O radical de Jacobson de anéis de polinômios diferenciais

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 28/08/2015. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Profª. Drª. Lucia Satie Ikemoto Murakami (orientadora) - IME-USP
- Prof. Dr. Ivan Shestakov - IME-USP
- Prof. Dr. Plamen Kochloukov - IMECC-UNICAMP

Agradecimentos

Gostaria de agradecer a Universidade de São Paulo e, em particular, ao Instituto de Matemática e Estatística da USP, por possibilitar o desenvolvimento deste trabalho.

Também gostaria de agradecer a CAPES e o CNPq, pelo financiamento durante o mestrado.

A comissão julgadora, por aceitar prontamente o convite. Em particular, gostaria de agradecer imensamente minha orientadora, Lucia Murakami, cujos conselhos têm me ensinado sobre matemática e sobre ser uma pessoa melhor. Também gostaria de agradecer ao professor Ivan Shestakov, pelas sugestões a este trabalho.

Aos meus pais, Marilete e Gilson, meus primeiros professores que me ensinaram as mais valiosas lições. Aos meus irmãos, Ana Paula e Felipe, por todo o carinho e todo o apoio, sobretudo nos tempos mais difíceis.

Aos meus amigos, por toda a paciência comigo. Em particular, Junior (obrigado por todo o apoio e pela força), Maria, André Porto, Carla, Éverton, Fabiana, Kaíque, Antônio, Bartira, Luciana, David, Ana Luiza, Danilo, Elias, Rebecca, Luiza, Mathias, Elisa, Felipe, Talita, Marcelo, Bruna, Cíntia, Ana Carolina, Anor, Gabi, aos colegas da pós-graduação, aos colegas do apartamento 304.

Resumo

SANTOS FILHO, G. R. **O radical de Jacobson de anéis de polinômios diferenciais**. 2015. 92 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2015.

O objetivo desta dissertação é estudar o radical de Jacobson de anéis de polinômios diferenciais. Mostramos um resultado de M. Ferrero, K. Kishimoro, K. Motose, que mostra que no caso geral, o radical de um anel de polinômios diferenciais é um anel de polinômios diferenciais sobre algum ideal do anel dos coeficientes. Assumindo que o anel dos coeficientes satisfaça uma identidade polinomial, mostramos seguindo B. Madill que este ideal é um ideal nil. Se o anel dos coeficientes é adicionalmente localmente nilpotente, seguindo J. Bell, B. Madill, F. Shinko, mostramos que o anel de polinômios diferenciais será localmente nilpotente. Ainda seguindo J. Bell et al, se o anel dos coeficientes é uma álgebra sobre um corpo de característica zero e tal álgebra satisfaz uma identidade polinomial, mostramos que o ideal nil é o radical de Köthe. Para tais demonstrações, cobriremos os tópicos preliminares necessários para entender os enunciados: radical nil, radical de Levitzki, radical de Baer, radical de Jacobson e propriedades, anéis PI, polinômios centrais, teorema de Kaplansky.

Palavras-chave: radical de Jacobson, anéis de polinômios diferenciais, anéis PI.

Abstract

SANTOS FILHO, G. R. **The Jacobson radical of differential polynomial rings**. 2015. 92 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2015.

The aim of this work is to study the Jacobson radical of differential polynomial rings. We show a result of M. Ferrero, K. Kishimoto, K. Motose, which shows that in general, the radical of a differential polynomial ring is a differential polynomial ring over some ideal of the ring of coefficients. Assuming that the ring of coefficients satisfies a polynomial identity, we show following B. Madill that this ideal is nil. If the ring of coefficients is additionally locally nilpotent, following J. Bell, B. Madill, F. Shinko, we show that the differential polynomial ring is locally nilpotent. Still following J. Bell et al, if the ring of coefficients is an algebra over a field of zero characteristic and this algebra satisfies a polynomial identity, we show that the nil ideal is the Köthe radical. For the proofs, we cover the preliminary topics necessary for understanding the statements: nil radical, Levitzki radical, Baer radical, Jacobson radical and its properties, PI-rings, central polynomials, Kaplansky's theorem.

Keywords: Jacobson radical, differential polynomial rings, PI-rings.

Introdução

O objetivo principal deste texto é demonstrar dois resultados devidos a J. Bell, B. Madill e F. Shinko sobre radicais de anéis de polinômios diferenciais [BMS15]. O primeiro mostra que se R é um anel localmente nilpotente que satisfaz uma identidade polinomial e δ é um derivação de R, então o anel de polinômios diferenciais $R[x;\delta]$ é localmente nilpotente (em outras palavras, $R[x;\delta]$ é radical segundo Levitzki). O segundo mostra que se R é uma álgebra com unidade sobre um corpo de característica zero que satisfaz uma identidade polinomial, δ é uma derivação de R e N é o maior ideal nil de R, então o anel de polinômios diferenciais $R[x;\delta]$ tem como radical de Jacobson o anel de polinômios diferenciais $N[x;\delta]$.

A estrutura do radical de Jacobson do anel de polinômios diferenciais $R[x;\delta]$ é um problema em aberto com algumas soluções parciais. Em 1956, S. A. Amitsur [Ami56] provou que o radical de Jacobson do anel de polinômios é um anel de polinômios com coeficientes em algum ideal nil. Em outras palavras, $\mathrm{rad}(R[x;\delta]) = N[x;\delta]$ onde δ é a derivação trivial e $N \subseteq R$ é um ideal nil. Posteriormente, em 1983, M. Ferrero, K. Kishimoto e K. Motose provaram que, para todo anel R, sempre existe um ideal N tal que $\mathrm{rad}(R[x;\delta]) = N[x;\delta]$ (Teorema 2.5.3) e, se adicionalmente R for comutativo, então N é nil. O problema de determinar se N é nil no caso geral permaneceu aberto até recentemente quando, em 2015, A. Smoktunowicz [Smo15] mostrou que existe um anel R não nil e uma derivação δ tal que $R[x;\delta]$ seja radical segundo Jacobson. Portanto, o problema tem resposta negativa.

Também houve tentativas bem sucedidas para provar o Teorema de Amitsur para anéis de polinômios diferenciais se forem satisfeitas certas condições sobre R ou δ. Em 1975, D. A. Jordan [Jor75] provou que, se R é um anel noetheriano com unidade, então existe um ideal nil $N \subseteq R$ tal que $\mathrm{rad}(R[x;\delta]) = N[x;\delta]$. Em 1987, J. Bergen, S. Montgomery e D. S. Passman [BMP87] estudaram o radical de Jacobson do produto cruzado de uma álgebra envelopante de uma álgebra de Lie: se L é um álgebra de Lie sobre um corpo k que age na k-álgebra associativa R, então podemos definir o produto cruzado $R * U(L)$, onde $U(L)$ é a álgebra envelopante universal de L (para mais detalhes sobre a álgebra $U(L)$, consultar [MR87, 7.10, p. 33]). A k-álgebra $R * U(L)$ é associativa e os autores provaram que $\mathrm{rad}(R * U(L)) = N * U(L)$, onde N é um ideal nil de R, no caso que R é noetheriano à direita ou no caso em que R é uma k-álgebra PI. No caso em que $L = k \cdot x$ é uma álgebra de Lie unidimensional, temos que $R * U(L) = R[x;\delta]$, onde $\delta(r) = [x, r]$ é a ação de $x \in L$ em $r \in R$. Segue, portanto, que o Teorema de Amitsur vale se uma das condições anteriores for satisfeita. Em 2015, A. Smoktunowicz provou que se R é uma álgebra sobre um corpo de característica positiva e δ é uma derivação fr R localmente nilpotente, ou seja, se para todo

$r \in R$ existir um inteiro positivo n tal que $\delta^n(r) = 0$, então vale o Teorema de Amitsur em $R[x;\delta]$.

Um problema relacionado ao anterior foi formulado por S. Montgomery e compilado no *Dniester's Notebook* [dni06, Problem 3.58]: Se R não possuir ideais nil não nulos, é verdade que $\mathrm{rad}(R[x;\delta]) = 0$? Se R e δ são tais que o Teorema de Amitsur vale para $R[x;\delta]$, então o problema de S. Montgomery tem resposta afirmativa. Em 2007, Y.T. Tsai, T.Y. Wu e C.L. Chuang [TWC07] provaram que o problema tem resposta afirmativa em alguns casos particulares, dentre eles quando R é um anel PI ou quando R satisfaz a condição de cadeia ascendente sobre os anuladores à direita de seus subconjuntos unitários. Recentemente, outras condições suficientes foram provadas em [BG12] e [NI14].

Ainda sobre a estrutura do radical de Jacobson de $R[x;\delta]$ em casos particulares, temos o seguinte problema proposto em 2011 por I. P. Shestakov na conferência *"Non-Associative Algebras and Related Topics"*, em Coimbra: Se R é um anel localmente nilpotente e δ é uma derivação, é verdade que o anel $R[x;\delta]$ é radical segundo Jacobson? Em 2014, A. Smoktunowicz e M. Ziembowski [SZ14] mostraram que, para todo corpo k, existe uma k-álgebra localmente nilpotente R e uma derivação δ tais que $R[x;\delta]$ não é radical segundo Jacobson. Por sua vez, os autores perguntaram se o problema tem resposta afirmativa com a hipótese adicional de que R satisfaz alguma identidade polinomial. Ainda em 2014, J. P. Bell, B. W. Madill e F. Shinko provaram que o anel $R[x;\delta]$ é localmente nilpotente se R é um anel PI, conforme demonstraremos no Capítulo 4 deste texto.

O segundo resultado de [BMS15] que aqui demonstraremos, mostra que se R é uma álgebra PI com unidade sobre um corpo de característica zero, então $\mathrm{rad}(R[x;\delta]) = N[x;\delta]$, onde N é o maior ideal nil de R (ou seja, N é igual ao radical de Köthe de R). Também mostraremos um exemplo onde R é uma álgebra comutativa com unidade sobre um corpo de característica positiva e tal que N não é nil.

No Capítulo 1 são introduzidas algumas notações e convenções usadas. No Capítulo 2, nosso principal objetivo é apresentar os radicais nil, de Levitzki, primo e de Jacobson. Os três primeiros são temas da Seção 2.1 enquanto o último será introduzido no caso de anéis com unidade na Seção 2.2 e no caso geral na Seção 2.4. A teoria do radical de Jacobson é extensa, como pode ser conferido em [Lam01], e existem muitos teoremas sobre a sua descrição em classes específicas de anéis. Para demonstrar o resultado de M. Ferrero, K. Kishimoto e K. Motose sobre o radical de Jacobson em anéis de polinômios diferenciais, abordamos na Seção 2.3 resultados sobre o radical de Jacobson de extensões de escalares. A Seção 2.4 introduz a definição do radical de Jacobson para anéis arbitrários e na Seção 2.5 demonstramos o resultado de Ferrero et al. Por fim, iremos explorar na Seção 2.6 algumas das propriedades comuns entre os radicais aqui definidos.

O Capítulo 3 é dedicado à demonstração de resultados envolvendo anéis que satisfazem identidades polinomiais. Os resultados aqui expostos são os necessários para demonstrar que os ideais não nulos de um anel PI semiprimo têm intersecção não nula com o centro. Depois da pequena introdução feita na Seção 3.1, provamos na Seção 3.2 a existência de polinômios centrais em anéis de matrizes sobre corpos. A seguir, na Seção 3.3, provaremos o Teorema de Kaplansky, que afirma que qualquer anel primitivo à esquerda que satisfaz uma identidade

polinomial é isomorfo a um anel de matrizes com entradas em uma álgebra de divisão central de dimensão finita. Os resultados das três seções anteriores serão usados na Seção 3.4 para estudar anéis semiprimos e primos que satisfazem identidades polinomiais.

No Capítulo 4 nos concentramos em estudar o radical de Jacobson de anéis de polinômios diferenciais em casos particulares. Se R é um anel, então o radical de $R[x;\delta]$ é $N[x;\delta]$, onde N é um ideal de R. A Seção 4.1 mostra que se R satisfaz uma identidade polinomial, então N é nil. O caso em que R é adicionalmente semiprimo foi provado por Y.T. Tsai, T.Y. Wu e C.L. Chuang em [TWC07], baseado em um resultado de C.L. Chuang e T.K. Lee [CL06], que por sua vez utiliza técnicas da teoria de quocientes de Martindale. No entanto, iremos expor neste texto uma demonstração devida a B. Madill [Mad14], que o provou usando o resultado de M. Ferrero et al, além, é claro, de elementos da teoria de anéis PI. No resto do capítulo, abordamos a demonstração dos dois resultados de J. Bell et al. A Seção 4.2 começa com uma abordagem ingênua à demonstração de que $R[x;\delta]$ é localmente nilpotente se R for um anel PI localmente nilpotente (Teorema 4.4.1) e concluímos com a sugestão que é possível uma abordagem combinatória, de forma a tirar proveito da identidade polinomial satisfeita por R. Na Seção 4.3 expomos definições e provamos um lema sobre combinatória em palavras que, por sua vez, é usado na Seção 4.4 para concluir a demonstração do Teorema 4.4.1. Por fim, ainda na seção 4.4, aplicaremos este resultado para provar que se R é uma álgebra PI com unidade sobre um corpo de característica zero, então $\mathrm{rad}(R[x;\delta]) = N[x;\delta]$, onde N é o maior ideal nil de R.

Sumário

Capítulo 1

Preliminares

Neste texto, consideramos anéis associativos e possivelmente sem unidade. Em todo o texto entendemos o termo *módulo* como um módulo sobre um anel com unidade e unital. Se R é um anel com unidade e M é um grupo abeliano, então escrevemos ${}_RM$ (respectivamente, M_R) para indicar que M é um R-módulo à esquerda (respectivamente, à direita). por consequência, consideramos neste texto que uma álgebra sobre um anel comutativo com unidade é unital, embora a própria álgebra não necessariamente tenha unidade.

Usamos as notações padrões $\mathfrak{A} \lhd_e R$, $\mathfrak{A} \lhd_d R$ e $\mathfrak{A} \lhd R$ para indicar que $\mathfrak{A}$ é um ideal à esquerda, à direita e bilateral do anel R, respectivamente. Também usamos o termo *ideal unilateral* para indicar um ideal à esquerda ou à direita. Dizemos que um anel R é *simples* se $R^2 \neq 0$ e seus únicos ideais são 0 e R.

Se S é um subconjunto do anel R, denotamos o ideal gerado por S como $\mathrm{id}\langle S\rangle$. Se S é unitário, digamos, $S = \{a\}$, denotamos o ideal gerado por $\mathrm{id}\langle a\rangle$. De maneira geral, temos a seguinte expressão para $\mathrm{id}\langle a\rangle$:

$$\mathrm{id}\langle a\rangle = RaR + Ra + aR + \mathbb{Z}a = \{r_1ar_2 + s_1a + as_2 + na \mid r_1, r_2, s_1, s_2 \in R, n \in \mathbb{Z}\}.$$

Se R possui unidade, obtemos a forma simplificada $\mathrm{id}\langle a\rangle = RaR$.

Consideramos conhecidas as noções de homomorfismo, endomorfismo, isomorfismo, etc. Nas seções onde consideramos que os anéis possuem unidade, assumimos a convenção que os homomorfismos de anéis preservam a unidade.

Se $T \neq \emptyset$ é um conjunto de indeterminadas e R é um anel, então assumimos conhecidas as definições e propriedades de um polinômio nas indeterminadas T com coeficientes no anel R. Denotamos o anel formado por estes polinômios por $R[T]$. Lembramos que, neste caso, as indeterminadas do subconjunto $T \subseteq R[T]$ comutam entre si e com os elementos de R. No caso em que $T = \{t_1, \ldots, t_n\}$ é finito, denotamos o anel de polinômios sobre T por $R[t_1, \ldots, t_n]$.

Definição 1.0.1. Se R é um anel e $\sigma : R \to R$ é um homomorfismo de R, então uma *σ-derivação* de R é uma função $\delta : R \to R$ que satisfaz, para quaisquer $a, b \in R$:

(1) $\delta(a + b) = \delta(a) + \delta(b)$;

(2) $\delta(ab) = \delta(a)b + \sigma(a)\delta(b)$.

No caso em que σ é a função identidade, dizemos simplesmente que δ é uma *derivação* de R.

Definição 1.0.2. Se R é um anel, $\sigma : R \to R$ é um homomorfismo, δ é uma σ-derivação em R e x é uma variável independente, então o conjunto dos polinômios sobre x com coeficientes em R é um anel quando munido da soma usual de polinômios e da multiplicação dada pela regra

$$xa = \sigma(a)x + \delta(a), \text{ para todo } a \in R$$

Dizemos este anel é uma *Extensão de Ore* de R e o denotamos por $R[x; \sigma; \delta]$[1].

Damos nomes especiais aos seguintes casos particulares de Extensões de Ore:

- Se δ é uma derivação em R e $\sigma : R \to R$ é a função identidade, então δ é uma σ-derivação em R. Nesse caso, usamos a notação $R[x; \delta]$ ao invés de $R[x; \sigma; \delta]$ e chamamos esse anel de *anel de polinômios diferenciais*.
- Se σ é um endomorfismo de R e $\delta : R \to R$ é a função nula, então δ é uma σ-derivação em R. Nesse caso, usamos a notação $R[x; \sigma]$ ao invés de $R[x; \sigma; \delta]$ e chamamos esse anel de *anel de polinômios skew*.

Se n é um inteiro positivo e $a \in R$, então é válida em $R[x; \delta]$ a seguinte fórmula:

$$x^n a = \sum_{t=0}^{n} \delta^t(a) x^{n-t}, \tag{1.0.3}$$

onde δ^t denota a composição da função δ t-vezes e $\binom{n}{t}$ é o número binomial. De maneira geral, se $r \in \mathbb{R}$ é não negativo e t é um inteiro positivo, então definimos:

$$\binom{r}{t} = \frac{r(r-1)(r-2)\dots(r-t+1)}{t!}$$

Se R é um anel com unidade e n é um inteiro positivo, então denotamos o anel das matrizes $n \times n$ com entradas em R como $M_n(R)$. Lembremos que, como R é um anel com unidade, fixado o inteiro positivo n, para todos $r, s = 1, \dots, n$, podemos considerar a *matriz elementar* $E_{rs} = (a_{ij}) \in M_n(R)$, que é dada por

$$a_{ij} = \begin{cases} 1, & \text{se } i = r \text{ e } j = s; \\ 0, & \text{caso contrário.} \end{cases}$$

[1] A verificação de que a regra dada define uma única multiplicação associativa pode ser conferida em [GW04b, p. 43-38]

Lembremos também que as matrizes elementares satisfazem a relação $E_{ri}E_{js} = \delta_{ij}E_{rs}$, para todos $i, j, r, s = 1, \ldots, n$, onde δ_{ij} é o delta de Kronecker, dado por

$$\delta_{ij} = \begin{cases} 1, & \text{se } i = j; \\ 0, & \text{caso contrário.} \end{cases}$$

Sejam k um anel, $n \geq 2$ um inteiro e $p(t) = t^n + a_{n-1}t^{n-1} \cdots + a_1 t + a_0 \in k[t]$ um polinômio mônico. A *matriz companheira* do polinômio $p(t)$ é a matriz

$$C_{p(t)} = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

A matriz $C_{p(t)}$ tem tanto o polinômio característico quanto o polinômio minimal iguais a $p(t)$. Em particular, se $p(t)$ tiver n raízes distintas, então a matriz $C_{p(t)}$ é diagonalizável.

Se R é um anel e $X \subseteq R$ um conjunto qualquer, então definimos o *centro* de X como o conjunto $Z(X) = \{r \in R \mid rx = xr, \text{ para todo } x \in X\}$.

Fixe, para o resto desta seção, um anel com unidade R.

Seja M um R-módulo à esquerda (respectivamente, à direita). Dizemos que M é *fiel* se a ação de R for injetora, ou seja, se para todo $r \in R$ e quaisquer $m_1, m_2 \in M$

$$rm_1 = rm_2 \Rightarrow m_1 = m_2 \qquad (\text{resp., } m_1 r = m_2 r \Rightarrow m_1 = m_2).$$

Sejam M um R-módulo à esquerda e $S \subset M$ um conjunto arbitrário. O *anulador* de S é $\text{Ann}_\ell(S) = \{r \in R \mid rS = 0\}$. Analogamente, se N é um R-módulo à direita e $S' \subset N$ é arbitrário, o *anulador* de S' é $\text{Ann}_r(S') = \{r \in R \mid S'r = 0\}$. Embora existam casos em que um mesmo conjunto tenha estrutura de módulo sobre mais de um anel, usamos a mesma notação para o anulador, explicitando sempre qual estrutura de módulo considerar.

