor. E se r é tal que $0 = \Psi(r) = \widehat{r}$, então $r = 0$, pois M é gr-fiel como R-módulo. Portanto, $R \approx \mathrm{END}_D(M) \approx M_n(D)(\overline{g})$ para algum $\overline{g} = (g_1, \ldots, g_n) \in G^{(n)}$ pelo Lema 3.1.14.

(2) Se $[M : D]$ não é finita, dado qualquer $n \in \mathbb{Z}^+$ e elementos homogêneos D-independentes $m_1, \ldots, m_n$ em M. Seja $V = Dm_1 + \cdots + Dm_n$ e $R' = \{r \in R \mid rV \subseteq V\}$ D-subespaço. Temos que V é um D-subespaço graduado de M, pois é gerado por elementos homogêneos e $R' \neq \varnothing$ já que $0 \in R'$. Pelo teorema anterior, toda gr-transformação D-linear de V em V pode ser induzida por um elemento de R. Portanto, existe um gr-homomorfismo sobrejetor f de R em $\mathrm{END}_D(M)$. □

Agora que já definimos módulos graduados e anéis graduados ficará bem mais fácil perceber o que entendemos como uma álgebra graduada.

Definição 3.2.14. *Seja A uma F-álgebra. A álgebra A é dita G-***graduada** *(ou simplesmente 'graduada') se*

$$A = \bigoplus_{g \in G} A_g$$

onde os A_g's são subespaços vetoriais de A e $A_g A_h \subseteq A_{gh}$ para todo $g, h \in G$.

Exemplo 3.2.15. *Seja $\mathbf{G}$ a álgebra de Grassmann (exterior) de um espaço vetorial de dimensão enumerável sobre um corpo F cuja característica é diferente de 2. Como no Exemplo 1.6.5, $\mathbf{G}_0$ (resp. $\mathbf{G}_1$) denota o F-sebespaço de $\mathbf{G}$ gerado pelo conjunto $\{e_{i_1} \cdots e_{i_{2k}} \mid 1 \leqslant i_1 < \cdots < i_{2k}, k \geqslant 0\}$ (resp. $\{e_{i_1} \cdots e_{i_{2k+1}} \mid 1 \leqslant i_1 < \cdots < i_{2k+1}, k \geqslant 0\}$). Rapidamente pode-se verificar que $\mathbf{G}_0\mathbf{G}_0 + \mathbf{G}_1\mathbf{G}_1 \subseteq \mathbf{G}_0$ e $\mathbf{G}_0\mathbf{G}_1 + \mathbf{G}_1\mathbf{G}_0 \subseteq \mathbf{G}_1$. Isto diz que a decomposição $\mathbf{G} = \mathbf{G}_0 \oplus \mathbf{G}_1$ é uma $\mathbb{Z}_2$-graduação de $\mathbf{G}$.*

Uma álgebra $\mathbb{Z}_2$-graduada é chamada **superálgebra**.

Definição 3.2.16. *O* **radical de Jacobson graduado** *de um anel graduado R, denotado por $\mathrm{Jac}_{\mathrm{gr}}(R)$, é a interseção de todos os ideais à esquerda de R que são gr-maximais.*

Definição 3.2.17. *Um anel R é* **gr-semissimples** *se $\mathrm{Jac}_{\mathrm{gr}}(R) = (0)$.*

Definição 3.2.18. *Seja R um anel graduado. Um* **nil ideal graduado** *de R é um ideal graduado cujos elementos homogêneos são nilpotentes.*

Assim como as versões graduadas do Teorema de Densidade, do Lema se Schur, etc, o próximo teorema tem demonstração análoga ao caso não graduado apresentado no capítulo anterior.

Teorema 3.2.19. *Se R é uma anel graduado e não possui nil ideais graduados, então* $\mathrm{Jac}_{\mathrm{gr}}(R[X]) = (0)$.

Tudo o que definimos até agora para anéis graduados (até mesmo as notações) tem a sua versão para álgebras graduadas e para obter essas definições tudo o que se deve fazer é substituir a palavra 'anel' (resp. subanel, subgrupo aditivo) por 'álgebra' (resp. subálgebra, subespaço vetorial). Sendo assim, não vamos definir termos como, por exemplo, ideal graduado de uma gr-álgebra ou o que entendemos por uma álgebra gr-primitiva, etc.