Um R-módulo (à esquerda ou à direita) $M \neq 0$ é dito *simples* se 0 e M são seus únicos submódulos. Dizemos que M é *semissimples* ou *completamente redutível* se, para todo submódulo $N \subseteq M$, existe um submódulo $N' \subseteq M$ tal que $M = N \oplus N'$. Existem várias definições equivalentes para semissimplicidade, como pode ser consultado em [Lam01, p. 25-29]. A nós, é interessante a seguinte equivalência, cuja demonstração é omitida, mas pode ser encontrada na referência anterior:

Proposição 1.0.4. *Para um R-módulo ${}_RM$, são equivalentes as seguintes propriedades:*

1. *M é semissimples.*
2. *M é a soma direta de uma família de submódulos simples.*

3. M é a soma de uma família de submódulos simples.

Segue da proposição acima a fácil consequência:

Corolário 1.0.5. *Se R é um anel com unidade e ${}_RM$ e ${}_RN$ são R-módulos semissimples, então o R-módulo ${}_R(M \oplus N)$ é semissimples.*

Assumimos conhecida a definição do produto tensorial de álgebras sobre corpos. Definições e propriedades podem ser conferidas em [Rom08, Chapter 14]. Explicitamos, no entanto, as seguintes propriedades básicas:

Proposição 1.0.6. *[Rom08, p. 361-364] Se k é um corpo e V, W são espaços vetoriais sobre k com bases $\mathcal{B}, \mathcal{B}'$, respectivamente, então o conjunto $\{v \otimes w \mid v \in \mathcal{B}, w \in \mathcal{B}'\}$ é uma base do k-espaço vetorial $V \otimes_K W$.*

É consequência da Proposição 1.0.6 que, se V e W são k-espaços vetoriais de dimensão finita, então

$$\dim_k(V \otimes_k W) = (\dim_k V)(\dim_k W).$$

Além disso, segue que:

Proposição 1.0.7. *Sejam k um corpo e V, W espaços vetoriais sobre k. Para todo elemento $v \in V \otimes_k W$, existe um inteiro positivo n e únicos $a_1, \ldots, a_n \in V$ e $b_1, \ldots, b_n \in W$, tais que $\{b_1, \ldots, b_n\}$ é um subconjunto de W linearmente independente e*

$$v = \sum_{i=1}^{n} a_i \otimes b_i.$$

Sejam k e $K \supseteq k$ corpos e V um k-espaço vetorial. Chamamos o produto tensorial $V \otimes_k K$ de *extensão de escalares* de V e $V \otimes_k K$ tem estrutura de K-espaço vetorial dado pela seguinte regra:

$$\alpha \cdot (v \otimes \beta) = v \otimes \alpha\beta, \ \forall \alpha, \beta \in K, \ \forall v \in V$$

Temos as seguintes proposições:

Proposição 1.0.8. *[Rom08, p. 379] Sejam V um espaço vetorial sobre o corpo k, $\{v_i \mid i \in I\}$ uma base de V e $K \supseteq k$ um corpo. Então $\{v_i \otimes 1 \mid i \in I\}$ é base do K-espaço vetorial $(K \otimes_k V)$ e, em particular,*

$$\dim_K(K \otimes_k V) = \dim_k V$$

Proposição 1.0.9. *Sejam D um anel de divisão, $k \subseteq D$ o centro de D e K um corpo tal que $k \subseteq K \subseteq D$. Segue que D é um k-espaço vetorial e para todo inteiro positivo n,*

$$M_n(D) \otimes_k K \simeq M_n(D \otimes_k K)$$

como K-álgebras.

Capítulo 2

Radicais

A noção de radical foi desenvolvida inicialmente no estudo de algumas classes de álgebras não-associativas. Nos seus trabalhos, E. Cartan introduziu os conceitos de álgebra de Lie semissimples e radical de uma álgebra de Lie: uma álgebra de Lie de dimensão finita é chamada de semissimples em função da sua forma de Killing, enquanto que o (hoje conhecido como) radical de uma álgebra de Lie de dimensão finita é definido como a soma de seus ideais solúveis. Em seguida, mostrou que uma álgebra de Lie é semissimples se, e somente se, o seu radical é nulo, e que uma álgebra de Lie é semissimples se, e somente se, é uma soma direta de álgebras de Lie simples. Adicionalmente, E. Cartan classificou as álgebras de Lie simples sobre $\mathbb{C}$ e sobre $\mathbb{R}$.

Em 1893, T. Molien, na sua tese de doutorado *"Über Systeme höherer komplexer Zahlen"*, provou que uma álgebra associativa, com unidade e simples sobre $\mathbb{C}$ é isomorfa a uma álgebra de matrizes (de ordem conveniente) com entradas em $\mathbb{C}$. Posteriormente, em 1898, E. Cartan provou o mesmo resultado de maneira independente e adicionalmente provou que toda $\mathbb{C}$-álgebra de dimensão finita é a soma direta de um ideal nilpotente e uma soma direta de ideais simples.

Os resultados sobre álgebras associativas semissimples são casos particulares de um resultado devido a J. Wedderburn – a primeira tentativa de desenvolver uma teoria geral sobre a estrutura de álgebras de dimensão finita sobre corpos arbitrários [vdW85, p. 210]. J. Wedderburn mostrou que se A é uma álgebra associativa, com unidade e de dimensão finita sobre um corpo k, então existe um ideal N nilpotente que contém todas os ideais nilpotentes de A – em particular, N é o ideal nilpotente maximal de A. Se $N = 0$ então a álgebra A é chamada de semissimples. Na nomenclatura atual, o ideal N é chamado de *radical* de A. Com essas convenções, podemos enunciar o Teorema de Wedderburn, provado em 1907 em seu artigo *"On hypercomplex numbers"*.

Teorema 2.0.1 (Teorema Principal de Wedderburn)**.** *(1) Toda álgebra de dimensão finita é a soma direta (de espaços vetoriais) de seu radical e uma subálgebra semissimples;*

(2) Toda álgebra semissimples é soma direta de ideais simples únicos a menos de ordem e isomorfismos;

(3) Toda álgebra simples é isomorfa a uma álgebra de matrizes sobre um anel de divisão.

Em 1927, E. Artin provou que, assim como no caso de álgebras de dimensão finita, também existe em um anel artiniano à esquerda um ideal nilpotente maximal N, também chamado de radical. Além disso, E. Artin define como semissimples um anel artiniano à esquerda que tem radical nulo e mostrou os itens (2) e (3) do Teorema Principal de Wedderburn para anéis semissimples e simples, respectivamente.

Tentativas de desenvolvimento dos resultados de J. Wedderburn e E. Artin para classes maiores de anéis se deram nas duas décadas seguintes por diversas abordagens. Um dos problemas era estender a definição do radical para anéis arbitrários ou, ao menos, uma classe maior de anéis. Em 1930, G. Köthe usou pela primeira vez o termo "radical": Se A é um anel, G. Köthe chamou de ideal nil aqueles ideais cujos elementos são nilpotentes e definiu o radical R do anel A como a soma de todos os ideais nil. No seguinte trecho adaptado de [vdW85, p. 211], o matemático B. L. van der Waerden – aluno de E. Noether em Göttingen – descreve este período:

> Dentre os que seguiam a linha de pesquisa de Emmy Noether, havia a sensação de que o radical R [de um anel A], como definido por Wedderburn ou por Köthe, é muito pequeno. Se a condição de cadeia descendente não for satisfeita, não é possível obter teoremas de estrutura satisfatórios para [o anel quociente] A/R. Assim, Reinhold Baer e Jakob Levitzki propuseram outras definições para o radical. (...) Estas definições, no entanto, ainda não permitiam o desenvolvimento de uma teoria de estrutura de anéis satisfatória sem [que fossem consideradas] condições de finitude. O primeiro a resolver esse problema e apresentar uma bela teoria geral foi Nathan Jacobson. [1]

As definições de radical sugeridas por G. Köthe, R. Baer, J. Levitzki e N. Jacobson podem ser interpretadas como definições alternativas para o radical de Wedderburn pois, como será provado na Seção 2.6, elas determinam um mesmo ideal no caso de anéis artinianos à esquerda (e em particular, em álgebras de dimensão finita). No entanto, quando considerados para anéis arbitrários, estes radicais são, em geral, distintos. De qualquer forma, todos são úteis para o estudo da estrutura de anéis e o objetivo das próximas seções será estudar alguns elementos da teoria de cada um deles.

2.1 O radical segundo Köthe, Levitzki e Baer

Nesta seção iremos introduzir e discutir brevemente os radicais sugeridos por G. Köthe, J. Levitzki e R. Baer e relações entre eles.

[1] In the school of Emmy Noether it was felt that the radical R, as defined by Wedderburn or by Köthe, is too small. If the descending chain condition is not satisfied, it was not possible to obtain satisfactory structure theorems for A/R. Therefore, Reinhold Baer and Jakob Levitzki have proposed other definitions of the radical. (...) However, these definitions still did not lead to a satisfactory structure theory of rings without finiteness conditions. The first to solve the riddle and to present a beautiful general theory was Nathan Jacobson.

2.1.1 O radical nil

Se R é um anel, dizemos que um elemento $a \in R$ é dito *nilpotente* se existe um inteiro positivo n tal que $a^n = 0$. Um subconjunto $S \subseteq R$ é dito *nil* se todo elemento de S é nilpotente. O subconjunto $S \subseteq R$ é chamado de *nilpotente* se existe um inteiro positivo n tal que $S^n = 0$, ou seja, se $x_1 \dots x_n = 0$ para quaisquer $x_1, \dots, x_n \in S$.

Antes da definição do radical nil, é necessário provar a seguinte proposição:

Proposição 2.1.1. *Se R é um anel e $\mathfrak{A}, \mathfrak{B}$ são ideais nil de R, então $\mathfrak{A} + \mathfrak{B}$ é um ideal nil de R.*

Demonstração. Assuma que $\mathfrak{A}, \mathfrak{B}$ são ideais nil de R e observe que $\mathfrak{A}/(\mathfrak{A} \cap \mathfrak{B}) \lhd R/(\mathfrak{A} \cap \mathfrak{B})$ é nil. Como $(\mathfrak{A} + \mathfrak{B})/\mathfrak{B} \simeq \mathfrak{A}/(\mathfrak{A} \cap \mathfrak{B})$, segue que $(\mathfrak{A} + \mathfrak{B})/\mathfrak{B}$ também é um ideal nil de $R/\mathfrak{B}$. Daí, para qualquer $x \in \mathfrak{A} + \mathfrak{B}$, existe um inteiro positivo n tal que $x^n + \mathfrak{B} = 0 + \mathfrak{B}$, ou seja, $x^n \in \mathfrak{B}$. Mas, como $\mathfrak{B}$ é um ideal nil, segue que existe um inteiro positivo m tal que $(x^n)^m = x^{mn} = 0$, donde segue que $\mathfrak{A} + \mathfrak{B}$ é um ideal nil, provando a afirmação. □

Usando indução, a Proposição 2.1.1 nos permite concluir que a soma finita de ideais nil também é um ideal nil. Por consequência, segue que a soma dos ideais nil de R é um ideal nil. De fato, se A_i, com $i \in I$, são os ideais nil de R, e x é um elemento arbitrário de $\sum_{i \in I} A_i$, então existem $i_1, \dots, i_n \in I$ tais que $x \in A_{i_1} + \cdots + A_{i_n}$, e daí, segue que x é nilpotente. Podemos concluir que, se R é um anel, então a soma dos ideais nil de R é o seu maior ideal nil. Chamamos esse ideal nil maximal de *radical nil* e o denotamos por $\operatorname{Nil} R$. A definição de $\operatorname{Nil} R$ e o termo "radical" foram usados no contexto de teoria de anéis pela primeira vez em [Köt30], por G. Köthe. Por essa razão, $\operatorname{Nil} R$ é frequentemente chamado de *radical de Köthe*.

Um problema clássico ainda em aberto da teoria de anéis é a validade da seguinte versão mais forte da Proposição 2.1.1:

Problema 2.1.2. Se R é um anel e $\mathfrak{A}, \mathfrak{B} \subseteq R$ são ideais à esquerda nil, então $\mathfrak{A} + \mathfrak{B}$ é nil?

Tal conjectura é conhecida como *Conjectura de Köthe* e sua resposta implica na resolução de outros problemas na teoria de anéis (para mais detalhes, ver [Kre72]). Essa conjectura tem outras formulações equivalentes, como pode ser visto na proposição seguinte. A demonstração das equivalências será omitida, mas pode ser conferida em [Lam01].

Proposição 2.1.3. *São equivalentes as seguintes afirmações:*

(1) *(Köthe) Em todo anel, a soma de dois ideais à esquerda nil é nil;*

(2) *Todo ideal unilateral nil está contido em* $\operatorname{Nil} R$*, para todo anel R;*

(3) *Para todo anel R, se $I \lhd R$ é um ideal nil, então $M_n(I) \subseteq M_n(R)$ é nil, para todo inteiro positivo n;*

(4) *Para todo anel R, se $I \lhd R$ é um ideal nil, então $M_2(I) \subseteq M_2(R)$ é nil;*

(5) *Para todo anel R e para todo inteiro positivo n,* $\operatorname{Nil}(M_n(R)) = M_n(\operatorname{Nil} R)$*;*

2.1.2 O radical de Levitzki

Se R é um anel, então um subconjunto $S \subseteq R$ é chamado de *localmente nilpotente* se, para todo subconjunto $S' \subseteq S$ finito, o anel gerado por S' é nilpotente.

Se a conjectura de Köthe for verdadeira, então, para todo anel R e quaisquer $\mathfrak{A} \lhd_d R, \mathfrak{B} \lhd_e R$ nil, os conjuntos $\mathfrak{A} + \mathfrak{B}$, $R\mathfrak{A}R$, $R\mathfrak{B}R$ estarão contidos em $\operatorname{Nil} R$ e, portanto, serão todos conjuntos nil. A proposição a seguir mostra que a versão "localmente nilpotente" da afirmação anterior é verdadeira.

Proposição 2.1.4. *Se R é um anel e $\mathfrak{A}, \mathfrak{B}$ são ideais unilaterais localmente nilpotentes, então os conjuntos $\mathfrak{A} + \mathfrak{B}$, $R\mathfrak{A}R$, $R\mathfrak{B}R$ são todos localmente nilpotentes.*

Demonstração. Suponha que $\mathfrak{A} \subseteq R$ seja um ideal à esquerda localmente nilpotente. Vamos provar que o ideal $\mathfrak{A}R$ é localmente nilpotente e, como $R\mathfrak{A}R \subseteq \mathfrak{A}R$, isto é suficiente para concluir que $R\mathfrak{A}R$ é localmente nilpotente. Tome um conjunto finito $X = \{x_i \mid i \in I\} \subseteq \mathfrak{A}R$. Podemos assumir que existe um inteiro positivo m e elementos $r_j \in R$, com $j \in J$ e J finito, tais que $X \subseteq \sum_{j\in J} \mathfrak{A}r_j$. Em particular, existe $\{a_{ij} \in \mathfrak{A} \mid (i,j) \in I \times J\}$ tal que, para todo $i \in I$,

$$x_i = \sum\nolimits_{j\in J} a_{ij} r_j.$$

Daí, temos que $A = \{r_j a_{pq} \mid j \in J, (p,q) \in I \times J\} \subseteq \mathfrak{A}$ e, como o primeiro conjunto é finito e o último é localmente nilpotente, existe um inteiro positivo N tal que $A^N = 0$. É fácil ver que qualquer produto de $N+1$ elementos de X é uma soma de parcelas do tipo

$$(a_{i_1 j_1} r_{j_1})(a_{i_2 j_2} r_{j_2}) \dots (a_{i_N j_N} r_{j_N})(a_{i_{N+1} j_{N+1}} r_{j_{N+1}}).$$

Por outro lado, como $A^N = 0$, temos que

$$(r_{j_1} a_{i_2 j_2})(r_{j_2} \dots a_{i_N j_N})(r_{j_N} a_{i_{N+1} j_{N+1}}) = 0$$

e, portanto, segue que qualquer produto de $N+1$ elementos de X é igual a zero. Segue que X é nilpotente e que o anel gerado por X também é. Conclui-se que $\mathfrak{A}R$ é localmente nilpotente. Um argumento análogo também mostra os demais casos da proposição. □

A Proposição 2.1.4 nos permite concluir que a soma dos ideais localmente nilpotentes de um anel é o maior ideal localmente nilpotente deste anel. Definimos o *radical de Levitzki* de um anel R como a soma de seus ideais localmente nilpotentes e o denotamos por $\ell\text{-rad}\, R$. Esta definição se deve a J. Levitzki e foi publicada pela primeira vez em [Lev43].

Todo ideal localmente nilpotente é nil, uma vez que qualquer subconjunto unitário é nilpotente. Segue que $\ell\text{-rad}\, R$ é um ideal nil do anel R e, portanto,

$$\ell\text{-rad} \subseteq \operatorname{Nil} R. \tag{2.1.5}$$

Em geral, essa inclusão é estrita: Em 1966, E. S. Golod mostrou que, para qualquer corpo k, existe uma k-álgebra R nil que não é localmente nilpotente. Para mais detalhes, consultar [Row88, Theorem 6.2.9].

2.1.3 O radical primo

Um anel R é chamado de *anel primo* se, para quaisquer ideais $\mathfrak{A}, \mathfrak{B} \subseteq R$ tais que $\mathfrak{AB} = 0$, temos que $\mathfrak{A} = 0$ ou $\mathfrak{B} = 0$. Um anel R é chamado de *anel semiprimo* se, para qualquer ideal $\mathfrak{A} \subseteq R$ tal que $\mathfrak{A}^2 = 0$, temos que $\mathfrak{A} = 0$. Podemos substituir em ambas as definições o termo "ideais" por "ideais à esquerda" (respectivamente, à direita). De fato, se $\mathfrak{A}, \mathfrak{B}$ são ideais à esquerda do anel primo R tais que $\mathfrak{AB} = 0$, então $\mathfrak{A}R + \mathfrak{A}, \mathfrak{B}R + \mathfrak{B}$ são ideais de R tais que

$$(\mathfrak{A}R + \mathfrak{A})(\mathfrak{B}R + \mathfrak{B}) \subseteq \mathfrak{AB}R + \mathfrak{AB} \subseteq 0$$

e, como R é primo, segue que $\mathfrak{A}R + \mathfrak{A} = 0$ ou $\mathfrak{B}R + \mathfrak{B} = 0$, donde temos que $\mathfrak{A} = 0$ ou $\mathfrak{B} = 0$. Como a recíproca é claramente verdadeira, segue a afirmação. O caso em que R é semiprimo é tratado de maneira análoga. Vamos agora construir o radical primo.

Se R é um anel, então defina $N_0(R) = 0$ e, para todo ordinal α, defina recursivamente o ideal $N_\alpha(R)$ da seguinte forma:

> *Caso 1:* α não é um ordinal limite. Se β é o ordinal tal que $\beta + 1 = \alpha$, defina $N_\alpha(R) = \sum\{\mathfrak{A} \lhd R \mid \mathfrak{A}^2 \subseteq N_\beta(R)\}$.
>
> *Caso 2:* α é um ordinal limite. Defina $N_\alpha = \bigcup_{\beta<\alpha} N_\beta(R)$.