Definição 3.2.20. *Uma álgebra graduada A é uma* **gr-PI-álgebra** *se existe um polinômio não trivial f em $F\langle X\rangle$ tal que $f(a_1, \ldots, a_n) = 0$ para quaisquer elementos $a_1, \ldots, a_n \in h(A)$. Além disso, uma álgebra graduada A é uma PI-álgebra se, sem graduação, A é uma PI-álgebra.*

Seja A uma álgebra graduada. O centro $Z(A)$ de A pode não ser graduado.

Exemplo 3.2.21. *Seja F um corpo e G um grupo não-abeliano de ordem n. A álgebra de grupo $A = F[G]$ é um anel de divisão graduado ($A_{g_i} = \{\alpha g_i \mid \alpha \in F\}$, $i = 1, \ldots, n$, e se $\beta g_i \in h(A) - \{0\}$, então $\beta^{-1} g_i^{-1} \beta g_i = 1$), mas o seu centro $Z(F[G])$ não é um corpo graduado uma vez que $g_1 + \cdots + g_n \in Z(F[G])$, mas $g_i \notin Z(F[G])$ se $g_i \notin Z(G)$.*

Para uma álgebra graduada A denotaremos por $Z_{\rm gr}(A)$ a subálgebra graduada maximal em $Z(A)$. A subálgebra $Z_{\rm gr}(A)$ será chamada de **centro graduado** de A. Claro que $Z_{\rm gr}(A)$ é gerada pelos elementos de $Z(A) \cap h(A)$. Vale notar que se o grupo G é abeliano vale a igualdade $Z_{\rm gr}(A) = Z(A)$ (caso haja interesse, consulte a página 259 do livro [14]).

Para um anel graduado R, chamamos **centróide graduado**, denotado por $C_{\rm gr}(R)$, ao subanel graduado de $E(R)$ gerado pelos endomorfismos homogêneos de $E(R)$ que comutam com os elementos de $B(R)$. $C_{\rm gr}(R)$ é o anel de endomorfismos graduados do bimódulo graduado ${}_RR_R$ e $C_{\rm gr}(R) \subseteq C(R)$.

Teorema 3.2.22. *Se R é um anel gr-simples, então seu centróide graduado $C_{\rm gr}(R)$ é um corpo graduado. Além disso, $Z_{\rm gr}(R) \approx C_{\rm gr}(R)$.*

Demonstração. Como R é gr-simples, temos que $R^2 = R$ e segue do Lema 2.1.18 que $C(R)$ é comutativo e portanto $C_{\rm gr}(R)$ é comutativo uma vez que vale a inclusão $C_{\rm gr}(R) \subseteq C(R)$. Já que R não contém ideais graduados não-triviais, pelo gr-Lemade Schur cada elemento homogêneo de $C_{\rm gr}(R)$ é invertível. Portanto $C_{\rm gr}(R)$ é um corpo graduado.

Agora vamos demonstrar a segunda parte. Se $a \in h(Z_{\rm gr}(R))$, então $T_a \in h(C_{\rm gr}(R))$ e a aplicação $\Phi : Z_{\rm gr}(R) \to C_{\rm gr}(R)$, onde $\Phi(a) = T_a$ é um homomorfismo injetivo de grau e ($e \in G$). Se $f \in h(C_{\rm gr}(R))$, então para qualquer $r \in R$ temos $f(r) = f(1r) = f(r1) = f(1)r = rf(1)$. Tomando $a = f(1)$ obtemos que $a \in h(Z_{\rm gr}(R))$ e $f(r) = ra$, assim $f = T_a$. □

Usando o Teorema 3.2.12 podemos obter o análogo graduado do Teorema de Kaplansky que foi provado por Zhu em [21].