Os ideais $N_\alpha(R)$ assim definidos formam uma sequência crescente (sob a inclusão) e $N_{\alpha+1}(R)/N_\alpha(R) = N_1(R/N_\alpha(R))$, para todo ordinal α. De fato, se α é um ordinal então $N_\alpha(R)^2 \subseteq N_\alpha(R)$ e, portanto, $N_\alpha(R) \subseteq N_{\alpha+1}(R)$; para todo ordinal α e para todo ideal $\mathfrak{A} \subseteq R$ contendo $N_\alpha(R)$, $(\mathfrak{A}/N_\alpha(R))^2 = 0$ se, e somente se, $\mathfrak{A}^2 \subseteq N_\alpha(R)$ e daí é fácil ver que segue o afirmado. Além disso, se existir um ordinal γ tal que $N_\gamma(R) = N_{\gamma+1}(R)$, segue que $R/N_\gamma(R)$ é semiprimo; se R for semiprimo, então para todo ordinal α, $N_\alpha(R) = 0$.

Seja κ um cardinal infinito maior do que a cardinalidade de R. Considere a sequência $(N_\alpha(R))_{\alpha\leq\kappa}$ e suponha que ela seja estritamente crescente. Segue que, para todo $\alpha < \kappa$, o conjunto $S_{\alpha+1} = N_{\alpha+1}(R) \setminus N_\alpha(R)$ é não vazio. Pelo axioma da escolha, existe uma função $f : \kappa \to R$ que associa a cada ordinal $\alpha < \kappa$ um elemento $f(\alpha) \in S_\alpha$ e que $f(0) = 0$. Essa função f é injetora, uma vez que os conjuntos $(S_\alpha)_{\alpha<\kappa}$ são disjuntos dois a dois e, portanto, $\kappa \geq card(R)$, um absurdo.

É fácil ver que os dois parágrafos anteriores mostram que a sequência dos ideais $N_\alpha(R)$ estabiliza. Definimos o *radical primo*, também conhecido como *radical de Baer* ou *nilradical inferior*, como $\operatorname{nil} R = \bigcup_\alpha N_\alpha(R) = N_\gamma(R)$, onde γ é um ordinal tal que $N_\gamma(R) = N_{\gamma+1}(R)$. Dizemos que um ideal $\mathfrak{A}$ do anel R é um *ideal primo* (respectivamente, *ideal semiprimo*) se $R/\mathfrak{A}$ for um anel primo (respectivamente, anel semiprimo). O leitor familiarizado com álgebra comutativa pode facilmente observar que estas definições são compatíveis com os conceitos de ideais primos e semiprimos daquele contexto.

Proposição 2.1.6. *Se R é um anel, então* $\operatorname{nil} R$ *é seu menor ideal semiprimo.*

Demonstração. Fixando o ideal $\mathfrak{p} = \bigcap\{\mathfrak{A} \lhd R \mid \mathfrak{A} \text{ é semiprimo}\}$ temos que $\mathfrak{p}$ é um ideal semiprimo. De fato, se $\mathfrak{A} \subseteq R$ é um ideal que contém $\mathfrak{p}$ e é tal que $\mathfrak{A}^2 \subseteq \mathfrak{p}$, então $\mathfrak{A}^2$ está

contido em todo ideal semiprimo de R e, portanto, $\mathfrak{A}$ está contido em todo ideal semiprimo de R, donde temos que $\mathfrak{A} \subseteq \mathfrak{p}$. Concluímos que $\mathfrak{p}$ é o menor ideal semiprimo de R e resta provar que $\mathfrak{p} = \operatorname{nil} R$.

Como provamos que $R/\operatorname{nil} R$ é semiprimo, temos que $\mathfrak{p} \subseteq \operatorname{nil} R$. Para provar a inclusão inversa, suponha por absurdo que $\operatorname{nil} R \nsubseteq \mathfrak{p}$. Segue que existe um ordinal mínimo γ tal que $N_\gamma(R) \nsubseteq \mathfrak{p}$. Como $N_0(R) \subseteq \mathfrak{p}$, γ é um ordinal limite ou é um ordinal sucessor. Pela minimalidade de γ, $N_\alpha(R) \subseteq \mathfrak{p}$ para todo ordinal $\alpha < \gamma$ e, se γ fosse ordinal limite, então

$$N_\gamma(R) = \bigcup_{\alpha<\gamma} N_\alpha(R) \subseteq \mathfrak{p}.$$

Por outro lado, suponha que exista um ordinal β tal que $\beta + 1 = \gamma$. Como

$$N_\gamma(R) = \sum \{\mathfrak{A} \lhd R \mid \mathfrak{A}^2 \subseteq N_\beta(R)\} \nsubseteq \mathfrak{p},$$

existe um ideal $\mathfrak{A}$ tal que $\mathfrak{A}^2 \subseteq N_\beta(R) \subseteq \mathfrak{p}$ e $\mathfrak{A} \nsubseteq \mathfrak{p}$, um absurdo, visto que $\mathfrak{p}$ é semiprimo. Segue que $\operatorname{nil} R = \mathfrak{p}$. □

Nosso objetivo agora é provar que o radical primo é a intersecção dos ideais primos. Para isso, precisamos de algumas convenções e de dois lemas.

Se R é um anel e $M = (m_1, m_2, \dots)$ é uma sequência de elementos, então dizemos que M é uma *m-sequência* se, para todo $i \geq 1$, $m_{i+1} \in (\mathrm{id}\langle m_i \rangle)^2$. Dizemos que a m-sequência M é infinita (respectivamente, finita) se o conjunto dos seus elementos não nulos for infinito (respectivamente, finito). Por abuso de linguagem, identificaremos a sequência M e o conjunto dos termos de M. Assim, M é infinita se, e somente, $0 \notin M$.

Lema 2.1.7. *Se $\mathfrak{A}$ é um ideal semiprimo do anel R e $a \in R \backslash \mathfrak{A}$, então existe uma m-sequência infinita M tal que $M \cap \mathfrak{A} = \emptyset$.*

Demonstração. Definiremos uma sequência $(a_1, a_2, \dots)$ recursivamente da seguinte forma: faça $a_1 = a$ e observe que $a_1 \notin \mathfrak{A}$; suponha definido um elemento $a_i \notin \mathfrak{A}$, temos que $\mathrm{id}\langle a_i \rangle \nsubseteq \mathfrak{A}$ e, como $\mathfrak{A}$ é semiprimo, temos que $(\mathrm{id}\langle a_i \rangle)^2 \nsubseteq \mathfrak{A}$, de forma que podemos tomar um elemento $a_{i+1} \in (\mathrm{id}\langle a_i \rangle)^2 \setminus \mathfrak{A}$. A sequência $M = (a_1, a_2, \dots) \subseteq R$ assim definida é claramente uma m-sequência e é infinita, pois $a_i \notin \mathfrak{A}$, para $i = 1, 2, \dots$ e, portanto, M não contém o elemento nulo. □

Lema 2.1.8. *Se R é um anel e $M = (m_1, m_2, \dots) \subseteq R$ uma m-sequência infinita, então existe um ideal primo $\mathfrak{p} \subseteq R$ tal que $M \cap \mathfrak{p} = \emptyset$.*

Demonstração. Seja $\mathscr{F}$ a família dos ideais de R tais que a intersecção com M é vazia. Aplicaremos o Lema de Zorn sobre o conjunto parcialmente ordenado $(\mathscr{F}, \subseteq)$ para encontrar um elemento maximal e provaremos que tal elemento é um ideal primo.

Como a intersecção do ideal nulo e M é vazia, uma vez que a m-sequência M é infinita, temos que $\mathscr{F} \neq \emptyset$. Tomemos agora uma cadeia ascendente de elementos de $\mathscr{F}$, digamos

$$\mathfrak{A}_1 \subseteq \mathfrak{A}_2 \subseteq \cdots \subseteq \mathfrak{A}_i \subseteq \dots$$

e observe que, para cada $i = 1, 2, \ldots$, vale que $\mathfrak{A}_i \cap M = \emptyset$ e, portanto, $(\bigcup_{i=1}^{\infty} \mathfrak{A}_i) \cap M = \emptyset$, donde segue que $\bigcup_{i=1}^{\infty} \mathfrak{A}_i \in \mathscr{F}$. Concluímos que toda cadeia ascendente de elementos de $\mathscr{F}$ é limitada superiormente (por um elemento de $\mathscr{F}$) e, pelo Lema de Zorn, segue que existe um ideal $\mathfrak{p} \in \mathscr{F}$ maximal.

Para provar que $\mathfrak{p}$ é primo, suponha por absurdo que existam ideais $\mathfrak{A}, \mathfrak{B} \subseteq R$ tais que $\mathfrak{AB} \subseteq \mathfrak{p}$ mas $\mathfrak{A}, \mathfrak{B} \nsubseteq \mathfrak{p}$. Segue que os ideais $\overline{\mathfrak{A}} = \mathfrak{A} + \mathfrak{p}$, $\overline{\mathfrak{B}} = \mathfrak{B} + \mathfrak{p}$ contêm propriamente o ideal $\mathfrak{p}$ e são tais que $\overline{\mathfrak{A}}\ \overline{\mathfrak{B}} \subseteq \mathfrak{p}$ e, em particular, não pertencem à família $\mathscr{F}$ (caso contrário $\mathfrak{p}$ não seria maximal). Segue que existem $m_i, m_j \in M$ tais que $m_i \in \overline{\mathfrak{A}}$ e $m_j \in \overline{\mathfrak{B}}$. Podemos supor sem perda de generalidade que $i < j$. Como $m_i \in \overline{\mathfrak{A}}$, segue que $(\mathrm{id}\langle m_i \rangle)^2 \subseteq \overline{\mathfrak{A}}$ e, lembrando que $m_{i+1} \in (\mathrm{id}\langle m_i \rangle)^2$, segue que $m_{i+1} \in \overline{\mathfrak{A}}$. Repetindo o argumento $j - i - 1$ vezes, temos que $m_j \in \overline{\mathfrak{A}}$ e, por consequência,

$$\mathrm{id}\langle m_j \rangle \subseteq \overline{\mathfrak{A}}, \overline{\mathfrak{B}}, \quad \text{e daí,} \quad (\mathrm{id}\langle m_j \rangle)^2 \subseteq \overline{\mathfrak{A}}\ \overline{\mathfrak{B}} \subseteq \mathfrak{p},$$

um absurdo, pois dessa forma teríamos que $m_{j+1} \in \mathfrak{p}$. Conclui-se que $\mathfrak{p}$ é primo. □

Teorema 2.1.9. *Para todo anel R, $\operatorname{nil} R$ é a intersecção dos ideais primos de R.*

Demonstração. Se $\mathfrak{p}$ é um ideal primo de R, ele é, em particular, um ideal semiprimo. Pela Proposição 2.1.6, segue que $\operatorname{nil} R \subseteq \mathfrak{p}$. Logo, $\operatorname{nil} R$ está contido na intersecção de todos os ideais primos.

Para mostrar a inclusão inversa, tome um elemento $a \notin \operatorname{nil} R$. Pelo Lema 2.1.7, a pertence a uma m-sequência M que é disjunta de $\operatorname{nil} R$ e pelo Lema 2.1.8 existe um ideal primo $\mathfrak{p}$ que é disjunto desta sequência, donde segue que $a \notin \mathfrak{p}$ e, portanto, a não pertence à intersecção dos ideais primos de R. Segue daí o afirmado. □

A estrutura de anéis primos e semiprimos que satisfazem uma identidade polinomial será estudada com mais detalhes na Seção 3.4. A caracterização alternativa do radical primo dada pelo Teorema 2.1.9 será usada na demonstração do Teorema 3.4.3, que relaciona anéis primos e anéis semiprimos através do produto subdireto.

O radical primo foi definido e estudado inicialmente por R. Baer, em [Bae43]. A exposição acima é particularmente notável por independer da associatividade do anel R, de forma que podemos também definir o ideal $\operatorname{nil} R$ em álgebras não-associativas.

Observe que $\ell\text{-rad}\, R$ é um ideal semiprimo de R. De fato, para todo ideal $\mathfrak{A} \subseteq R$ tal que $\mathfrak{A}^2 \subseteq \ell\text{-rad}\, R$, vale que $\mathfrak{A}^2$ é um ideal localmente nilpotente. Assim, se $A = \{a_1, \ldots, a_m\} \subseteq \mathfrak{A}$ e S é o subanel gerado por A, então S^2 está contido no subanel gerado por $\{a_i a_j \mid i, j = 1, \ldots, m\} \subseteq \mathfrak{A}^2$, que por sua vez é nilpotente, pois $\mathfrak{A}^2$ é localmente nilpotente. por consequência, o subanel gerado por A é nilpotente. Segue daí que $\mathfrak{A}$ é localmente nilpotente e, portanto, $\mathfrak{A} \subseteq \ell\text{-rad}\, R$, donde segue que $\ell\text{-rad}\, R$ é um ideal semiprimo. Aplicando a Proposição 2.1.6, temos que

$$\operatorname{nil} R \subseteq \ell\text{-rad}\, R. \tag{2.1.10}$$

Essa inclusão é em geral estrita: Se k é um corpo, então defina R como o anel dos polinômios sobre indeterminadas t_i, com $i \in \mathbb{Z}$, e com relações $t_{i_1} t_{i_2} t_{i_3} = 0$, para todos inteiros $i_1 <$

$i_2 < i_3$ que formem uma progressão aritmética de razão 3. Assim, podemos definir um automorfismo de R como k-álgebra, dado por $\sigma(t_i) = t_{i+1}$, para todo $i \in \mathbb{Z}$. Em [Ram84], J. Ram mostrou que o anel $R[x;\sigma]$ é um anel primo que contém um ideal localmente nilpotente não nulo e, em particular, $\operatorname{nil}(R[x;\sigma]) \nsubseteq \ell\text{-rad}(R[x;\sigma])$.

Antes de prosseguir, vamos mostrar a seguinte caracterização alternativa de anéis semiprimos:

Proposição 2.1.11. *Se R é um anel, são equivalentes:*

(1) *R é semiprimo;*

(2) $\operatorname{nil} R = 0$*;*

(3) *R não tem ideais nilpotentes não nulos.*

Demonstração. (1) $\Rightarrow$ (2) Pela definição, R é semiprimo se, e somente se, $0 \subseteq R$ é um ideal semiprimo. Pela Proposição 2.1.6, segue que $\operatorname{nil} R = 0$.

(2) $\Rightarrow$ (1) Se $\mathfrak{A}$ é um ideal de R tal que $\mathfrak{A}^2 = 0$, então $\mathfrak{A}^2$ está contido em $\operatorname{nil} R$ e, portanto, está contido em todos os ideais primos de R. Segue daí que $\mathfrak{A}$ está contido em todos os ideais primos de R e, portanto, $\mathfrak{A} \subseteq \operatorname{nil} R = 0$.

(3) $\Rightarrow$ (1) É imediata.

(1) $\Rightarrow$ (3) Suponha que exista um ideal $\mathfrak{A}$ nilpotente não nulo e tome um inteiro $n \geq 2$ minimal tal que $\mathfrak{A}^n = 0$. Daí, $(\mathfrak{A}^{n-1})^2 = \mathfrak{A}^{2n-2} = 0$ e, como R é semiprimo, segue que $\mathfrak{A}^{n-1} = 0$, contrariando a minimalidade de n. Segue que R não possui ideais nilpotentes não nulos. □

Corolário 2.1.12. *Para todo anel R,* $\operatorname{nil}(R/\operatorname{nil} R) = 0$.

Demonstração. Basta observar que $R/\operatorname{nil} R$ é semiprimo e aplicar a Proposição 2.1.11. □

2.2 O radical de Jacobson em anéis com unidade

Definiremos inicialmente o radical de Jacobson para anéis com unidade e demonstraremos algumas propriedades neste caso. A definição no caso geral está contida na Seção 2.4. Nesta seção, portanto, entenderemos o termo "anel" como um anel com unidade.

O radical de Jacobson foi definido e estudado inicialmente por Nathan Jacobson em [Jac45a] e [Jac45b], ambos publicados em 1945.

Tome R um anel. Definimos o *radical de Jacobson* de R como a intersecção dos seus ideais à esquerda maximais. Se R é não nulo, então R sempre admite ideais à esquerda maximais (e, portanto, próprios), de forma que sempre temos $\operatorname{rad} R \neq R$. Se R é o anel nulo, então definimos o radical de R como o ideal nulo.

A princípio, existe uma noção distinta do radical de Jacobson tomando os ideais à direita maximais na definição anterior. Provaremos logo mais adiante, no entanto, que as noções são as mesmas.

Lema 2.2.1. *Para todo $y \in R$, são equivalentes:*

(1) $y \in \operatorname{rad} R$;

(2) $1 - xy$ *tem um inverso à esquerda, para todo* $x \in R$;

(3) $yM = 0$, *para todo R-módulo à esquerda simples.*

Demonstração. (1) $\Rightarrow$ (2) Suponha que $y \in \operatorname{rad} R$ e que existe $x \in R$ tal que $1 - xy$ não possui um inverso à esquerda. por consequência, o ideal à esquerda $R(1 - xy)$ é próprio e, portanto, está contido em algum ideal à esquerda maximal $\mathfrak{m} \subseteq R$. Como $y \in \operatorname{rad} R$, segue que $y \in \mathfrak{m}$ e, daí, $1 = xy + (1 - xy) \in \mathfrak{m}$, um absurdo.

(2) $\Rightarrow$ (3) Seja M um R-módulo simples e $y \in R$ satisfazendo (2). Suponha que $ym \neq 0$ para algum $m \in M$. Como M é simples, temos que $R(ym) = M$ e existe $x \in R$ tal que $x(ym) = m$. Dessa forma, temos que $(1 - xy)m = 0$, e, como $1 - xy$ é inversível à esquerda, segue que $m = 0$, uma contradição.

(3) $\Rightarrow$ (1) Se $\mathfrak{m} \subseteq R$ é um ideal à esquerda maximal, então $M = R/\mathfrak{m}$ é um R-módulo à esquerda simples. Daí, $yM = 0$, ou seja, $yR \subseteq \mathfrak{m}$. Em particular, $y \in \mathfrak{m}$. Segue que $y \in \operatorname{rad} R$. □

Podemos escrever a condição (3) do Lema 2.2.1 como: "y pertence ao anulador de qualquer R-módulo à esquerda simples". Além disso, no caso em que M é um R-módulo à esquerda, $\operatorname{Ann}_\ell M$ é um ideal de R. Unindo isso ao fato de que uma intersecção arbitrária de ideais de R ainda é um ideal de R, temos deduzido o seguinte corolário:

Corolário 2.2.2. *Para todo anel R,* $\operatorname{rad} R = \bigcap_M \operatorname{Ann}_\ell M$, *onde a intersecção percorre todos os R-módulos à esquerda simples M. Em particular, segue que* $\operatorname{rad} R$ *é um ideal de R.*

Usando o Corolário 2.2.2, podemos adicionar uma condição ao Lema 2.2.1:

Proposição 2.2.3. *Para todo $y \in R$, são equivalentes:*

(1) $y \in \operatorname{rad} R$;

(2′) $1 - xyz$ *é um elemento inversível para quaisquer* $x, z \in R$.

Demonstração. Como (2') $\Rightarrow$ (2) $\Rightarrow$ (1), é suficiente mostrar que (1) $\Rightarrow$ (2'). Sejam $x, z \in R$. Como $\operatorname{rad} R$ é um ideal de R e $y \in \operatorname{rad} R$, temos que $yz \in \operatorname{rad} R$. Segue, pelo Lema 2.2.1, que existe $u \in R$ tal que $u(1 - xyz) = 1$ ou equivalentemente, $u = 1 + u(xyz)$. Em particular, u é inversível à direita. Mas, como $\operatorname{rad} R$ é um ideal e $yz \in \operatorname{rad} R$, temos que $xyz \in \operatorname{rad} R$. Logo, pelo Lema 2.2.1, $u = 1 + u(xyz) = 1 - (-u)(xyz)$ é inversível à esquerda. Segue que u é inversível e, portanto, $u^{-1} = 1 - xyz$ também o é. □

Por simetria, se definíssemos o radical de Jacobson como a intersecção dos ideais à direita maximais, poderíamos mostrar que esta definição é equivalente à condição (2') da Proposição 2.2.3. Portanto, em um anel (com unidade), a intersecção de todos os ideais à esquerda

maximais é igual à interseção de todos os ideais à direita maximais.