Teorema 3.2.23 (gr-Kaplansky)**.** *Seja A uma álgebra gr-primitiva satisfazendo uma identidade polinomial de grau d. Então A é gr-simples e de dimensão finita sobre $Z_{\rm gr}(A)$. Além disso, $[A : Z_{\rm gr}(A)] \leqslant [d/2]^2$.*

Demonstração. Já que A é uma álgebra gr-primitiva, pelo Teorema 3.2.13 temos uma das duas possibilidades: $A \approx M_n(D)(\overline{g})$, para algum $\overline{g} = (g_1, \ldots, g_n) \in G^{(n)}$ e um anel de divisão graduado D, ou para qualquer $m \in \mathbb{Z}^+$ existe uma subálgebra graduada S_m em A, que tem $M_m(D)(\overline{g})$ como imagem homomorfa. Veremos que esta última possibilidade não é possível. De fato, se A satisfaz uma identidade polinomial, todas as suas subálgebras e imagens homomorfas de A satisfazem as mesmas identidades. Consequentemente, para qualquer $m \in \mathbb{Z}^+$ a álgebra $M_m(F)$ satisfaz a identidade dada, onde F é o centro de D_e. Como m é arbitrário (podendo ser igual a $2d$), isto é uma contradição (com o Teorema de Amitsur-Levitzki), pois $M_m(F)$ não pode satisfazer uma identidade de grau menor do que $2m$.

Portanto resta que $A \approx M_n(D)(\overline{g})$ para algum $\overline{g} \in G^{(n)}$ e assim A é uma álgebra gr-simples.

Seja $Z = Z_{\rm gr}(D) = Z_{\rm gr}(A)$ (a segunda igualdade é fruto de uma identificação, i.e., $Z_{\rm gr}(D)$ pode ser visto como $Z_{\rm gr}(M_n(D)(\overline{g})) = Z_{\rm gr}(A)$) e seja L o subcorpo graduado maximal em D. Considere a PI-álgebra graduada $D \otimes_Z L$. De modo similar ao Lema 2.2.2, temos que $D \otimes_Z L$ é um anel gr-denso em $\mathrm{END}_L(D)$. Consequentemente $D \otimes_Z L \approx M_m(L)$ para algum $m \in \mathbb{Z}^+$. Assim

$$A \otimes_Z L \approx M_n(D) \otimes_Z L \approx M_{mn}(L).$$

Então $d \geqslant (2mn)$ e $mn \leqslant [d/2]$.

Portanto, $[A \otimes_Z L : L] = [A : Z] = (mn)^2 \leqslant [d/2]^2$ como buscávamos. □

Recorde que o **radical primo** de um anel R, denotado por $N(R)$, é a interseção de todos os ideais primos de R. Seja R um anel graduado. Um ideal P de R é **gr-primo** se sempre que $aRb \subseteq P$, onde $a, b \in h(R)$, implicar que $a \in P$ ou $b \in P$ ou, equivalentemente, sempre que $J_1 J_2 \subseteq P$, para J_1, J_2 ideais graduados de R, tem-se $J_1 \subseteq P$ ou $J_2 \subseteq P$. O **radical primo graduado** de R, denotado por $N_{\mathrm{gr}}(R)$, é a interseção de todos os ideais gr-primos de R. O anel R é dito **gr-primo** se (0) é um ideal gr-primo de R. E R é dito **gr-semiprimo** se $N_{\mathrm{gr}}(R) = (0)$.

Lema 3.2.24. *Seja R é um anel graduado e $I \lhd R$. Então I é gr-primo se, e só se, $I = P_{\mathrm{gr}}$, o ideal graduado associado a algum ideal primo P de R. Isto é, P_{gr} é gerado pelo conjunto $P \cap h(R)$. Consequentemente $N_{\mathrm{gr}}(R) = N(R)_{\mathrm{gr}}$, o ideal graduado associado a $N(R)$.*

Demonstração. Uma das implicações é trivial. A saber, se P é um ideal primo, então P_{gr} é um ideal gr-primo. Reciprocamente, digamos que I é gr-primo. Seja Ω o conjunto de todos os ideais J de R tais que $J_{\mathrm{gr}} = I$ [Claro que $\Omega \neq \varnothing$, pois $I \in \Omega$]. Podemos aplicar o Lema de Zorn e escolher um tal ideal que seja maximal, vamos chamá-lo de P. Digamos que $J \supseteq P$, $J' \supseteq P$ são ideais com $JJ' \subseteq P$, então $J_{\mathrm{gr}} J'_{\mathrm{gr}} \subseteq P_{\mathrm{gr}}$, assim $J_{\mathrm{gr}} \subseteq P_{\mathrm{gr}}$ ou $J'_{\mathrm{gr}} \subseteq P_{\mathrm{gr}}$ uma vez que $P_{\mathrm{gr}} = I$ é um ideal gr-primo. Pela maximalidade de P, segue que $J \subseteq P$ ou $J' \subseteq P$. Portanto P é um ideal primo de R. □

Existe outra forma de caracterizar o radical primo de um anel R por meio de uma união ascendente de ideais. Daremos esta caracterização com o intuito de tornar clara a notação utilizada no próximo lema. Denote por $N_0(R)$ o ideal zero e por $N_{i+1}(R)$, quando $N_i(R)$ já está definido, a pré-imagem em R das somas de todos os ideais nilpotentes do anel $R/N_i(R)$.

Tendo construído $N_i(R)$ para todo $i = 1, 2, \ldots$, obtemos o ideal $N_\omega(R) = \bigcup_{i=1}^{\infty} N_i(R)$. Pode acontecer que $R/N_\omega(R)$ também tenha ideais nilpotentes diferentes de zero. Então definimos $N_{\omega+1}(R)$ do mesmo modo como fizemos acima. Mais geralmente falando, para qualquer α da forma $\beta + 1$ (i.e., α não é um ordinal limite no sentido da teoria de conjuntos), definimos $N_\alpha(R)$ como a pré-imagem de todos os ideais nilpotentes em $R/N_\beta(R)$. Se α é um ordinal limite (Um ordinal α é um ordinal limite se existe um ordinal menor do que α e, sempre que β é um ordinal menor do que α, existe um ordinal γ tal que $\beta < \gamma < \alpha$.), então $N_\alpha(R) = \bigcup_{\beta<\alpha} N_\beta(R)$. Pelo princípio da indução transfinita, existe α tal que $N_\alpha(R) = R$ ou $N_\alpha(R) = N_{\alpha+1}(R)$ e neste último caso $N_\alpha(R)$ é chamado de menor nilradical ou radical primo de R.

A demonstração para o lema seguinte pode ser encontrada na página 252 da referência [5].

Lema 3.2.25. *Para todo α, $(N_{\mathrm{gr}}(R))_\alpha = (N_\alpha(R))_{\mathrm{gr}}$, e assim $N_{\mathrm{gr}}(R) = \cup_\alpha (N_{\mathrm{gr}}(R))_\alpha$.*

Segue dos dois lemas anteriores que $N_{\mathrm{gr}}(R)$ é um radical primo graduado de R e $N_{\mathrm{gr}}(R) = N(R)_{\mathrm{gr}}$ é o maior ideal graduado de R contido em $N(R)$.

Teorema 3.2.26 (Balaba)**.** *Seja A uma PI-álgebra gr-prima, $Z(A)$ o centro de A, e S o conjunto dos elementos regulares de $h(A) \cap Z(A) = h(Z(A))$. Então:*

(1) $S = h(Z(A))$;

(2) *a álgebra de quocientes centrais A_S é uma PI-álgebra gr-prima;*

(3) $Z_{\mathrm{gr}}(A_S) = Z_{\mathrm{gr}}(A)_S$.

Demonstração. Seja $c \in h(Z(A))$, $c \neq 0$ e $ac = 0$ para algum $a \in h(A)$; então $aAc = (0)$, mas A é gr-prima, consequentemente $a = 0$ e portanto $S = h(Z(A))$.