Mostraremos, a seguir, que o radical de Jacobson é igual ao radical definido por J. Wedderburn no caso de álgebras de dimensão finita. Para isso, lembremos que um anel R é chamado de *artiniano à esquerda* (respectivamente, à direita) se toda cadeia descendente de ideais à esquerda (respectivamente, à direita) estabiliza. Em particular, toda álgebra de dimensão finita é um anel artiniano à esquerda. Lembramos também que um anel é artiniano à esquerda se, e somente se, toda coleção não vazia de ideais à esquerda tem um elemento minimal.

Proposição 2.2.4. *Se R é um anel, então* $\operatorname{rad} R$ *é um ideal que contém todos os ideais unilaterais nil (em particular, todos os ideais unilaterais nilpotentes). Se R é adicionalmente artiniano à esquerda, então* $\operatorname{rad} R$ *é um ideal nilpotente.*

Demonstração. Seja $\mathfrak{A}$ um ideal à esquerda nil de R e $y \in \mathfrak{A}$. Então, para qualquer $x \in R$, temos $xy \in \mathfrak{A}$ é nil. Daí, existe inteiro positivo n tal que $(xy)^n = 0$ e, portanto, $(1 + (xy) + (xy)^2 + \cdots + (xy)^{n-1})(1 - xy) = (1 - (xy)^n) = 1$, ou seja, $1 - xy$ é inversível à esquerda. Segue que $y \in \operatorname{rad} R$, para todo $y \in \mathfrak{A}$, ou seja, $\mathfrak{A} \subseteq \operatorname{rad} R$.

Mostremos agora que $\operatorname{rad} R$ é um ideal nilpotente. Faça $J = \operatorname{rad} R$ e observe que, como R é artiniano à esquerda, a cadeia descendente $J \supseteq J^2 \supseteq \ldots$ estabiliza. Tome um inteiro positivo n tal que $J^n = J^{n+1} = ... = I$ e suponha que I seja não nulo. Daí, segue que o conjunto $\mathscr{F} = \{\mathfrak{A} \lhd_e R \mid I \cdot \mathfrak{A} \neq 0\}$ é não vazio, pois $R \in \mathscr{F}$. Como R é artiniano à esquerda, podemos tomar $\mathfrak{A}_0 \in \mathscr{F}$ minimal.

Tome $a \in \mathfrak{A}_0$ não nulo. Então $I \cdot a \subset \mathfrak{A}_0$ é um ideal à esquerda de R e

$$I(I \cdot a) = I^2 \cdot a = I \cdot a.$$

Assim, $I \cdot a \in \mathscr{F}$ e, pela minimalidade de $\mathfrak{A}_0$, $\mathfrak{A}_0 = I \cdot a$. Mas, como $a \in \mathfrak{A}_0$, existe $x \in I$ tal que $a = xa$, ou seja, $(1 - x)a = 0$. Como $x \in \operatorname{rad} R$, $1 - x$ é inversível à esquerda, e, portanto, segue que $a = 0$, um absurdo. Segue que $I = J^n = 0$. □

Demonstraremos a seguir duas proposições que estudam como o radical de Jacobson se comporta sob alguns homomorfismos. Ambas serão usadas na próxima seção, para mostrar que o radical de Jacobson do anel $R \otimes_k K$ é o ideal $(\operatorname{rad} R) \otimes_k K$, onde $k \subseteq K$ são corpos tais que K/k seja uma extensão finita e separável e R é uma k-álgebra.

Proposição 2.2.5. *Seja R um anel e $\mathfrak{A}$ um ideal de R contido em* $\operatorname{rad} R$. *Então* $\operatorname{rad}(R/\mathfrak{A}) = (\operatorname{rad} R)/\mathfrak{A}$.

Demonstração. Observe inicialmente que:

- Se $A \lhd_e R$ é maximal, então $A + \mathfrak{A} = A$ ou R. Dessa forma, temos que $\bigcap_A A = \bigcap_A (A + \mathfrak{A})$, onde ambas as intersecções percorrem os ideais à esquerda de R que são maximais;
- Os ideais maximais à esquerda de $R/\mathfrak{A}$ são da forma $A/\mathfrak{A}$, onde $A \lhd_e R$ é maximal e contém $\mathfrak{A}$. Além disso, se $A \lhd_e R$ é maximal, então $(A + \mathfrak{A})/\mathfrak{A} = R/\mathfrak{A}$ ou é um ideal à esquerda maximal de $R/\mathfrak{A}$. Dessa forma, $\bigcap_A ((A + \mathfrak{A})/\mathfrak{A})$ é igual à intersecção de todos os ideais à esquerda de $R/\mathfrak{A}$ maximais.

Daí, temos que:

$$(\operatorname{rad} R)/\mathfrak{A} = (\cap_A A)/\mathfrak{A} = (\cap_A (A+\mathfrak{A}))/\mathfrak{A} = \bigcap\nolimits_A ((A+\mathfrak{A})/\mathfrak{A}) = \operatorname{rad}(R/\mathfrak{A}).$$

Segue, portanto, o resultado desejado. □

Proposição 2.2.6. *Se R é um anel e $f : R \to R$ é um automorfismo, então $f(y) \in \operatorname{rad} R$, para todo $y \in \operatorname{rad} R$. Em outras palavras,* $\operatorname{rad} R$ *é um ideal fixo por todos automorfismos de R.*

Demonstração. Seja f um automorfismo, $y \in \operatorname{rad} R$ e $x \in R$ qualquer. Então, como f é sobrejetora, existe $x' \in R$ tal que $f(x') = x$. Dessa forma, $1 - xf(y) = f(1 - x'y)$. Como $y \in \operatorname{rad} R$, $1 - x'y$ é inversível à esquerda e, portanto, $1 - xf(y) = f(1 - x'y)$ também é. Segue que $f(y) \in \operatorname{rad} R$, como desejado. □

Em alguns casos, é possível usar a Proposição 2.2.5 para reduzir a demonstração de proposições sobre anéis para o caso particular em que os anéis têm radical de Jacobson nulo, como feito nas demonstrações do Teorema 2.3.10 e do Teorema 4.4.9. Encerrando esta pequena introdução, demonstremos o Lema de Nakayama, que descreve os ideais contidos no radical de Jacobson de um anel por meio dos seus módulos.

Lema 2.2.7 (T. Nakayama)**.** *Se R é um anel e $J \subseteq R$ é um ideal, então são equivalentes:*

(1) $J \subseteq \operatorname{rad} R$*;*

(2) *Para todo R-módulo à esquerda finitamente gerado ${}_RM$, se $J \cdot M = M$, então $M = 0$;*

(3) *Para todo R-módulo à esquerda M e todo submódulo $N \subseteq M$ tais que M/N seja finitamente gerado, se $N + J \cdot M = M$, então $N = M$.*

Demonstração. (1) ⇒ (2) Suponha que exista ${}_RM$ finitamente gerado tal que $J \cdot M = M$, mas $M \neq 0$. Como M é finitamente gerado, pelo Lema de Zorn, existe $M' \subsetneq M$ submódulo maximal. Dessa forma, M/M' é simples e, pelo Lema 2.2.1, vale que $J \cdot (M/M') = 0$. Em outras palavras, temos que $J \cdot M \subseteq M' \subsetneq M$, um absurdo, pois $J \cdot M = M$.

(2) ⇒ (3) Segue aplicando a condição (2) ao R-módulo finitamente gerado M/N.

(3) ⇒ (1) Suponha que exista $y \in J \setminus \operatorname{rad} R$. Segue que existe um ideal à esquerda maximal $\mathfrak{m} \subsetneq R$ tal que $y \notin \mathfrak{m}$ e, por consequência, $\mathfrak{m} + J \cdot R = \mathfrak{m} + J = R$. Além disso, como $R/\mathfrak{m}$ é um módulo simples, também é finitamente gerado. Pela aplicação da condição (3), temos que $\mathfrak{m} = R$, um absurdo. □

2.3 Radical de Jacobson e extensão de escalares

Nesta seção manteremos a convenção de que anéis e álgebras possuem unidade. O objetivo desta seção é mostrar que, se $k \subseteq K$ são corpos tais que a extensão K/k seja finita e separável, então, para qualquer k-álgebra R, o radical de Jacobson de $R \otimes_k K$ é igual a

$(\operatorname{rad} R) \otimes_k K$, onde R é identificado com o subanel $R \otimes 1 \subseteq R \otimes_k K$. Este resultado será usado para estudar o radical de Jacobson do anel de polinômios diferenciais (Lema 2.5.1). Seguiremos a exposição de [Lam01, p. 70-76]

Sejam S um anel e $R \subseteq S$ um subanel de S. Estamos particularmente interessados em relações de inclusão entre os conjuntos $R \cap \operatorname{rad} S$ e $\operatorname{rad} R$, que em geral não ocorre, como pode ser visto nos próximos exemplos.

Exemplo 2.3.1. Se R é um domínio local comutativo com ideal maximal $\mathfrak{m} \neq 0$, então $\operatorname{rad} R = \mathfrak{m}$. No entanto, se $S = R \setminus \{0\}$, então R é subanel da localização $S^{-1}R$, que é um corpo e, portanto, $\operatorname{rad} S^{-1}R = 0$.

Segue, neste caso, que $\operatorname{rad} R \nsubseteq R \cap \operatorname{rad} S^{-1}R$.

Exemplo 2.3.2. Se $R = \mathbb{Z}$ e $S = \mathbb{Z} \setminus 2\mathbb{Z}$, então

$$S^{-1}R = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; m \in \mathbb{Z} \text{ e } n \text{ é ímpar} \right\}$$

é um subanel tal que $\operatorname{rad} S^{-1}R = 2 \cdot S^{-1}R$. Como $\operatorname{rad} R = 0$, temos que $\operatorname{rad} R \not\supseteq R \cap \operatorname{rad} S^{-1}R$.

A seguir, mostraremos uma condição suficiente para que $R \cap \operatorname{rad} S \subseteq \operatorname{rad} R$.

Proposição 2.3.3. *Sejam S um anel e $R \subseteq S$ um subanel de S. Se o R-módulo ${}_RR$ é somando direto do R-módulo ${}_RS$, então $R \cap \operatorname{rad} S \subseteq \operatorname{rad} R$.*

Demonstração. Seja $T \subseteq R$ um ideal à esquerda tal que $S = R \oplus T$. É suficiente provar que, para todo $y \in R \cap \operatorname{rad} S$, $1 - y$ é inversível à direita em R. De fato, se isso for provado, então, para quaisquer $y \in R \cap \operatorname{rad} S$ e qualquer $x \in R$, $xy \in R \cap \operatorname{rad} S$ e, portanto, $1 - xy$ será inversível em S. Mas $1 - xy$ é inversível à direita em R, logo, pela unicidade do elemento inverso, teremos que $1 - xy$ é inversível em R.

Como $y \in \operatorname{rad} S$, $1 - y$ é inversível à esquerda em S. Ou seja, existem $r \in R$ e $t \in T$ tais que $(1 - y)(r + t) = 1$. Segue que

$$1 = (1 - y)(r + t) = (1 - y)r + (1 - y)t.$$

Como $1, (1 - y)r \in R$, $(1 - y)t \in T$ e a soma é direta, segue que $1 = (1 - y)r$, como desejado. □

Sejam R, S anéis e $\phi : R \to S$ um homomorfismo de anéis (lembre-se que pela nossa convenção, nesta seção estes homomorfismos preservam a unidade). Também estamos interessados na relação de inclusão $\phi(\operatorname{rad} R) \subseteq \operatorname{rad} S$. No caso em que ϕ é sobrejetor, temos que $\phi(\operatorname{rad} R) \subseteq \operatorname{rad} S$, pois, para todo $x \in \operatorname{rad} R$ e todo $f(y) \in S$, $1 - f(x)f(y) = f(1 - xy)$ é inversível pois $1 - xy$ o é. Será necessária, no entanto, uma condição alternativa sobre o homomorfismo ϕ.

Observe que S pode ser visto como um (R, R)-bimódulo através da estrutura $r \cdot s = \phi(r)s$ e $s \cdot r = s\phi(r)$, para quaisquer $r \in R$ e $s \in S$.

Proposição 2.3.4. *Tome R, S anéis, $\phi : R \to S$ um homomorfismo de anéis e considere S como um R-módulo à esquerda como acima. Se existirem $x_1, \ldots, x_n \in S$ que comutam com os elementos de $\phi(R)$ e são tais que*

$$S = R \cdot x_1 + \cdots + R \cdot x_n,$$

então $\phi(\operatorname{rad} R) \subseteq \operatorname{rad} S$.

Demonstração. Observe inicialmente que, se M é um S-módulo, então M tem estrutura de R-módulo através de ϕ. Em outras palavras, ${}_RM$ é um R-módulo com a estrutura $r \cdot m = \phi(r)m$.

Fixe $J = \operatorname{rad} R$. Para provar que $\phi(J) \subseteq \operatorname{rad} S$ é suficiente mostrar que, para todo S-módulo simples M, vale que $J \cdot M = 0$ (Lema 2.2.1). Para tal, usaremos o Lema de Nakayama (Lema 2.2.7). Tome ${}_SM$ um S-módulo simples e tome $m \in M$ não nulo. Dessa forma, $M = Sm$ e

$$M = Sm = (R \cdot x_1 + \cdots + R \cdot x_n)m = R \cdot x_1 m + \ldots R \cdot x_n m.$$

Concluímos que ${}_RM$ é um R-módulo finitamente gerado.

O conjunto $J \cdot M$ é um S-submódulo de M, pois, para qualquer $j = 1, \ldots, n$:

$$x_j(J \cdot M) = x_j\phi(J)M = \phi(J)x_jM = J \cdot (x_jM) \subseteq J \cdot M.$$

Como M é não nulo, pelo Lema de Nakayama, vale que $J \cdot M \subsetneq M$ e como M é simples, temos que $J \cdot M = 0$, como desejado. □

Através das próximas proposições, vamos estudar o radical de Jacobson da extensão de escalares.

Lema 2.3.5. *Seja k um corpo e K/k uma extensão de k. Então, para toda k-álgebra R, temos que $R \cap \operatorname{rad}(R \otimes_k L) \subseteq \operatorname{rad} R$. Se, adicionalmente, K/k for uma extensão finita ou $\dim_k R < \infty$, então $R \cap \operatorname{rad}(R \otimes_k K) = \operatorname{rad} R$.*

Demonstração. Tome $\{e_i\}_{i \in I}$ uma base de K como k-espaço vetorial com, digamos, $e_{i_0} = 1$, para algum $i_0 \in I$. Lembremos que $R \otimes_k K$ tem uma estrutura de R-módulo à esquerda dada por

$$r \cdot (r' \otimes e) = rr' \otimes z, \text{ para quaisquer } r, r' \in R \text{ e qualquer } z \in K.$$

Como identificamos R e $R \otimes 1$, temos que $R = R(1 \otimes 1)$ e podemos decompor ${}_R(R \otimes_k K)$ como a seguinte soma direta:

$$R \otimes_k K = R \oplus \bigoplus_{i \neq i_0} R(1 \otimes e_i). \tag{2.3.6}$$

Pela Proposição 2.3.3, temos que $R \cap \operatorname{rad}(R \otimes_k K) \subseteq \operatorname{rad} R$.

Se $\dim_k R < \infty$, então R é artiniano à esquerda e, pela Proposição 2.2.4, segue que $\operatorname{rad} R$ é um ideal nilpotente de R. Logo, $(\operatorname{rad} R) \otimes_k K$ é um ideal nilpotente de $R \otimes_k K$ e, novamente pela Proposição 2.2.4, $(\operatorname{rad} R) \otimes_k K \subseteq \operatorname{rad}(R \otimes_k K)$. Assim,

$$\operatorname{rad} R \subseteq R \cap ((\operatorname{rad} R) \otimes_k K) \subseteq R \cap \operatorname{rad}(R \otimes_k K),$$

obtendo a inclusão reversa.

Suponha agora que $[K : k] = n < \infty$. Nesse caso, a soma direta em (2.3.6) é finita e, para cada $i \in I$, $1 \otimes e_i$ comuta com os elementos de $R = R \otimes 1$. Pela Proposição 2.3.4 (usando ϕ como a inclusão de R em $R \otimes_k K$), segue que $\operatorname{rad} R \subseteq R \cap \operatorname{rad}(R \otimes_k K)$. □

Para a próxima demonstração iremos assumir alguns conceitos da Teoria de Galois. Os conceitos e teoremas assumidos podem ser encontrados em [Lan02, Cox04].

Lema 2.3.7. *Seja k um corpo, R uma k-álgebra e K/k uma extensão separável e algébrica. Se $\operatorname{rad} R = 0$, então $\operatorname{rad}(R \otimes_k K) = 0$.*

Demonstração. Podemos reduzir a demonstração para o caso em que a extensão é finita. De fato, suponha que este caso esteja demonstrado e tome R, k, K como no enunciado. Se $x \in \operatorname{rad}(R \otimes_k K)$, então existe um corpo L tal que $k \subseteq L \subseteq K$, $x \in R \otimes_k L$ e L/k é finita. Para simplificar a notação, vamos identificar as k-álgebras isomorfas $L \otimes_L K$ e K, de forma que

$$R \otimes_k K \equiv R \otimes_k (L \otimes_L K) = (R \otimes_k L) \otimes_L K$$

e, por consequência,

$$x \in \operatorname{rad}((R \otimes_k L) \otimes_L K).$$

Aplicando o Lema 2.3.5 para a L-álgebra $R \otimes_k L$ e a extensão K/L, temos que

$$x \in (R \otimes_k L) \cap \operatorname{rad}((R \otimes_k L) \otimes_L K) \subseteq \operatorname{rad}(R \otimes_k L).$$

Assumindo que o lema vale para o caso de extensões finitas e lembrando que L/k é finita, segue que $\operatorname{rad}(R \otimes_k L) = 0$ e que $x = 0$. Portanto, $\operatorname{rad}(R \otimes_k K) = 0$.

Assumiremos, assim, que K/k é um extensão finita.

Seja E o fecho normal do corpo K sobre k, ou seja, o menor corpo que contém K e tal que E/k é normal. [Cox04, p. 156, Ex. 6,7]. Daí, E/k é uma extensão de Galois finita e, aplicando como anteriormente o Lema 2.3.5 à K-álgebra $R \otimes_k K$ e à extensão finita E/K, temos que

$$\operatorname{rad}(R \otimes_k K) = (R \otimes_k K) \cap \operatorname{rad}((R \otimes_k K) \otimes_K E) \subseteq \operatorname{rad}((R \otimes_k K) \otimes_K E) = \operatorname{rad}(R \otimes_k E).$$

É suficiente, portanto, mostrar que $\operatorname{rad}(R \otimes_k E) = 0$. Seja $\{e_1, \ldots, e_n\}$ uma k-base de E e seja G o grupo de Galois de E/k. Podemos estender a ação de G em K para $\operatorname{rad}(R \otimes_k E)$ identificando $g \in G$ com o automorfismo de anéis $\mathrm{Id}_R \otimes g : R \otimes_k E \to R \otimes_k E$.

Para todo $x = \sum_i r_i \otimes e_i \in \operatorname{rad}(R \otimes_k E)$, para todo $g \in G$ e todo $j = 1, \ldots, n$,

$$g(xe_j) = g\left(\sum_{i=1}^{n} r_i \otimes e_i e_j\right) = \sum_{i=1}^{n} r_i \otimes g(e_i e_j) \tag{2.3.8}$$

Como o radical de Jacobson é um ideal invariante sob automorfismos, $xe_j \in \operatorname{rad}(R \otimes_k E)$ e g é um automorfismo, temos que $g(xe_j) \in \operatorname{rad}(R \otimes_k E)$.