Pelo que provamos no início deste capítulo, A_S é G-graduada, onde

$$(A_S)_g = \{as^{-1} \in A_S \mid s \in S, a \in h(a), g = (\deg a)(\deg s)^{-1}\}.$$

Vamos mostrar que A_S é gr-prima. De fato, se $as^{-1}A_Sbt^{-1} = (0)$, $as^{-1}, bt^{-1} \in h(A_S)$, então

$$as^{-1}cr^{-1}bt^{-1} = 0$$

para qualquer $cr^{-1} \in A_S$. Como $srt \in S \subseteq Z(A)$, podemos multiplicá-lo na equação anterior e obter $acb = 0$ para todo $c \in A$, donde temos que $a = 0$ ou $b = 0$, uma vez que A é gr-prima.

Pela Proposição 2.3.7 segue que A e A_S satisfazem as mesmas identidades. Finalmente, a Proposição 2.3.3 implica que $Z(A_S) = Z(A)_S$, consequentemente $Z_{\mathrm{gr}}(A_S) = Z_{\mathrm{gr}}(A)_S$. □

Definição 3.2.27. *O* **nilradical** *de um anel R, denotado por* $\mathrm{Nil}(R)$*, é a soma de todos os nil ideais de R. Em outras palavras,* $\mathrm{Nil}(R)$ *é a somas dos ideais de R que consistem de elementos nilpotentes. Quando R é um anel graduado, o* **gr-nilradical** *(ou nilradical graduado) de R, denotado por* $\mathrm{Nil}_{\mathrm{gr}}(R)$*, é a soma de todos os nil ideais graduados de R.*

Note que $N(R)$ é um subconjunto de $\mathrm{Nil}(R)$.

Observação 3.2.28. *Na página 363 do livro [1], Bahturin apresenta uma demonstração de que, para uma PI-álgebra A,* $\mathrm{Nil}(A) = N(A)$*. Usaremos este fato na demonstração da proposição abaixo.*

O resultado a seguir é a versão graduada do Teorema 2.2.9 (Rowen) e foi provado por Balaba em [2]. Aliás, os próximos resultados são todos devidos à Balaba.

Teorema 3.2.29 (Rowen-Balaba)**.** *Seja A uma PI-álgebra gr-prima, Z_{gr} o centro graduado de A, e I um ideal graduado não-nulo de A. Então $I \cap Z_{\mathrm{gr}} \neq (0)$.*

Demonstração. Já que A é uma PI-álgebra, segue da observação anterior que o nilradical e o radical primo de A coincidem. Além disso, $\mathrm{Nil}_{\mathrm{gr}}(A) = \mathrm{Nil}(A)_{\mathrm{gr}}$ e, portanto, segue do que foi concluído após o Lema 3.2.25 que $N_{\mathrm{gr}}(A) = N(A)_{\mathrm{gr}} = \mathrm{Nil}(A)_{\mathrm{gr}} = \mathrm{Nil}_{\mathrm{gr}}(A)$.

A álgebra A não pode conter ideais graduados nilpotentes não-nulos, uma vez que A é gr-prima e consequentemente também não possui nil ideais graduados não-nulos. Então, pelo Teorema 3.2.19, a álgebra graduada $A[X] = \bigoplus_{g \in G} A_g[X]$ é gr-semissimples. Além disso, $A[X]$ é uma PI-álgebra [De fato, A satisfaz uma identidade multilinear e $A[X]$ é uma extensão central de A logo satisfaz as mesmas identidades multilineares que A]. Consequentemente, pelo Teorema 3.2.23 (gr-Kaplansky), $A[X]$ é um produto subdireto de PI-álgebras gr-primitivas de grau limitado (ver a página 44 do capítulo anterior). Então, para qualquer ideal graduado gr-primitivo P em $A[X]$, P é gr-maximal logo tem-se que $P + I[X] = A[X]$ ou $I[X] \subseteq P$. Já que $\mathrm{Jac}_{\mathrm{gr}}(A[X]) = (0)$. Em outras palavras, a interseção de todos os ideais graduados gr-primitivos é igual a zero (novamente

veja a página 44 do capítulo anterior), existe P tal que $P + I[X] = A[X]$; do contrário teríamos $(0) \neq I[X] \subseteq \bigcap P = (0)$. Entre todos os P's para os quais vale a igualdade anterior escolha um P_0 tal que o grau da álgebra de matriz $A[X]/P_0 \approx M_{n_0}(K)$ é maximal (aqui K é um corpo graduado). Seja f um polinômio de Razmyslov central para a álgebra $M_{n_0}(K_e)$.