Lembre que a função traço de E/k é

$$\begin{aligned} \operatorname{tr} : E &\to k \\ e &\mapsto \sum_{g \in G} g(e) \end{aligned}$$

Somando (2.3.8) para todo $g \in G$, temos que

$$\begin{aligned} \sum_{g \in G} g(xe_j) = \sum_{i=1}^{n} \left(r_i \otimes \sum_{g \in G} g(e_i e_j) \right) &= \sum_{i=1}^{n} r_i \otimes \operatorname{tr}(e_i e_j) \\ &= \sum_{i=1}^{n} r_i \ \operatorname{tr}(e_i e_j) \otimes 1 \end{aligned}$$

e, portanto, tal elemento pertence à $R \cap \operatorname{rad}(R \otimes_k E)$. Pelo Lema 2.3.5,

$$R \cap \operatorname{rad}(R \otimes_k E) \subseteq \operatorname{rad} R = 0$$

e segue daí que $\sum_{i=1}^{n} r_i \operatorname{tr}(e_i e_j) = 0$, para todo $j = 1, \ldots, n$. Alternativamente, em forma matricial,

$$\begin{pmatrix} r_1 & \cdots & r_n \end{pmatrix} \begin{pmatrix} \operatorname{tr}(e_1e_1) & \operatorname{tr}(e_1e_2) & \cdots & \operatorname{tr}(e_1e_n) \\ \operatorname{tr}(e_2e_1) & \operatorname{tr}(e_2e_2) & \cdots & \operatorname{tr}(e_2e_n) \\ \vdots & \vdots & & \vdots \\ \operatorname{tr}(e_ne_1) & \operatorname{tr}(e_ne_2) & \cdots & \operatorname{tr}(e_ne_n) \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix} \tag{2.3.9}$$

Como E/k é separável, a forma bilinear

$$(x, y) \mapsto \operatorname{tr}(xy)$$

é não-degenerada ([Lan02, p. 286]). Equivalentemente, a matriz $(\operatorname{tr}(e_i e_j))$ é inversível. Segue de (2.3.9) que $r_1 = \cdots = r_n = 0$, e, portanto, $x = 0$. □

Podemos finalmente demonstrar o resultado almejado.

Teorema 2.3.10. *Seja R uma k-álgebra e K/k uma extensão finita e separável. Então* $\operatorname{rad}(R \otimes_k K) = (\operatorname{rad} R) \otimes_k K$.

Demonstração. Pelo Lema 2.3.5, $(\operatorname{rad} R) \otimes_k K \subseteq \operatorname{rad}(R \otimes_k K)$. Além disso, observe que

$$(R \otimes_k K)/((\operatorname{rad} R) \otimes_k K) \simeq (R/\operatorname{rad} R) \otimes_k K.$$

Considere a k-álgebra $S = R/\operatorname{rad} R$. Sabemos que $\operatorname{rad} S = 0$. Aplicando o Lema 2.3.7 para S e a extensão K/k, temos que o radical de $(S \otimes_k K)$ é nulo e, portanto, o radical de $(R \otimes_k K)/((\operatorname{rad} R) \otimes_k K)$ também é nulo. Mas pela Proposição 2.2.5, segue que $\operatorname{rad}(R \otimes_k K) \supseteq (\operatorname{rad} R) \otimes_k K$. Logo, $\operatorname{rad}(R \otimes_k K) = (\operatorname{rad} R) \otimes_k K$. □

O Teorema 2.3.10 foi adaptado da versão mais geral contida em [Lam01, (5.17), p. 76], onde a condição de que K/k é finita é substituída pela condição de que K/k é algébrica. Esta versão mais abrangente foi demonstrada inicialmente por S. A. Amitsur, em [Ami58].

2.4 Radical de Jacobson em anéis arbitrários

Nesta seção, veremos a extensão do conceito de radical de Jacobson em anéis possivelmente sem unidade. Comecemos com algumas definições preliminares.

Definição 2.4.1. Se $x \in R$ e $S \subseteq R$, então

- dizemos que x é *quasi-regular à esquerda*[2] em R (respectivamente, à direita) se existir $y \in R$ tal que $x+y-yx = 0$ (respectivamente, $x+y-xy = 0$). Se x for simultaneamente quasi-regular à esquerda e à direita, dizemos que x é *quasi-regular*;

- dizemos que S é *quasi-regular à esquerda* em R (respectivamente, à direita) se todo elemento de S for quasi-regular à esquerda (à direita). Se S for simultaneamente quasi-regular à esquerda e à direita, dizemos que S é *quasi-regular*.

Exemplo 2.4.2. Se $a, b \in R$ e ab é quasi-regular à esquerda, então ba também é. De fato, seja $u \in R$ tal que $ab + u - uab = 0$. Definindo $v = b(ua - a)$, temos que

$$\begin{aligned} ba + v - vba &= ba + b(ua - a) - b(ua - a)ba \\ &= bua + b(a - ua)ba \\ &= b(u + ab - uab)a = 0. \end{aligned}$$

Exemplo 2.4.3. Se a é nilpotente então a é quasi-regular. De fato, se n é um inteiro positivo tal que $a^n = 0$, então fazendo $x = -(a + a^2 + \cdots + a^{n-1})$, temos que

$$\begin{aligned} a + x - xa &= a + x + (a^2 + a^3 + \cdots + a^n) \\ &= x + (a + a^2 + \cdots + a^{n-1} + a^n) \\ &= x + (-x) + a^n = a^n = 0. \end{aligned}$$

Como claramente $a + x - ax = a + x - xa$, vale o resultado. Segue também que, se $S \subseteq R$ é um conjunto nil, então S é quasi-regular.

Exemplo 2.4.4. Seja $\mathfrak{A} \subseteq R$ um ideal à esquerda. Se $\mathfrak{A}$ é quasi-regular à esquerda, então ele é quasi-regular. De fato, seja $a \in \mathfrak{A}$ e tome $b \in \mathfrak{A}$ tal que $a + b - ba = 0$. Daí, $b = ba - a \in \mathfrak{A}$ e, portanto, existe $a' \in R$ tal que $a' + b - a'b = 0$. Mas

$$\begin{aligned} a' &= a' + (a + b - ba) - a'(a + b - ba) \\ &= (a' + b - a'b) + a - (a' + b - a'b)a = a. \end{aligned}$$

E, portanto, segue que $a + b - ab = 0$.

[2]Quando não houver risco de confusão, vamos omitir a menção ao anel e nos referir a elementos e conjuntos quasi-regulares à esquerda/direita, simplesmente.

O segredo da "mágica" do Exemplo 2.4.4 é revelado com a seguinte notação: Defina, para quaisquer $a, b \in R$ o elemento $a \circ b = a + b - ab$. Daí, $\circ : R \times R \to R$ é uma operação associativa cujo elemento neutro é $0 \in R$. Nesta notação, o desenvolvimento no exemplo é expresso como:

$$a' = a' \circ 0 = a' \circ (b \circ a) = (a' \circ b) \circ a = 0 \circ a = a.$$

Além disso, temos que

- um elemento $a \in R$ é quasi-regular se, e somente se, existe $b \in R$ tal que $a \circ b = 0$, ou em outras palavras, a é inversível em relação a $\circ$;

- um ideal à esquerda $\mathfrak{A} \subseteq R$ é quasi-regular se, e somente se, $(\mathfrak{A}, \circ)$ é um grupo. Claramente se $(\mathfrak{A}, \circ)$ é um grupo, então todo elemento de $\mathfrak{A}$ é quasi-regular. Reciprocamente, se $\mathfrak{A}$ é quasi-regular, então, para todo $a \in \mathfrak{A}$, existe $b \in R$ tal que $a + b - ab = 0$ e, portanto, $b = ab - a \in \mathfrak{A}$, donde segue que a é inversível em $(\mathfrak{A}, \circ)$.

Exemplo 2.4.5. Se R é um anel com unidade, então o elemento $a \in R$ é quasi-regular à esquerda (respectivamente, à direita) se, e somente se, $1 - a$ é inversível à esquerda. De fato, se $b \in R$ é tal que $a + b - ba = b \circ a = 0$, então $(1 - b)(1 - a) = 1 - (b + a - ba) = 1$. Reciprocamente, se $u \in R$ é tal que $u(1 - a) = 1$, então

$$(1 - u) \circ a = 1 - u + a - (1 - u)a = 1 - (u - ua) = 0.$$

A definição do radical de Jacobson da Seção 2.2 não pode ser diretamente estendida para anéis sem unidade, uma vez que não é garantida nestes a existência de ideais à esquerda maximais. Tampouco podemos defini-lo como o conjunto dos elementos $y \in R$ tais que $1 - xy$ é inversível à esquerda em R para todo $x \in R$. Por outro lado, em vista do Exemplo 2.4.5, se R possui unidade, o radical de Jacobson de R é o conjunto dos elementos $y \in R$ tais que Ry é quasi-regular à esquerda. Mostraremos a seguir que esta é uma boa propriedade para generalizar a definição da Seção 2.2.

Definição 2.4.6. Se R é um anel, então definimos o radical de Jacobson como

$$\begin{aligned} \operatorname{rad} R &= \{y \in R \mid (Ry, \circ) \text{ é grupo}\} \\ &= \{y \in R \mid Ry \text{ é quasi-regular}\} \quad (= \{y \in R \mid yR \text{ é quasi-regular}\}) \\ &= \{y \in R \mid xy \text{ é quasi-regular à esquerda, para todo } x \in R\}. \end{aligned}$$

Assim como no caso de anéis com unidade, $\operatorname{rad} R$ é um ideal de R. De fato, sejam $a, b \in \operatorname{rad} R$. Para mostrar que $a + b \in \operatorname{rad} R$ devemos mostrar que, para qualquer $r \in R$, $r(a + b)$ é um elemento quasi-regular à esquerda. Como $a, b \in \operatorname{rad} R$, temos que $ra \in Ra$ é um elemento quasi-regular. Podemos, portanto, tomar $u \in R$ tal que $u \circ ra = 0$ e, uma vez que $(r - ur)b \in Rb$ é quasi-regular, podemos tomar $v \in R$ tal que $v \circ ((r - ur)b) = 0$. Dessa

forma, temos que $(v \circ u) \in R$ é tal que:

$$\begin{aligned}(v \circ u) \circ (r(a+b)) &= v \circ (u \circ (r(a+b))) \\ &= v \circ (u + r(a+b) - ur(a+b)) \\ &= v \circ ((u + ra - ura) + (r - ur)b) \\ &= v \circ ((u \circ ra) + (r - ur)b) \\ &= v \circ ((r - ur)b) = 0\end{aligned}$$

E, portanto, segue que $a + b \in \operatorname{rad} R$.

É imediato da definição que, se $r \in R$ e $a \in \operatorname{rad} R$, então $ra \in \operatorname{rad} R$. Além disso, $(rs)a$ é quasi-regular à esquerda, para todo $s \in R$, e, portanto, $s(ar)$ também é quasi-regular à esquerda (Exemplo 2.4.2), para todo $s \in R$. Segue que $ar \in \operatorname{rad} R$.

Também temos que $\operatorname{rad} R$ é um ideal quasi-regular de R. De fato, se $a \in \operatorname{rad} R$, então $a^2 \in Ra$ é quasi-regular e, portanto, existe $b \in R$ tal que $b \circ a^2 = 0$. Mas daí, temos que $(b \circ (-a)) \circ a = b \circ (-a \circ a) = b \circ a^2 = 0$, donde segue que a é quasi-regular à esquerda.

Além disso, se $\mathfrak{A} \subseteq R$ é um ideal à esquerda quasi-regular e $a \in \mathfrak{A}$, então, para todo $r \in R$, $ra \in \mathfrak{A}$ e, portanto, ra é um elemento quasi-regular à esquerda. Segue que se $a \in \mathfrak{A}$, então $a \in \operatorname{rad} R$. O mesmo vale para se $\mathfrak{A}$ fosse um ideal à direita quasi-regular. Em outras palavras, $\operatorname{rad} R$ contém todos ideais à esquerda (à direita) quasi-regulares. O desenvolvido nos parágrafos anteriores pode ser resumido na seguinte proposição:

Proposição 2.4.7. *Se R é um anel, então* $\operatorname{rad} R$ *é um ideal de R quasi-regular que contém todos os ideais unilaterais quasi-regulares de R. Em particular, R contém todos os ideais unilaterais nil de R e*

$$\operatorname{Nil} R \subseteq \operatorname{rad} R. \tag{2.4.8}$$

Façamos algumas observações. A inclusão (2.4.8) é, em geral, estrita. Se R é um domínio local comutativo com ideal maximal não nulo (por exemplo, o anel das potências formais $\mathbb{R}[[x]]$, ver Definição 3.4.9), então R tem apenas um ideal maximal, que é o radical de Jacobson, enquanto $\operatorname{Nil} R = 0$.

Se $f : R \to S$ é um homomorfismo sobrejetor de anéis, então $f(\operatorname{rad} R) \subseteq \operatorname{rad} S$. De fato, se $y \in \operatorname{rad} R$, então, para todo $s \in S$, existe $x \in R$ tal que $f(x) = s$ e existe $u \in R$ tal que $u \circ xy = 0$. Daí,

$$f(u) \circ (sf(y)) = f(u) + f(x)f(y) - f(u)f(x)f(y) = f(u + xy - uxy) = f(0) = 0.$$

Assim, $f(y) \in \operatorname{rad} S$.

Por fim, se R é um anel nil, então, pela Proposição 2.4.7, $R = \operatorname{rad} R$. De maneira geral, se R é um anel tal que $R = \operatorname{rad} R$, então dizemos que R é um *anel radical segundo Jacobson* ou, simplesmente, *anel radical*. Outros exemplos importantes de anéis radicais são os anéis localmente nilpotentes. Também damos um nome especial aos anéis com radical de Jacobson nulo: são os chamados *anéis semiprimitivos*.

Provaremos agora outra caracterização do radical de Jacobson. Dizemos que um ideal à esquerda $I \subsetneq R$ é *modular* se existe um elemento $e \in R$ tal que, para todo $r \in R$, $r - re \in I$ ou, em outras palavras, $r \equiv re \pmod{I}$.

Proposição 2.4.9. *São válidas as seguintes afirmações:*

(1) *Todo ideal à esquerda modular está contido num ideal à esquerda modular maximal;*

(2) *O radical de Jacobson de um anel é a intersecção de seus ideais à esquerda modulares maximais (considerando a intersecção de uma família vazia como o anel inteiro).*

Demonstração. Para provar (1), tome um ideal à esquerda modular $I \subsetneq R$ e considere a família $\mathscr{F} = \{\mathfrak{A} \lhd_e R \mid I \subseteq \mathfrak{A} \subsetneq R\}$. A família $\mathscr{F}$ é não vazia e é tal que toda cadeia ascendente de seus elementos tem um limitante superior. É fácil ver isto, uma vez que um ideal à esquerda I' é tal que $I' \neq R$ se, e somente se, $e \notin I'$, onde $e \in I$ é tal que $r \equiv re \pmod{I}$. Segue que $(\mathscr{F}, \subseteq)$ satisfaz as hipóteses do Lema de Zorn e existe $\mathfrak{m} \in \mathscr{F}$ maximal em $\mathscr{F}$. Se M é um ideal à esquerda modular tal que $\mathfrak{m} \subseteq M \subsetneq R$, então ele contém I e, portanto, pertence à família $\mathscr{F}$. Mas como $\mathfrak{m}$ é maximal em $\mathscr{F}$, segue que $M = \mathfrak{m}$, ou seja, $\mathfrak{m}$ é modular maximal e contém I.

Provemos agora (2). Seja J a intersecção de todos os ideais à esquerda modulares maximais e tome $e \in R$ um elemento que não é quasi-regular à esquerda. Segue que o conjunto $\{r - re \mid r \in R\}$ é um ideal à esquerda modular que não contém o elemento e. Por (1), existe um ideal modular maximal $\mathfrak{m} \subsetneq R$ que contém tal conjunto e temos que $e \notin \mathfrak{m}$, pois, caso contrário, para todo $r \in R$, $r = (r - re) + re \in \mathfrak{m}$, um absurdo. Conclui-se que $e \notin \mathfrak{m}$ e, portanto, $e \notin J$. Segue que J é um ideal à esquerda contido no conjunto dos elementos quasi-regulares à esquerda de R.

Se $y \in J$, então, para todo $x \in R$, $xy \in J$, pois J é ideal à esquerda e, pelo parágrafo anterior, xy é quasi-regular à esquerda. Segue que $y \in \operatorname{rad} R$ e, por consequência, $J \in \operatorname{rad} R$.

Suponha agora que $J \subsetneq \operatorname{rad} R$. Segue que $\operatorname{rad} R \nsubseteq J$ e, em particular, $\mathfrak{m} + \operatorname{rad} R$ é um ideal modular que contém propriamente $\mathfrak{m}$ e, por consequência, $\mathfrak{m} + \operatorname{rad} R = R$. Tome $e \in R$ tal que $r - re \in \mathfrak{m}$, para todo $r \in R$. Em particular, $e - e^2 \in \mathfrak{m}$. Além disso, existem $a \in \mathfrak{m}$ e $b \in \operatorname{rad} R$ tais que $e = a + b$ ou, alternativamente, $e - b = a \in \mathfrak{m}$. por consequência, $e - eb = (e - b) + (b - be) \in \mathfrak{m}$. Mas, como $\operatorname{rad} R$ é quasi-regular e $b \in \operatorname{rad} R$, temos que existe $b' \in R$ tal que $b + b' - b'b = 0$ e

$$e = e - (b + b' - b'b)e = (e - be) - b'(e - be) \in \mathfrak{m},$$

um absurdo. Logo, $\operatorname{rad} R = J$. □

A Proposição 2.4.9 mostra uma generalização da caracterização do radical de Jacobson dada como intersecção dos ideais à esquerda maximais. De fato, em um anel com unidade todo ideal é modular e, portanto, o conjunto dos ideais à esquerda modulares maximais é igual ao conjunto dos ideais à esquerda maximais. Como consequência, temos o seguinte resultado:

Proposição 2.4.10. *Para todo anel R vale que*

(1) $\operatorname{rad}(R/\operatorname{rad} R) = 0$;

(2) *se I é um ideal de R então, considerando I como um anel,* $\operatorname{rad} I = I \cap \operatorname{rad} R$.

Demonstração. (1) Seja $\mathfrak{m} \subseteq R$ um ideal à esquerda modular que contém $\operatorname{rad} R$. Segue que o conjunto $\mathfrak{m}/\operatorname{rad} R \lhd_e R/\operatorname{rad} R$ é modular. De fato, se $e \in R$ é tal que $r - re \in \mathfrak{m}$, para todo $r \in R$, então, para todo $r \in R$,

$$(r + \operatorname{rad} R) - (r + \operatorname{rad} R)(e + \operatorname{rad} R) = (r - re) + \operatorname{rad} R \in \mathfrak{m}/\operatorname{rad} R.$$

Além disso, supondo adicionalmente que $\mathfrak{m}$ é modular maximal, então é fácil ver que $\mathfrak{m}/\operatorname{rad} R$ também é modular maximal. Logo, se $y+\operatorname{rad} R \in \operatorname{rad}(R/\operatorname{rad} R)$, então $y \in \mathfrak{m}$, para todo $\mathfrak{m} \lhd_e R$ modular maximal que contém $\operatorname{rad} R$, ou seja, $y \in \operatorname{rad} R$. Conclui-se que $\operatorname{rad}(R/\operatorname{rad} R) = 0$.

(2) Em vista da Proposição 2.4.7, para provar que $I \cap \operatorname{rad} R \subseteq \operatorname{rad} I$, é suficiente mostrar que $I \cap \operatorname{rad} R$ é um ideal quasi-regular de I. Se $a \in I \cap \operatorname{rad} R$, então existe $b \in R$ tal que $a+b-ba = 0$. Mas $b = ba - a \in I$ e segue que a é quasi-regular em I. Para provar a inclusão inversa, tome $a \in \operatorname{rad} I$, observe que $(Ra)^2 \subseteq Ia \subseteq \operatorname{rad} I$. Assim, temos que $(Ra)^2$ é um ideal à esquerda quasi-regular e $(Ra)^2 \subseteq \operatorname{rad} R$. Segue que o conjunto $(Ra+\operatorname{rad} R)/\operatorname{rad} R \subseteq R/\operatorname{rad} R$ é tal que $((Ra + \operatorname{rad} R)/\operatorname{rad} R)^2 = 0$, ou seja, $(Ra + \operatorname{rad} R)/\operatorname{rad} R$ é um conjunto nilpotente e, em particular, é nil. Pela Proposição 2.4.7, segue que $(Ra + \operatorname{rad} R)/\operatorname{rad} R \subseteq \operatorname{rad}(R/\operatorname{rad} R) = 0$, donde segue que $Ra \subseteq \operatorname{rad} R$. Em particular, Ra é quasi-regular e temos que $a \in \operatorname{rad} R$, donde segue que $a \in I \cap \operatorname{rad} R$. □

A Proposição 2.4.10 nos permite concluir que, se R é um anel e I é um ideal contido no radical de Jacobson de R, então $\operatorname{rad} I = I$.

2.5 O radical de Jacobson de anéis de polinômios diferenciais

O objetivo desta seção é provar que o radical de Jacobson do anel $R[x;\delta]$ é o anel $N[x;\delta]$, onde N é um ideal do anel R fixo pela derivação δ. Seguiremos a exposição de [FKM83].

Fixe um anel R, um primo positivo $p \in \mathbb{Z}$ e defina o ideal $R_p = \{r \in R \mid pr = 0\}$. Se $\delta : R \to R$ é uma derivação, então, para qualquer $r \in R$, $p\delta(r) = \delta(pr) = \delta(0) = 0$, ou seja, $\delta(R_p) \subseteq R_p$. Podemos, portanto, considerar que δ é uma derivação de R_p quando restrita a esse ideal e, dessa forma, $R_p[x;\delta]$ é um ideal de $R[x;\delta]$. Pelo item (2) da Proposição 2.4.10,

$$\operatorname{rad}(R_p[x;\delta]) = \operatorname{rad}(R[x;\delta]) \cap R_p[x;\delta].$$

Considere o grupo abeliano $R_p^{\#} = R_p \oplus \mathbb{Z}_p$ e a multiplicação $(a,m)(b,n) = (ab + na + mb, mn)$, para quaisquer $(a,m),(b,n) \in R_p^{\#}$. Com tal multiplicação, $R_p^{\#}$ é uma $\mathbb{Z}_p$-álgebra com unidade $(0,1)$ e que contém R_p como ideal. Estenderemos a derivação δ para $\delta : R_p^{\#} \to R_p^{\#}$ dada por $\delta(a,m) = (\delta(a),0)$, para qualquer $(a,m) \in R_p^{\#}$. Dessa forma, $\delta : R_p^{\#} \to R_p^{\#}$ ainda é uma derivação. Assim, podemos construir o anel $R_p^{\#}[x;\delta]$ que contém $R_p[x;\delta]$ como ideal.

Vamos agora estudar o radical de Jacobson de $R_p^{\#}[x;\delta]$. Seja $f(x) \in \mathrm{rad}(R_p^{\#}[x;\delta])$. Como grupo aditivo, $R_p^{\#}[x;\delta] = R_p[x;\delta] \oplus \mathbb{Z}_{\text{ı}}[x;\delta]$ e, daí, existem $f_1(x) \in R_p[x;\delta]$ e $f_2(x) \in \mathbb{Z}_p[x;\delta]$ tais que $f(x) = f_1(x) + f_2(x)$. Como $R_p^{\#}[x;\delta]$ tem unidade, $f(x) \in \mathrm{rad}(R_p^{\#}[x;\delta])$ se, e somente se, para todo $g(x) \in R_p^{\#}[x;\delta]$, $1 - g(x)f(x)$ é inversível à esquerda. Em particular, para todo $g(x) \in \mathbb{Z}_p[x;\delta]$, temos que:

$$1 - g(x)f(x) = 1 - g(x)(f_1(x) + f_2(x)) = -\underbrace{g(x)f_1(x)}_{\in R_p[x;\delta]} + \underbrace{(1 - g(x)f_2(x))}_{\in \mathbb{Z}_p[x;\delta]}.$$

Analisando a multiplicação de $R_p^{\#}[x;\delta]$, temos que, se $1-g(x)f(x)$ é inversível à esquerda em $R_p^{\#}[x;\delta]$, então $1 - g(x)f_2(x)$ é inversível à esquerda em $\mathbb{Z}_p[x;\delta]$, para todo $g(x) \in \mathbb{Z}_p[x;\delta]$, e segue que $f_2(x) \in \mathrm{rad}(\mathbb{Z}_p[x;\delta])$. No entanto, com esta derivação, $\mathbb{Z}_p[x;\delta] = \mathbb{Z}_p[x]$ e como $\mathrm{rad}(\mathbb{Z}_p[x]) = 0$, segue que $f_2(x) = 0$. Conclui-se que $\mathrm{rad}(R_p^{\#}[x;\delta]) \subseteq R_p[x;\delta]$.

Usando o item (2) da Proposição 2.4.10, temos que

$$\mathrm{rad}(R_p[x;\delta]) = \mathrm{rad}(R_p^{\#}[x;\delta]) \cap R_p[x;\delta] = \mathrm{rad}(R_p^{\#}[x;\delta]).$$

Defina o conjunto $S = R \cap \mathrm{rad}(R[x;\delta])$ e, para todo inteiro $n \geq 2$, fixe k_q uma extensão de $\mathbb{Z}_p$ com $q = p^n$ elementos. Estamos finalmente em condições de provar duas proposições de M. Ferrero, K. Kishimoto e K. Motose.

Lema 2.5.1 ([FKM83])**.** *Seja R um anel e $\delta : R \to R$ uma derivação de R. Se $S = 0$, então* $\mathrm{rad}(R[x;\delta]) = 0$.

Demonstração. Suponha que o lema seja válido para anéis com unidade e tome A um anel sem unidade. Daí, podemos construir a seguinte multiplicação no grupo aditivo $A^{\#} = A \oplus \mathbb{Z}$:

$$(a,m)(b,n) = (ab + na + mb, mn), \text{ para quaisquer } a,b \in A, m,n \in \mathbb{Z}$$

Com essa multiplicação, $A^{\#}$ é um anel com unidade que contém A como ideal. Se $\delta : A \to A$ é uma derivação, podemos estender δ para uma derivação de $\delta : A^{\#} \to A^{\#}$ de forma que, como anteriormente, $\mathrm{rad}\, A^{\#}[x;\delta] = \mathrm{rad}\, A[x;\delta]$. Daí, se $A \cap \mathrm{rad}(A[x;\delta]) = 0$, então

$$A^{\#} \cap \mathrm{rad}(A^{\#}[x;\delta]) = A^{\#} \cap \mathrm{rad}(A[x;\delta]) \subseteq A \cap \mathrm{rad}(A[x;\delta]) = 0.$$

Segue que $A^{\#}$ é um anel com unidade satisfazendo as hipóteses do lema e, portanto, segue que $\mathrm{rad}(A[x;\delta]) = \mathrm{rad}(A^{\#}[x;\delta]) = 0$.

Assim, iremos assumir daqui em diante que R é um anel com unidade.

Suponha, por absurdo, que $S = 0$ e $\mathrm{rad}(R[x;\delta]) \neq 0$ e tome $f(x) \in \mathrm{rad}(R[x;\delta])$ não nulo com grau minimal, digamos, n. Como R tem unidade, podemos considerar o polinômio $f(x+1)$, que também pertence ao radical uma vez que, a função

$$\begin{aligned} R[x;\delta] &\to R[x;\delta] \\ f(x) &\mapsto f(x+1) \end{aligned}$$

é um homomorfismo sobrejetor. Mas daí, se $f(x) = \sum_{i=0}^{n} a_i x^i$, então

$$\begin{aligned} f(x+1) = \sum_{i=0}^{n} a_i (x+1)^i &= \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{i} \binom{i}{j} x^j \right) \\ &= \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} a_i x^j \\ &= \sum_{j=0}^{n} \left(\sum_{i=j}^{n} \binom{i}{j} a_i \right) x^j = a_n x^n + \sum_{j=0}^{n-1} \left(\sum_{i=j}^{n} \binom{i}{j} a_i \right) x^j. \end{aligned}$$

Em particular, conclui-se que $f(x+1)$ tem o mesmo coeficiente líder que $f(x)$. Assim, $f(x) - f(x+1) \in \mathrm{rad}(R[x;\delta])$ é um polinômio de grau menor do que n, donde segue que $f(x) = f(x+1)$. Desta relação, temos que

$$\begin{aligned} \sum_{j=0}^{n} a_j x^j = \sum_{j=0}^{n} \left(\sum_{i=j}^{n} \binom{i}{j} a_i \right) x^j \Rightarrow \\ a_j = \sum_{i=j}^{n} \binom{i}{j} a_i \end{aligned} \tag{2.5.2}$$

Em particular, fazendo $j = n-1$ em (2.5.2), temos que

$$a_{n-1} = \binom{n-1}{n-1} a_{n-1} + \binom{n}{n-1} a_n = a_{n-1} + n a_n \Rightarrow n a_n = 0.$$

Segue daí, que existe um primo positivo $p \in \mathbb{Z}$ tal que $p a_n = 0$. Ainda pela minimalidade do grau de $f(x)$, temos que $p f(x) = 0$, donde segue que

$$f(x) \in R_p[x;\delta] \cap \mathrm{rad}(R[x;\delta]) = \mathrm{rad}(R_p[x;\delta]) = \mathrm{rad}(R_p^{\#}[x;\delta]).$$

Considere $q = p^n$ e defina o anel $R_* = R_p^{\#} \otimes_{\mathbb{Z}_p} k_q$ e a derivação $\delta_* : R_* \to R_*$ definida por $\delta_*(a \otimes v) = \delta(a) \otimes v$, para todo $a \otimes v \in R_*$. Daí, $R_*[x;\delta_*] \simeq R_p^{\#}[x;\delta] \otimes_{\mathbb{Z}_p} k_q$ e, como a extensão $k_q/\mathbb{Z}_p$ é finita e separável, pelo Teorema 2.3.10, vale que:

$$\mathrm{rad}(R_p^{\#}[x;\delta]) \otimes_{\mathbb{Z}_p} k_q \simeq \mathrm{rad}(R_*[x;\delta_*]).$$

Seja $f_*(x) = \sum_{i=0}^{n} b_i x^i$ um polinômio de grau minimal pertencente a $\mathrm{rad}(R_*[x;\delta_*])$. Daí, como $n < p^n = q$, podemos tomar n elementos não nulos e distintos dois a dois $v_1, \ldots, v_n \in F_q$. Pelo mesmo argumento usado anteriormente, temos que $f_*(x) = f_*(x + v_j)$, para todo $j = 1, \ldots, n$. Em particular, fazendo $x = 0$ e lembrando que $v_1, \ldots, v_n \neq 0$, temos que $\sum_{i=1}^{n} b_i {v_j}^{i-1} = 0$ para todo $j = 1, \ldots, n$, ou, em forma matricial:

$$\begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 & \ldots & 1 \\ v_1 & v_2 & \ldots & v_n \\ \vdots & \vdots & & \vdots \\ {v_1}^{n-1} & {v_2}^{n-1} & \ldots & {v_n}^{n-1} \end{pmatrix}}_{=A} = \begin{pmatrix} 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Observe que o determinante $\det A$ é o determinante de Vandermonde, e portanto,

$$\det A = \prod_{1 \leq i < j \leq n} (v_i - v_j).$$

Como os elementos $v_1, \ldots, v_n$ são distintos, segue que $\det A \neq 0$. donde concluímos que $b_1 = \cdots = b_n = 0$, um absurdo, pois dessa forma, teríamos que $f(x) \in R \cap \operatorname{rad}(R[x;\delta]) = S = 0$. □

Teorema 2.5.3 ([FKM83])**.** *Para todo anel R e toda derivação $\delta : R \to R$,* $\operatorname{rad}(R[x;\delta]) = S[x;\delta]$*, onde $S = R \cap \operatorname{rad}(R[x;\delta])$ é tal que $\delta(S) \subseteq S$.*

Demonstração. Observe que S é um ideal de R fixo por δ pois, para todo $r \in S$, $rx, xr \in \operatorname{rad}(S[x;\delta])$ e daí, $\delta(r) = xr - rx \in \operatorname{rad}(S[x;\delta])$. Assim, podemos definir sobre o anel $\overline{R} = R/S$ a derivação $\overline{\delta}$ definida por $\overline{\delta}(r+S) = \delta(r) + S$, para todo $r \in R$. A projeção de R em $\overline{R}$ nos permite definir o homomorfismo sobrejetor $\pi : R[x;\delta] \to \overline{R}[x;\overline{\delta}]$ que estende a projeção. Daí, temos que $\ker \pi = S[x;\delta]$ e pelo Teorema do Homomorfismo

$$R[x;\delta]/S[x;\delta] = R[x;\delta]/\ker \pi \simeq \overline{R}[x;\overline{\delta}].$$

Como $S[x;\delta] \subseteq \operatorname{rad}(R[x;\delta])$, temos que

$$\operatorname{rad}(\overline{R}[x;\overline{\delta}]) \simeq \operatorname{rad}(R[x;\delta]/S[x;\delta]) = \operatorname{rad}(R[x;\delta])/S[x;\delta]. \tag{2.5.4}$$

Faça $\overline{S} = \overline{R} \cap \operatorname{rad}(\overline{R}[x;\overline{\delta}])$ e tome $y \in R$ tal que $y + S \in \overline{S}$. Segue que, para todo $r \in R$, existe $t \in R$ tal que $(t+S) \circ (ry+S) = (t \circ ry) + S = 0 + S$. Por outro lado, como o radical de Jacobson é um ideal quasi-regular, $t \circ ry \in S$ é um elemento quasi-regular à esquerda e, portanto, ry é quasi-regular à esquerda. Conclui-se que $y \in \operatorname{rad} R[x;\delta]$ e que $y \in S$, ou seja, $y + S = 0 + S$. Logo, $\overline{S} = 0$. Pelo Lema 2.5.1, temos que $\operatorname{rad}(\overline{R}[x;\overline{\delta}]) = 0$ e por (2.5.4), $\operatorname{rad}(R[x;\delta]) = S[x;\delta]$. □

2.6 Relações entre radicais

Lembremos das definições dos radicais deste capítulo:

$$\begin{aligned}
\operatorname{nil} R &= \bigcap \{\mathfrak{A} \lhd R \mid \mathfrak{A} \text{ é um ideal primo}\} \\
\ell\text{-rad}\, R &= \sum \{\mathfrak{A} \lhd R \mid \mathfrak{A} \text{ é um ideal localmente nilpotente}\} \\
\operatorname{Nil} R &= \sum \{\mathfrak{A} \lhd R \mid \mathfrak{A} \text{ é um ideal nil}\} \\
\operatorname{rad} R &= \{y \in R \mid (Ry, \circ) \text{ é um grupo}\}
\end{aligned}$$

Unindo (2.1.5), (2.1.10) e (2.4.8), temos que:

$$\operatorname{nil} R \subseteq \ell\text{-rad}\, R \subseteq \operatorname{Nil} R \subseteq \operatorname{rad} R.$$

Como demonstrado anteriormente, estas inclusões são, em geral, estritas.

Quando R. Baer, J. Levitzki, G. Köthe e N. Jacobson desenvolveram as definições destes radicais, tinham em mente que todos eles gozassem de algumas propriedades comuns. Uma delas é que, no caso em que R é um anel com unidade e artiniano à esquerda, cada um deles é igual ao ideal nilpotente maximal de R.

De fato, suponha que R seja um anel com unidade e artiniano à esquerda. Pela Proposição 2.2.4, $\operatorname{rad} R$ é o ideal nilpotente maximal de R e, portanto, o ideal $(\operatorname{rad} R + \operatorname{nil} R)/\operatorname{nil} R \subseteq R/\operatorname{nil} R$ também é um ideal nilpotente. Mas pela Proposição 2.1.11, $R/\operatorname{nil} R$ não tem ideais nilpotentes não nulos, donde segue que $\operatorname{rad} R \subseteq \operatorname{nil} R$. Segue que $\operatorname{nil} R = \ell\text{-rad}\, R = \operatorname{Nil} R = \operatorname{rad} R$ é o ideal nilpotente maximal de R.

Outra propriedade desejada na definição destes radicais é a mostrada na próxima proposição. Tal propriedade pode ser interpretada como uma versão mais fraca do item (1) do Teorema Principal de Wedderburn (Teorema 2.0.1). Considere nil, ℓ-rad, Nil e rad como operadores na classe dos anéis que associam cada anel R ao anel $\operatorname{nil} R$, $\ell\text{-rad}\, R$, $\operatorname{Nil} R$ e $\operatorname{rad} R$, respectivamente.

Proposição 2.6.1. *Se R é um anel e $\gamma \in \{\operatorname{nil}, \ell\text{-rad}, \operatorname{Nil}, \operatorname{rad}\}$, então $\gamma(R/\gamma(R)) = 0$.*

Demonstração. Os casos onde $\gamma = \operatorname{nil}$ e $\gamma = \operatorname{rad}$ foram demonstrados na Proposição 2.1.12 e na Proposição 2.4.10, respectivamente. A demonstração do caso $\gamma = \operatorname{Nil}$ é trivial: Se $\mathfrak{A}/\operatorname{Nil} R$ é um ideal nil de $R/\operatorname{Nil} R$, para todo $a \in \mathfrak{A}$, $(a+\operatorname{Nil} R)^n = 0$, para algum inteiro positivo n e, portanto, $a^n \in \operatorname{Nil} R$, donde segue que a é nilpotente. Por consequência, $\operatorname{Nil}(R/\operatorname{Nil} R) = 0$. A demonstração do caso $\gamma = \ell$-rad é análoga. □

De maneira independente, S. A. Amitsur e A. G. Kurosh descobriram entre 1952 e 1954 que os chamados radicais concretos tem algumas propriedades em comum e a partir delas formularam uma teoria axiomática para radicais [GW04a, Chapter 2]. Para mais detalhes sobre a teoria geral dos radicais e suas aplicações, consultar [GW04a].

Capítulo 3

Teoria de anéis PI

3.1 Identidades polinomiais

O conceito de identidade polinomial foi introduzido por M. Dehn em um artigo [Deh22] publicado em 1922. Tal artigo trata de um problema de fundamentos de geometria [mcd74, p. 1] e sua conexão com a existência de identidades racionais[1] não universais satisfeitas em anéis de divisão, ou seja, identidades racionais que não são satisfeitas em qualquer anel de divisão. Como exemplos de identidades racionais universais, temos

$$x^{-1}y^{-1} = (yx)^{-1}$$

e

$$(x^{-1} + (y^{-1} - x^{-1})^{-1})^{-1} = x - xyx \quad \text{(identidade de Hua)}$$

Ciente das dificuldades da teoria de identidades racionais, M. Dehn concentrou seu artigo em identidades polinomiais. Para definir uma identidade polinomial, vamos introduzir o conceito de álgebra livre.

Sejam A um anel comutativo com unidade e $\mathbf{X}$ um conjunto não vazio de indeterminadas. Definimos a *A-álgebra (associativa) livre* sobre $\mathbf{X}$, denotada por $A\langle\mathbf{X}\rangle$, como o A-módulo livre com base formada pela unidade $1 \in A$ e as expressões

$$x_1x_2\ldots x_n, \quad \text{onde } n \text{ é um inteiro positivo e } x_1, \ldots, x_n \in \mathbf{X},$$

dotado da multiplicação definida por

$$(x_1 \ldots x_n)(x'_1 \ldots x'_m) = x_1 \ldots x_n x'_1 \ldots x'_m$$

e estendida por linearidade. No caso em que $A = \mathbb{Z}$, o anel $\mathbb{Z}\langle\mathbf{X}\rangle$ é chamado de anel livre sobre $\mathbf{X}$.

[1] Uma definição precisa de identidades racionais foi desenvolvida muito tempo depois, por S. A. Amitsur, em 1966. Em poucas palavras, uma identidade racional é uma identidade que envolve inversos multiplicativos. Para mais detalhes, ver [Row88].

De agora em diante, fixaremos $\mathbf{X}$ um conjunto infinito enumerável de indeterminadas.

Como no caso de polinômios, é essencial definir o grau de um elemento de $A\langle\mathbf{X}\rangle$. Vamos inicialmente definir o *grau* deg e o *i-grau* $\deg_i$, onde i é um inteiro positivo, para os casos mais simples:

- $\deg x_j = 1$ e $\deg_i x_j = \delta_{ij}$, para qualquer $j = 1, 2, \ldots$;
- $\deg a = \deg_i a = 0$, se $a \in A$ é não nulo;
- $\deg 0 = \deg_i 0 = -\infty$;

Em seguida, se $f, g \in A\langle\mathbf{X}\rangle$ são como acima, então definimos $\deg fg = \deg f + \deg g$ e $\deg_i fg = \deg_i f + \deg_i g$. Dessa forma, temos definido o grau dos monômios.