Já que K é um anel comutativo e o polinômio de Razmyslov é multilinear (Teorema 1.9.14), f é central para $M_{n_0}(K)$ também. Consequentemente, f é central ou é uma identidade para toda álgebra gr-primitiva de grau $n \leqslant n_0$. Segue que para quaisquer $a_1, \ldots, a_n \in A[X]$ e qualquer ideal gr-primitivo P, $(f(a_1, \ldots, a_n) + P)/P$ está no centro da álgebra $A[X]/P$. Logo, também pertence ao centro de $A[X]$. Já que f é central para $A[X]/P_0$ e $P_0 + I[X] = A[X]$, podemos encontrar $a_1^0, \ldots, a_n^0 \in I[X]$ tais que $f(a_1^0, \ldots, a_n^0) \neq 0$. Pela multilinearidade de f é possível escolher $a_1^0, \ldots, a_n^0$ homogêneos, assim $f(a_1^0, \ldots, a_n^0)$ é um elemento de $I[X]$ que é central, homogêneo e não-nulo.

Notemos além disso que se Z_{gr} é o centro graduado de A, então $Z_{\mathrm{gr}}[X]$ é o centro graduado de $A[X]$. Já que $Z_{\mathrm{gr}}[X] \cap I[X] \neq (0)$ e $Z_{\mathrm{gr}}[X] \cap I[X] = (Z_{\mathrm{gr}} \cap I)[X]$, temos que $Z_{\mathrm{gr}} \cap I \neq (0)$. E isto conclui a proposição. □

Corolário 3.2.30. *Seja A uma PI-álgebra gr-prima e assuma que seu centro graduado é um corpo graduado. Então A é gr-simples.*

Demonstração. Seja I um ideal graduado não-nulo de A, pela proposição anterior $I \cap Z_{\mathrm{gr}} \neq (0)$. Como por hipótese Z_{gr} é um corpo graduado, existe $u \neq 0$ em $h(A) \cap I$. Tomando o inverso de u, temos que $1 \in I$. □

Recorde que A_S, onde S é um conjunto de elementos homogêneos de $Z(A)$, é a **álgebra graduada de quocientes centrais de** A.

Definição 3.2.31. *Uma álgebra $Q(A) \supseteq A$ é a* **álgebra graduada de quocientes de** A *se:*

(1) *todo elemento homogêneo regular de A é invertível em $Q(A)$;*

(2) *todo elemento homogêneo $u \in Q(A)$ é da forma ab^{-1}, onde $a, b \in h(A)$ e b é um elemento regular.*

Agora podemos apresentar a demonstração do teorema de Posner na versão graduada.

Teorema 3.2.32 (Posner-Balaba)**.** *Seja A uma PI-álgebra gr-prima e A_S a álgebra de quocientes centrais de A. Então:*

(1) *A_S é gr-simples de dimensão finita sobre o seu centro graduado K e K é o corpo graduado de quocientes de $Z_{\mathrm{gr}}(A)$;*

(2) *A_S é a álgebra graduada de quocientes de A;*

(3) *A e A_S satisfazem as mesmas identidades.*

Demonstração. Pelo item 2 do Teorema 3.2.26 (Balaba) segue que A_S é uma PI-álgebra gr-prima e pelo item 3 da mesma proposição o centro graduado K de A_S é um corpo graduado de quocientes de $Z_{\mathrm{gr}}(A)$. Em resumo o que conseguimos até agora foi: A_S é um PI-álgebra gr-prima e seu centro graduado é um corpo graduado. Logo podemos invocar o corolário anterior e temos que A_S é gr-simples e consequentemente gr-primitiva. Agora estamos nas hipóteses do teorema 3.2.23 (gr-Kaplansky), portanto A_S é de dimensão finita sobre seu centro graduado. Isto prova o item (1).

A fim de provar o item (2) vamos verificar que A_S satisfaz as condições da definição acima. Note que, ainda pelo Teorema 3.2.23 (gr-Kaplansky), A_S é isomorfa ao anel graduado das matrizes sobre algum anel de divisão graduado. Logo todo elemento regular de $h(A_S)$ é invertível. Como qualquer elemento homogêneo de A_S tem a forma as^{-1}, $a \in A$, $s \in S$, segue que qualquer elemento regular de A é regular também em A_S, e portanto é invertível em A_S. Logo, A_S é a álgebra graduada de quocientes de A.

O item (3) deste teorema já foi provado no Teorema 3.2.26 (Balaba). □

A versão graduada do teorema de Posner demonstrado acima abriu o caminho para diversas aplicações importantes e dentre as tais gostaríamos de citar pelo menos uma. Centrone em [4] generalizou a noção de dimensão de Gelfand-Kirillov para álgebras graduadas por um grupo abeliano finito G e, mais recentemente, usou de maneira forte os resultados tratados aqui para obter em [3] uma relação entre a gr-dimensão de Gelfand-Kirillov de uma PI-álgebra gr-prima e seu grau de transcendência, onde a álgebra em questão é graduada por um grupo abeliano. Como consequência de tal relação, no mesmo artigo, é calculado o valor exato da dimensão de Gelfand-Kirillov $\mathbb{Z}_n$-graduada de $M_n(F)$.

Referências Bibliográficas

[1] Bahturin, Y. *Basic Structures of Modern Algebra*. Springer, 1993.

[2] Balaba, I. Graded prime pi-algebras. *Journal of Mathematical Sciences 128*, 6 (2005), 3345–3349.

[3] Centrone, L. The graded gelfand–kirillov dimension of verbally prime algebras. *Linear and Multilinear Algebra 59*, 12 (2011), 1433–1450.

[4] Centrone, L. A note on graded gelfand–kirillov dimension of graded algebras. *Journal of Algebra and Its Applications 10*, 05 (2011), 865–889.

[5] Cohen, M., and Montgomery, S. Group-graded rings, smash products, and group actions. *Transactions of the American Mathematical Society 282*, 1 (1984), 237–258.

[6] Dehn, M. Über die grundlagen der projektiven geometrie und allgemeine zahlsysteme. *Mathematische Annalen 85*.

[7] Drensky, V., and Formanek, E. *Polynomial Identity Rings*. Springer, 2004.

[8] Giambruno, A., and Zaicev, M. *Polynomial Identities and Asymptotic Methods*. No. 122. American Mathematical Soc., 2005.

[9] Herstein, I. N. *Noncommutative Rings*. No. 15. Cambridge University Press, 2005.

[10] Herstein, I. N. *Topics in Algebra*. John Wiley & Sons, 2006.

[11] Jacobson, N. Structure theory for algebraic algebras of bounded degree. *Annals of Mathematics* (1945), 695–707.

[12] Jacobson, N. *Structure of Rings*, vol. 37. American Mathematical Soc., 1984.

[13] Kanel-Belov, A., and Rowen, L. H. *Computational Aspects of Polynomial Identities*, vol. 10. 2005.

[14] Nastasescu, C., and Van Oystaeyen, F. *Graded Ring Theory*. Amsterdam, 1982.

[15] Nastasescu, C., and Van Oystaeyen, F. *Methods of Graded Rings*. Springer, 2004.

[16] Robinson, D. *A Course in the Theory of Groups*, vol. 80. Springer Science & Business Media, 1996.

[17] Rowen, L. H. *Polynomial Identities in Ring Theory*, vol. 84. Academic Press, 1980.

[18] Rowen, L. H. *Ring Theory, 83: Student Edition*. Academic Press, 2012.

[19] Shaoxue, L., Beattie, M., and Hongjin, F. Graded division rings and the jacobson density theorem. *Journal of Beijing Normal University (Natural Science) 27*, 2 (1991), 129–134.

[20] Wagner, W. Über die grundlagen der projektiven geometrie und allgemeine zahlensysteme. *Mathematische Annalen 113*, 1 (1937), 528–567.

[21] Zhu, B. Graded primitive rings and kaplansky's theorem. *Beijing Shuifan Daxue Xuebao 34* (1998), 6–12.