Por fim, se $f = a_1u_1 + \cdots + a_mu_m \in A\langle\mathbf{X}\rangle$, onde $u_1, \ldots, u_n \in A\langle\mathbf{X}\rangle$ são monômios distintos e $a_1, \ldots, a_m \in R$ são não nulos, definimos

$$\deg f = \max\{\deg u_1, \ldots, \deg u_n\} \quad \text{e} \quad \deg_i f = \max\{\deg_i u_1, \ldots, \deg_i u_n\}$$

Exemplo 3.1.1. Se $f = x_1^2x_2x_1 - x_1x_3$, então $\deg f = 4$, $\deg_1 f = 3$ e $\deg_2 f = \deg_3 f = 1$.

Exemplo 3.1.2. Se $f, g \in A\langle\mathbf{X}\rangle$, então $\deg fg = \deg f + \deg g$ e $\deg(f+g) \leq \max\{\deg f, \deg g\}$. Estas igualdades ainda são válidas se substituirmos "deg" por "$\deg_i$".

Dizemos que $f \in A\langle\mathbf{X}\rangle$ é *mônico* se f tiver um monômio de grau máximo acompanhado do coeficiente $1 \in A$.

Para todo $f = f(x_1, \ldots, x_n) \in A\langle\mathbf{X}\rangle$ e toda A-álgebra R, podemos definir uma função $f : R^{(n)} \to R$ que associa cada n-upla ordenada $(a_1, \ldots, a_n) \in R^{(n)}$ ao valor $f(a_1, \ldots, a_n) \in R$, obtido substituindo em $f(x_1, \ldots, x_n)$ cada variável x_i por a_i, $i = 1, \ldots, n$.

Se R é uma A-álgebra e $f = f(x_1, \ldots, x_n) \in A\langle\mathbf{X}\rangle$, dizemos que R *satisfaz* f se, para todos $a_1, \ldots, a_n \in R$, $f(a_1, \ldots, a_n) = 0$. No caso em que f é mônico, dizemos que f é uma *identidade polinomial* de R. Chamaremos de *álgebra PI* aquela álgebra que satisfaz uma identidade polinomial. Analogamente, chamamos de *anel PI* o anel que satisfaz uma identidade polinomial de $\mathbb{Z}\langle\mathbf{X}\rangle$.

Exemplos 3.1.3.

1. Se R é um anel comutativo, então R satisfaz a identidade polinomial $xy - yx \in \mathbb{Z}\langle\mathbf{X}\rangle$. Denotamos $[x, y] = xy - yx$ e chamamos $[x, y]$ de *comutador* de x e y;
2. Se R é um anel nilpotente, então existe um inteiro n tal que R satisfaz a identidade polinomial $x_1 \ldots x_n \in \mathbb{Z}\langle\mathbf{X}\rangle$;
3. Se p é um primo positivo, então $\mathbb{Z}_p$ satisfaz $x^p - x \in \mathbb{Z}\langle\mathbf{X}\rangle$ (Pequeno Teorema de Fermat). Também vale que $\mathbb{Z}_p$ satisfaz $px \in \mathbb{Z}\langle\mathbf{X}\rangle$, mas esta não é uma identidade polinomial, pois px não é mônico.

Exemplo 3.1.4. Seja k um corpo. Se $A \in M_2(k)$, então seu polinômio característico é

$$p(t) = t^2 - \mathrm{tr}(A)t + \det(A),$$

onde $\mathrm{tr}(A) \in k$ é o traço da matriz A. Se $A, B \in M_2(k)$, então sabemos, pelo Teorema de Cayley-Hamilton, que o comutador $[A, B]$ de A e B satisfaz a equação:

$$p([A, B]) = [A, B]^2 - \mathrm{tr}([A, B]) \cdot ([A, B]) + \det([A, B]) \cdot I = 0.$$

Como $\mathrm{tr}([A, B]) = \mathrm{tr}(AB - BA) = \mathrm{tr}(AB) - \mathrm{tr}(BA) = 0$, temos que

$$([A, B])^2 = -\det([A, B]) \cdot I.$$

Em particular, $([A, B])^2$ é uma matriz escalar e, portanto, pertence ao centro de $M_2(k)$, ou seja, para todas as matrizes $A, B, C \in M_2(k)$,

$$[[A, B]^2, C] = (AB - BA)^2C - C(AB - BA)^2 = 0.$$

Em outras palavras, $M_2(k)$ satisfaz a identidade polinomial $[[x, y]^2, z] \in \mathbb{Z}\langle \mathbf{X} \rangle$.

O exemplo anterior é devido a W. Wagner [Wag37] (cujo artigo é considerado por muitos [mcd74, p. 5][Kem91, p. 1] o primeiro importante avanço no desenvolvimento da teoria depois do artigo de M. Dehn). O autor também mostrou que $[[x, y]^2, z]$ é uma identidade polinomial em qualquer álgebra de quartérnios, ou seja, qualquer álgebra simples quadridimensional sobre seu centro. A justificativa moderna desta afirmação é relativamente simples, sendo provada como consequência do Teorema de Kaplansky (ver o comentário após a demonstração do Teorema 3.3.15). Além destes resultados, W. Wagner exibiu identidades polinomiais de anéis de matrizes $n \times n$ sobre corpos e mostrou que se D é um anel de divisão ordenado que satisfaz uma identidade polinomial, então D é comutativo.

Definição 3.1.5. Seja A um anel comutativo com unidade e $f = f(x_1, \ldots, x_n) \in A\langle \mathbf{X} \rangle$, então dizemos que

- f *é homogêneo de grau* d, se f for uma A-combinação linear de monômios de grau d;
- f *é multihomogêneo de multigrau* $(d_1, \ldots, d_n)$, se f for uma A-combinação linear de monômios com i-grau d_i, para todo $i = 1, \ldots, n$;
- f *é multilinear*, se f é multihomogêneo de multigrau $(1, \ldots, 1)$.

Observe que $f = f(x_1, \ldots, x_n) \in A\langle \mathbf{X} \rangle$ é multilinear se, e somente se, existirem $a_\sigma \in A$ para toda permutação $\sigma \in S_n$, tais que

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} a_\sigma \; x_{\sigma(1)} \ldots x_{\sigma(n)}.$$

O próximo teorema mostra que sempre podemos assumir que uma álgebra PI satisfaz uma identidade multilinear.

Teorema 3.1.6. *Suponha que A seja um anel comutativo com unidade e R seja uma A-álgebra que satisfaça uma identidade polinomial de $A\langle \mathbf{X}\rangle$ de grau d. Então R satisfaz uma identidade polinomial multilinear de $A\langle \mathbf{X}\rangle$ com grau no máximo d.*

Demonstração. Se $f = f(x_1, \ldots, x_n) \in A\langle \mathbf{X}\rangle$, $1 \leq i \leq n$ e j são inteiros positivos, então defina

$$\begin{aligned}\Delta_{i,j} f = f(x_1, \ldots, x_{i-1}, x_i + x_j, x_{i+1}, \ldots, x_n) - f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \\ - f(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_n)\end{aligned}$$

Daí se $f = f(x_1, \ldots, x_n) \in A\langle \mathbf{X}\rangle$ e $1 \leq i \leq n$ é um inteiro tal que $\deg_i f > 0$, então são verificadas as seguintes propriedades

i. $\deg_i(\Delta_{i,n+1} f) = \deg_i f - 1$;

ii. Se $j \neq i$, então $\deg_j(\Delta_{i,n+1} f) = \deg_j f$;

iii. $\deg(\Delta_{i,n+1} f) \leq \deg_1(\Delta_{i,n+1} f) + \cdots + \deg_n(\Delta_{i,n+1} f) + \deg_{n+1}(\Delta_{i,n+1} f)$;

iv. Os coeficientes de $\Delta_{i,n+1} f$ são coeficientes de f.

v. Toda A-álgebra que satisfaz f também satisfaz $\Delta_{i,j} f$ para qualquer inteiro positivo j.

Além disso, claramente $\Delta_{i,j}(af + bg) = a\ \Delta_{i,j} f + b\ \Delta_{i,j} g$, onde $f, g \in A\langle \mathbf{X}\rangle$ e $a, b \in A$. Assim, suponha que $f = f(x_1, \ldots, x_n)$ seja mônico, ou seja, que existam monômios distintos $u, u_1, \ldots, u_m$ e $a_1, \ldots, a_m \in A$ tais que u tenha grau maximal e

$$f(x_1, \ldots, x_n) = u + \sum_{t=1}^{m} a_t u_t$$

Seja $(d_1, \ldots, d_n)$ o multigrau de u e considere $\Delta_{1,n+d_1-1} \ldots \Delta_{1,n+2}\Delta_{1,n+1} f = \Delta_1 f$. Se algum monômio u_t tiver 1-grau menor do que d_1, então temos que $\Delta_{1,n+d_1-1} \ldots \Delta_{1,n+1} u_t = 0$, pela propriedade i. e podemos supor sem perda de generalidade que

$$\Delta_1 f = \Delta_{1,n+d_1-1} \ldots \Delta_{1,n+2}\Delta_{1,n+1} u + \sum_{t=1}^{m_1} a_t\ \Delta_{1,n+d_1-1} \ldots \Delta_{1,n+2}\Delta_{1,n+1} u_t,$$

onde u_t tem i-grau maior ou igual d_i.

Como u tem grau maximal, para todo $t = 1, \ldots, m$, se u_t tem multigrau diferente de $(d_1, \ldots, d_n)$, deve haver $j = 1, \ldots, n$ tal que o j-grau de u_t é menor do que d_j. Dessa forma, iterando o parágrafo anterior para as demais variáveis, obteremos operadores $\Delta_1, \Delta_2, \ldots, \Delta_n$ tais que

$$F = \Delta_n \ldots \Delta_1 f = \Delta_n \ldots \Delta_1 u + \sum_{t=1}^{M} a_t\ \Delta_n \ldots \Delta_1 u_t,$$

onde u_t é um monômio de multigrau $(d_1, \ldots, d_n)$ para todo $t = 1, \ldots, M$.

Pelas propriedades i. e ii., $\Delta_1 u, \Delta_1 u_1, \ldots, \Delta_1 u_M$ têm multigrau $(1, d_2, \ldots, d_n, 1, \ldots, 1)$ e, repetindo o argumento para as variáveis $x_2, \ldots, x_n$, temos que $F = \Delta_n \ldots \Delta_1 f$ tem multigrau $(1, \ldots, 1)$ e grau menor ou igual a $\deg f$ (propriedade iii.). Como u é distinto de cada u_j, podemos garantir que existe um monômio mônico em F proveniente de u, donde segue que F é mônico.

Pela propriedade v., toda A-álgebra que satisfaz f também satisfaz F e, portanto, satisfaz uma identidade polinomial multilinear de grau menor ou igual a $\deg f$. □

Exemplo 3.1.7. Suponha que R seja um anel que satisfaz a identidade

$$f(x, y) = xy - 3yx + x^2 \in \mathbb{Z}\langle \mathbf{X} \rangle.$$

Aplicando $\Delta_{x,z}$ a $f(x, y)$, temos que R satisfaz

$$\begin{aligned} \Delta_{x,z}(x, y, z) &= f(x + z, y) - f(x, y) - f(z, y) \\ &= xz + zx, \end{aligned}$$

que é uma identidade multilinear.

Exemplo 3.1.8. Se k é um corpo, então $M_2(k)$ satisfaz $f(x, y, z) = [[x, y]^2, z]$. Aplicando $\Delta_{x,w}$ a f, temos que

$$\Delta_{x,w} f = [[x, y][w, y], z] + [[w, y][x, y], z]$$

E aplicando $\Delta_{y,t}$, temos que

$$\Delta_{y,t}\Delta_{x,w} f = [[x, y][w, t], z] + [[x, t][w, y], z] + [[w, y][x, t], z] + [[w, t][x, y], z],$$

que é uma identidade multilinear de grau 5.

Corolário 3.1.9. *Se R é um anel com unidade e $n > 1$ é um inteiro, então $M_n(R)$ não satisfaz nenhuma identidade polinomial de $\mathbb{Z}\langle \mathbf{X} \rangle$ com grau menor do que $2n$.*

Demonstração. Suponha por absurdo que, para algum inteiro $n > 1$, exista uma identidade polinomial f satisfeita por $M_n(R)$ com grau $\deg f = d < 2n$. Pelo Teorema 3.1.6, podemos assumir que essa identidade é multilinear e podemos assumir que $d = 2n - 1$. De fato, se $f(x_1, \ldots, x_d)$ é multilinear e $d < 2n - 1$, então $g(x_1, \ldots, x_{2n-1}) = f(x_1, \ldots, x_d)x_{d+1} \ldots x_{2n-1}$ é uma identidade multilinear de $M_n(R)$.

Existem $a_\sigma \in R$, para todo $\sigma \in S_{2n-1}$, $\sigma \neq \mathrm{Id}$, tais que

$$f(x_1, \ldots, x_{2n-1}) = x_1 \ldots x_{2n-1} + \sum_{\substack{\sigma \in S_{2n-1} \\ \sigma \neq \mathrm{Id}}} a_\sigma \; x_{\sigma(1)} \ldots x_{\sigma(2n-1)}$$

Fazendo $x_1 = E_{11}, x_3 = E_{22}, \ldots, x_{2n-1} = E_{nn}$, e $x_2 = E_{12}, x_4 = E_{23}, \ldots, x_{2(n-1)} = E_{n-1,n}$ e lembrando que $E_i j \in M_n(R)$ é a matriz elementar (i, j), temos que

$$\begin{aligned} x_1 x_2 \ldots x_{2n-1} &= E_{11}E_{12}E_{22}E_{23} \ldots E_{nn} \\ &= E_{12}E_{22}E_{23} \ldots E_{nn} \\ &= E_{12}E_{23} \ldots E_{nn} = \cdots = E_{1n}E_{nn} = E_{1n} \neq 0 \end{aligned}$$

No entanto, como $x_i x_j = 0$, para todo $i > j$, temos que, para toda permutação $\sigma \in S_{2n-1}$ não trivial, $x_{\sigma(1)} \dots x_{\sigma(2n-1)} = 0$. Segue que, nesse caso, $f(x_1, \dots, x_{2n-1}) \neq 0$, um absurdo. □

O próximo lema ilustra uma das utilidades de identidades polinomiais multilineares.

Lema 3.1.10. *Seja A um anel comutativo com unidade, R uma A-álgebra, $S \subseteq R$ um conjunto gerador de R como A-módulo e $f(x_1, \dots, x_n) \in A\langle \mathbf{X} \rangle$ multilinear. Então f é uma identidade polinomial de R se, e somente se, $f(s_1, \dots, s_n) = 0$ para quaisquer $s_1, \dots, s_n \in S$.*

Demonstração. Trivialmente, se f é identidade polinomial, então $f(s_1, \dots, s_n) = 0$ para quaisquer $s_1, \dots, s_n \in S$.

Reciprocamente, suponha que $f(s_1, \dots, s_n) = 0$ para quaisquer $s_1, \dots, s_n \in S$. Sejam $r_1, \dots, r_n \in R$. Como S é gerador, existe $T = \{t_1, t_2, \dots, t_m\} \subseteq S$ tal que $r_1, \dots, r_n$ são gerados por T. Daí, existe $\{a_j^i \mid i = 1, \dots, n \text{ e } j = 1, \dots, m\}$ tal que $r_i = a_1^i t_1 + a_2^i t_2 + \dots + a_m^i t_m$ para todo i como anteriormente.

Segue que

$$\begin{aligned} f(r_1, \dots, r_n) &= f(a_1^1 t_1 + \dots + a_m^1 t_m, \dots, a_1^n t_1 + \dots + a_m^n t_m) \\ &= \sum_{1 \leq i_1, \dots, i_n \leq m} a_{i_1}^1 \dots a_{i_n}^n f(t_{i_1}, \dots, t_{i_n}) = 0 \end{aligned}$$

e, portanto, f é uma identidade polinomial de R. □

Corolário 3.1.11. *Se R é um anel PI, então o anel de polinômios $R[t]$ também é PI.*

Demonstração. Seja f uma identidade polinomial satisfeita por R. Pelo Teorema 3.1.6, podemos supor que f é multilinear, ou seja, existe um inteiro positivo n e $a_\sigma \in \mathbb{Z}$, para toda permutação não trivial $\sigma \in S_n$, tais que

$$f(x_1, \dots, x_n) = \sum_{\sigma \in S_n} a_\sigma \; x_{\sigma(1)} \dots x_{\sigma(n)}.$$

O conjunto $B = \{rt^i \mid r \in R, \; i = 0, 1, \dots\}$ é um gerador de R como $\mathbb{Z}$-módulo e portanto, pelo Lema 3.1.10, é suficiente mostrar que $f = 0$ quando avaliada nos elementos de B. Se $r_1, \dots, r_n \in R$ e $i_1, \dots, i_n > 0$ são inteiros, então

$$\begin{aligned} f(r_1 t^{i_1}, \dots, r_n t^{i_n}) &= \sum_{\sigma \in S_n} a_\sigma \; r_{\sigma(1)} t^{i_{\sigma(1)}} \dots r_{\sigma(n)} t^{i_{\sigma(n)}} \\ &= \left(\sum_{\sigma \in S_n} a_\sigma \; r_{\sigma(1)} \dots r_{\sigma(n)} \right) t^M = f(r_1, \dots, r_n) t^M \end{aligned}$$

onde $M = i_1 + \dots + i_n$. Daí, como f é identidade de R, segue que $f(r_1 t^{i_1}, \dots, r_n t^{i_n}) = 0$. Conclui-se que f é identidade de $R[t]$. □

Provaremos a seguir um resultado sobre extensões de escalares de álgebras PI. Precisaremos do seguinte lema.

Lema 3.1.12. *Se k é um domínio de integridade (ou seja, um anel comutativo, com unidade e sem divisores de zero) infinito e $p(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ é um polinômio tal que $p(r_1, \ldots, r_n) = 0$ para quaisquer $r_1, \ldots, r_n \in k$, então p é o polinômio nulo.*

Demonstração. Provemos por indução sobre o número n de variáveis do polinômio p. Seja k um domínio de integridade infinito, t uma indeterminada sobre k e $p(t) = \sum_{i=0}^{d} c_i t^i \in p[t]$ tal que $p(a) = 0$ para qualquer $a \in k$. Como k é infinito, podemos tomar $a_1, \ldots, a_{d+1} \in k$ distintos dois a dois e teremos que:

$$\begin{aligned} c_0 + c_1 a_1 + \cdots + c_d {a_1}^d &= 0 \\ c_0 + c_1 a_2 + \cdots + c_d {a_2}^d &= 0 \\ &\vdots \\ c_0 + c_1 a_d + \cdots + c_d {a_d}^d &= 0 \\ c_0 + c_1 a_{d+1} + \cdots + c_d {a_{d+1}}^d &= 0 \end{aligned}$$

ou, em notação matricial,

$$\underbrace{\begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_d \end{pmatrix}}_{=X} \underbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{d+1} \\ {a_1}^2 & {a_2}^2 & \cdots & {a_{d+1}}^2 \\ \vdots & \vdots & & \vdots \\ {a_1}^d & {a_2}^d & \cdots & {a_{d+1}}^d \end{pmatrix}}_{=A} = \begin{pmatrix} 0 & 0 & \cdots & 0 \end{pmatrix} \tag{3.1.13}$$

Observe que o determinante $\det A$ é o determinante de Vandermonde e como os elementos $a_1, \ldots, a_{d+1}$ são distintos, segue que $\det A \neq 0$. Como k é comutativo e com unidade, multiplicando (3.1.13) à direita pela matriz adjunta de A teremos

$$0 = XA(\text{adj } A) = X((\det A) \cdot I) = \begin{pmatrix} (\det A)c_0 & (\det A)c_1 & \cdots & (\det A)c_d \end{pmatrix}$$

E como k é um domínio, segue que $c_0 = c_1 = \cdots = c_d = 0$.

Suponha agora um número n tal que, para todo domínio de integridade infinito k e todo inteiro positivo $m < n$, se o polinômio $p = p(t_1, \ldots, t_m) \in k[t_1, \ldots, t_m]$ é tal que $p(a_1, \ldots, a_m) = 0$, para quaisquer $a_1, \ldots, a_m \in k$, então $p = 0$.

Seja k um domínio de integridade e tome $p(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ como no enunciado. Existem polinômios $p_0, p_1, \ldots, p_s \in k[t_1, \ldots, t_{n-1}]$ tais que

$$p = p_0 + p_1 t_n + \cdots + p_s {t_n}^s.$$

Se $r_1, \ldots, r_{n-1} \in R$, então escreva, para todo $i = 0, \ldots, s$, $\hat{p}_i = p_i(r_1, \ldots, r_{n-1}) \in k$ e observe que o polinômio

$$q = q(t_n) = \hat{p}_0 + \hat{p}_1 t_n + \cdots + \hat{p}_s {t_n}^s \in k[t_n]$$

é tal que, para todo $r \in R$,

$$q(r) = \hat{p}_0 + \hat{p}_1 r + \cdots + \hat{p}_s r^s = p(r_1, \ldots, r_{n-1}, r) = 0.$$

Por hipótese de indução, vale que $q = 0$ e, portanto, para todo $i = 0, \ldots, s$ e todos $r_1, \ldots, r_{n-1}$, vale que $p_i(r_1, \ldots, r_{n-1})$. Novamente por hipótese de indução, vale que $p_0 = p_1 = \cdots = p_s = 0$ e, portanto, $p = 0$.

Por indução, segue o resultado. □

Teorema 3.1.14. *Se k é um corpo infinito, R é uma k-álgebra e $K \subseteq k$ é um corpo que estende k, então R e $R \otimes_k K$ satisfazem as mesmas identidades polinomiais em $k\langle \mathbf{X} \rangle$.*

Demonstração. Se $f \in k\langle \mathbf{X} \rangle$ é uma identidade em $R \otimes_k K$ então claramente é uma identidade em R. Provemos a implicação inversa.

Faremos as identificações $R \equiv R \otimes 1$ e $K \equiv 1 \otimes K$ para simplificar a notação. Seja $B = \{r_\gamma \in R \mid \gamma \in \Gamma\}$ uma base de R como k espaço vetorial e, portanto, uma base de $R \otimes_k K$ como K espaço vetorial (usando a identificação). Considere a família de indeterminadas $T = \{t_{\gamma,i} \mid \gamma \in \Gamma, i = 1, 2, \ldots\}$, tome $f = f(x_1, \ldots, x_n) \in k\langle \mathbf{X} \rangle$ uma identidade polinomial de R e avalie f em $x_i = t_{\gamma_1,i} r_{\gamma_1} + \cdots + t_{\gamma_m,i} r_{\gamma_m}$, para todo $i = 1, \ldots, n$, onde $r_{\gamma_1}, \ldots, r_{\gamma_m}$ são elementos arbitrário da base B. Daí, temos que existe um subconjunto finito $\Gamma' \subseteq \Gamma$ tal que

$$f(x_1, \ldots, x_n) = \sum_{\beta \in \Gamma'} f_\beta(t_{\gamma,i}) r_\beta,$$

onde $f_\beta(t_{\gamma,i})$ é um polinômio de $k[T]$, para todo $\beta \in \Gamma'$. Como f é uma identidade de R, f se anula ao substituirmos as indeterminadas $t_{\gamma,i}$ por valores de k e, portanto, temos que o polinômio $f_\beta(t_{\gamma,i}) \in k[T]$ se anula sob substituições por valores de k, para todo $\beta \in \Gamma'$. Pelo Lema 3.1.12, segue que cada polinômio f_β é o polinômio nulo e, portanto, cada f_β se anula sob valores de K (usando a identificação $K \equiv 1 \otimes K$, de forma que $R \otimes_k K = RK$). Segue que f também é identidade de $R \otimes_k K$. □

3.2 Polinômios centrais

Seja A um anel comutativo e R uma A-álgebra com centro $Z = Z(A)$. Um elemento $f(x_1, \ldots, x_n) \in A\langle \mathbf{X} \rangle$ é dito um *polinômio central* em R se satisfaz as seguintes condições

(a) para quaisquer $r_1, \ldots, r_n \in R$, $f(r_1, \ldots, r_n) \in Z$;

(b) existem $r_1, \ldots, r_n \in R$ tais que $f(r_1, \ldots, r_n) \neq 0$;

(c) o termo constante de $f(r_1, \ldots, r_n)$ é nulo, ou seja, $f(0, \ldots, 0) = 0$.

Enquanto a condição (a) garante que um polinômio central assuma valores no centro, as condições (b) e (c) garantem que identidades polinomiais e constantes não sejam polinômios centrais.

Exemplos 3.2.1. 1. $f(x) = x$ é central em qualquer anel comutativo;

2. Se k é um corpo, então, pelo Exemplo 3.1.4, $f(x, y) = [x, y]^2$ é central em $M_2(k)$. Antes de 1972, este era o único polinômio central conhecido em anéis de matrizes;

3. Se k é um corpo, $R \subseteq M_n(k)$ é o subanel das matrizes triangulares superiores com diagonal nula e $A_1, \ldots, A_{n-1}$ são elementos arbitrários de R, então o produto $A_1 \ldots A_{n-1} = A$ é da forma

$$A = \begin{pmatrix} 0 & \cdots & 0 & a \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix},$$

para algum $a \in k$. Além disso, para todo $B \in R$, $AB = BA = 0$. Em particular, vale que

$$[A_1 \ldots A_{n-1}, B] = 0, \text{ para quaisquer } A_1, \ldots, A_{n-1}, B \in R.$$

É fácil verificar que $f(x_1, \ldots, x_{n-1}) = x_1 \ldots x_{n-1}$ não é uma identidade polinomial de R e, portanto, f é um polinômio central em R.

4. Se k é um corpo, então o subanel $R \subseteq M_n(k)$ das matrizes triangulares superiores não possui polinômios centrais, embora satisfaça identidades polinomiais. De fato, observe inicialmente que o centro de R é o conjunto $Z(R) = \{aI \mid a \in k\}$, o conjunto das matrizes escalares de $M_n(k)$. Se $f = f(x_1, \ldots, x_m)$ satisfaz as condições (a) e (c) da definição de polinômio central, então, para quaisquer $a_1, \ldots, a_m \in R$, segue que

$$f\left(\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \ldots, \begin{pmatrix} a_m & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}\right) = \begin{pmatrix} f(a_1, \ldots, a_m) & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

e, como a última matriz deve ser uma matriz escalar, devemos ter $f(a_1, \ldots, a_m) = 0$, para todos $a_1, \ldots, a_m \in k$, ou seja, f é identidade polinomial de k. Assim, para quaisquer matrizes triangulares superiores $A_1 = (a_{ij}^{(1)}), \ldots, A_m = (a_{ij}^{(m)}) \in R$, temos que

$$\begin{aligned} f(A_1, \ldots, A_m) &= f\left(\begin{pmatrix} a_{11}^{(1)} & & * \\ & \ddots & \\ 0 & & a_{nn}^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} a_{11}^{(m)} & & * \\ & \ddots & \\ 0 & & a_{nn}^{(m)} \end{pmatrix}\right) \\ &= \begin{pmatrix} f(a_{11}^{(1)}, \ldots, a_{11}^{(m)}) & & * \\ & \ddots & \\ 0 & & f(a_{nn}^{(1)}, \ldots, a_{nn}^{(m)}) \end{pmatrix} = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}, \end{aligned}$$

e, portanto, segue que $f(A_1, \ldots, A_m) = 0$, ou seja, f é uma identidade de R.

Em um artigo de 1957, I. Kaplansky propôs doze problemas em teoria de anéis [Kap70]. Tais problemas motivaram linhas de pesquisa em teoria de anéis nos anos subsequentes e um dos problemas propostos nos é de especial interesse: Existem polinômios centrais para anéis de matrizes de ordem maior do que 2 sobre um corpo qualquer? Em 1972-73, E. Formanek [For72] e Yu. P. Razmyslov [Raz73] construíram cada um, de forma independente, um elemento $\mathscr{F}_n \in \mathbb{Z}\langle \mathbf{X} \rangle$, para todo inteiro positivo n, tal que $\mathscr{F}_n$ é um polinômio central em $M_n(k)$, para todo corpo k.

Aqui apresentamos a construção de E. Formanek, seguindo o exposto em [DF04, p. 147-150]. Embora não sejam multilineares, os polinômios obtidos são da forma $\mathscr{F}_n(x, y_1, \ldots, y_n)$, homogêneos de grau $n^2 - n$ na variável x e multilineares nas variáveis $y_1, \ldots, y_n$, de forma que $\mathscr{F}_n$ tem grau n^2.[2] Usaremos polinômios centrais para demonstrar o Teorema 3.4.13 que afirma que todo ideal de um anel PI semiprimo contém ao menos um elemento não nulo do centro. Tal resultado, por sua vez, será usado na demonstração do Teorema 4.1.1, que caracteriza o radical de Jacobson de anéis de polinomiais diferenciais com coeficientes em um anel PI.

Para tal construção precisamos da seguinte definição:

Definição 3.2.2. Sejam u_{ij}, com $1 \leq i, j \leq n$, variáveis independentes, então a matriz $U = (u_{ij}) \in M_n(\mathbb{Z}[\{u_{ij}\}_{1 \leq i,j \leq n}])$ é chamada de *matriz genérica*.

Considere k um corpo qualquer, a matriz genérica $U = (u_{ij})$ e $\overline{k}$ o fecho algébrico do corpo $k(\{u_{ij}\}_{1 \leq i,j \leq n})$. Ao atribuir valores de k para as variáveis u_{ij}, concluímos que os autovalores de U em $\overline{k}$ são todos distintos e, portanto, $U \in M_n(\overline{k})$ é diagonalizável.

Lema 3.2.3. *Seja $n > 2$ um inteiro e suponha que exista $\mathscr{F}(x, y_1, \ldots, y_n) \in \mathbb{Z}\langle \mathbf{X} \rangle$ homogêneo de grau $n^2 - n$ em x, multilinear em $y_1, \ldots, y_n$ e tal que $\mathscr{F}(X, E_{i_1 j_1}, \ldots, E_{i_n j_n})$ é uma matriz escalar de $M_n(\overline{k})$, para quaisquer matrizes elementares $E_{i_1 j_1}, \ldots, E_{i_n j_n} \in M_n(\overline{k})$ e $X \in M_n(\overline{k})$ diagonal. Segue que $\mathscr{F}(X, Y_1, \ldots, Y_n)$ é uma matriz escalar para todos $X, Y_1, \ldots, Y_n \in M_n(k)$.*

Demonstração. Para mostrar que $\mathscr{F} = \mathscr{F}_n$ toma valores sobre as matrizes escalares de $M_n(k)$ (que são as matrizes que compõem o centro de $M_n(k)$) é suficiente mostrar que qualquer especialização $\mathscr{F}(X, Y_1, \ldots, Y_n)$ é uma matriz escalar, onde X é uma matriz genérica e $Y_1, \ldots, Y_n$ são matrizes de $M_n(k)$.

Como X é genérica, X é diagonalizável em $\overline{k}$, ou seja, existe $P \in M_n(\overline{k})$ tal que PXP^{-1} é diagonal. Daí,

$$P\mathscr{F}(X, Y_1, \ldots, Y_n)P^{-1} = \mathscr{F}(PXP^{-1}, PY_1P^{-1}, \ldots, PY_nP^{-1})$$

e, portanto, é suficiente mostrar que $\mathscr{F}(X, Y_1, \ldots, Y_n)$ é uma matriz escalar quando $X \in M_n(\overline{k})$ é diagonal e $Y_1, \ldots, Y_n$ são matrizes arbitrárias de $M_n(\overline{k})$.

[2] Em [Raz73], Yu. P. Razmyslov determina polinômios centrais multilineares de grau $3n^2 - 1$. No entanto, usando o método de Razmyslov, em 1983, P. Halpin [Hal83] também obteve um polinômio central de grau n^2.

Adicionalmente, como as matrizes elementares de $M_n(\overline{k})$ são geradoras de $M_n(\overline{k})$ como $\overline{k}$-espaço vetorial e $\mathscr{F}(x, y_1, \ldots, y_n)$ é multilinear em $y_1, \ldots, y_n$, é suficiente provar que $\mathscr{F}(X, Y_1, \ldots, Y_n)$ é uma matriz escalar sempre que $Y_1, \ldots, Y_n$ são matrizes elementares. De fato, se $A_1, \ldots, A_n \in M_n(\overline{k})$ são arbitrárias, então temos que, para todo $m = 1, \ldots, n$, existem $a_{ij}^{(m)} \in k$, com $1 \leq i, j \leq n$, tais que $A_m = \sum_{1 \leq i,j \leq n} a_{ij}^{(m)} E_{ij}$. Dessa forma, temos que, para todo $X \in M_n(\overline{k})$,

$$\begin{aligned}\mathscr{F}(X, A_1, \ldots, A_n) &= \mathscr{F}\left(X, \sum_{1 \leq i,j \leq n} a_{ij}^{(1)} E_{ij}, \ldots, \sum_{1 \leq i,j \leq n} a_{ij}^{(n)} E_{ij}\right) \\ &= \sum_{i_1, j_1, \ldots, i_n, j_n} a_{i_1 j_1}^{(1)} \ldots a_{i_n j_n}^{(n)} \mathscr{F}(X, E_{i_1 j_1}, \ldots, E_{i_n j_n}), \qquad (3.2.4)\end{aligned}$$

onde os índices $i_1, j_1, \ldots, i_n, j_n$ de (3.2.4) variam entre os inteiros positivos menores ou iguais a n. Supondo que provamos que $\mathscr{F}(X, E_{i_1 j_1}, \ldots, E_{i_n j_n}) \in M_n(\overline{k})$ é uma matriz escalar para todos $i_1, j_1, \ldots, i_n, j_n = 1, \ldots, n$ e $X \in M_n(\overline{k})$ diagonal, temos, por (3.2.4), que $\mathscr{F}(X, A_1, \ldots, A_n)$ é uma matriz escalar para quaisquer matrizes $A_1, \ldots, A_n \in M_n(\overline{k})$ e qualquer $X \in M_n(\overline{k})$ diagonal. □

Teorema 3.2.5 (E. Formanek, 1972)**.** *Se $n \geq 2$ é um inteiro, então existe $\mathscr{F}_n(x, y_1, \ldots, y_n) \in \mathbb{Z}[x, y_1, \ldots, y_n]$ tal que:*

- *$\mathscr{F}_n$ é homogêneo de grau $n^2 - n$ em x e multilinear em $y_1, \ldots, y_n$;*
- *Se k é um corpo, então $\mathscr{F}_n$ é um polinômio central em $M_n(k)$.*

Demonstração. Vamos mostrar inicialmente que existe $\mathscr{F} = \mathscr{F}_n$ satisfazendo as condições do lema anterior. Depois, mostraremos que $\mathscr{F}$ não é uma identidade polinomial e daí, concluiremos que $\mathscr{F}$ é um polinômio central. Fixe as indeterminadas $\{t_1, \ldots, t_n\}$ e construa uma transformação linear

$$\begin{aligned}\varphi : k[t_1, \ldots\ldots, t_{n+1}] &\to k\langle x, y_1, \ldots, y_n\rangle \\ t_1^{\alpha_1} \ldots t_{n+1}^{\alpha_n} &\mapsto x^{\alpha_1} y_1 x^{\alpha_2} \ldots y_{n-1} x^{\alpha_n} y_n x^{\alpha_{n+1}},\end{aligned}$$

e considere

$$g(t_1, \ldots, t_{n+1}) = \prod_{2 \leq i \leq n} (t_1 - t_i)(t_{n+1} - t_i) \prod_{2 \leq j,l \leq n} (t_j - t_l)^2 \qquad (3.2.6)$$

Aplicando a lei distributiva nos produtos de (3.2.6), existem, para toda $(n+1)$-upla de inteiros positivos $a = (a_1, \ldots, a_{n+1})$, inteiros não-negativos N_a (que são nulos, com exceção de uma quantidade finita deles), tais que

$$g(t_1, \ldots, t_{n+1}) = \sum_{a=(a_1, \ldots, a_{n+1})} N_a t_1^{a_1} \ldots t_{n+1}^{a_{n+1}}.$$

Faça $G(x, y_1, \ldots, y_n) = \varphi(g(t_1, \ldots, t_{n+1}))$ e defina

$$\mathscr{F}(x, y_1, \ldots, y_n) = G(x, y_1, \ldots, y_n) + G(x, y_2, y_3, \ldots, y_n, y_1) + \ldots \\ + G(x, y_n, y_1, \ldots, y_{n-1})$$

Segue que $\mathscr{F}$ é homogêneo de grau $n^2 - n$ em x e multilinear em $y_1, \ldots, y_n$. Mostremos agora que se $X \in M_n(\overline{k})$ é diagonal e $Y_1 = E_{i_1 j_1}, \ldots, Y_1 = E_{i_n j_n}$, onde $i_1, j_1, \ldots, i_n, j_n \in \{1, \ldots, n\}$, então $\mathscr{F}(X, Y_1, \ldots, Y_n)$ é uma matriz escalar.

Sejam $v_1, \ldots, v_n \in \overline{k}$ tais que $X = v_1 E_{11} + \cdots + v_n E_{nn}$. Para qualquer $(n+1)$-upla de inteiros positivos $a = (a_1, \ldots, a_{n+1})$,

$$X^{a_1} Y_1 X^{a_2} \ldots X^{a_n} Y_n X^{a_{n+1}} = v_{i_1}^{a_1} \ldots v_{i_n}^{a_n} v_{j_{n+1}}^{a_{n+1}} E_{i_1 j_1} \ldots E_{i_n j_n},$$

uma vez que, para todos $i, j \in \{1, \ldots, n\}$:

$$E_{ij} X = v_1 E_{ij} E_{11} + \cdots + v_n E_{ij} E_{nn} = v_j E_{ij} \\ X E_{ij} = v_1 E_{11} E_{ij} + \cdots + v_n E_{nn} E_{ij} = v_i E_{ij}$$

Daí, temos que

$$\begin{aligned} G(X, Y_1, \ldots, Y_n) &= \varphi(g(t_1, \ldots, t_{n+1})) \\ &= \varphi\left(\sum\nolimits_a N_a t_1^{a_1} \ldots t_{n+1}^{a_{n+1}}\right), \ a = (a_1, \ldots, a_{n+1}) \\ &= \sum\nolimits_a N_a \varphi(t_1^{a_1} \ldots t_{n+1}^{a_{n+1}}) \\ &= \sum\nolimits_a N_a X^{a_1} Y_1 X^{a_2} \ldots X^{a_n} Y_n X^{a_{n+1}} \\ &= \sum\nolimits_a N_a v_{i_1}^{a_1} \ldots v_{i_n}^{a_n} v_{j_{n+1}}^{a_{n+1}} E_{i_1 j_1} \ldots E_{i_n j_n} \\ &= \left(\sum\nolimits_a N_a v_{i_1}^{a_1} \ldots v_{i_n}^{a_n} v_{j_{n+1}}^{a_{n+1}}\right) E_{i_1 j_1} \ldots E_{i_n j_n} \\ &= g(v_{i_1}, \ldots, v_{i_n}, v_{j_n}) E_{i_1 j_1} \ldots E_{i_n j_n}. \end{aligned}$$

Por outro lado, por (3.2.6),

$$g(v_{i_1}, \ldots, v_{i_n}, v_{j_n}) = \prod_{2 \leq r \leq n} (v_{i_1} - v_{i_r})(v_{j_n} - v_{i_r}) \prod_{2 \leq s < t \leq n} (v_{i_s} - v_{i_{i_t}})^2.$$

Logo, temos que $g(v_{i_1}, \ldots, v_{i_n}, v_{j_n}) = 0$ exceto, possivelmente, se $(i_1, \ldots, i_n)$ for uma permutação de $(1, \ldots, n)$ com $j_n = i_1$ e, neste caso, temos que

$$g(v_{i_1}, \ldots, v_{i_n}, v_{j_n}) = \prod_{1 \leq r < s \leq n} (v_s - v_t)^2 = \Delta \in \overline{k}.$$

Além disso, temos que $E_{i_1 j_1} \ldots E_{i_n j_n}$ é diferente de zero se, e somente se, $j_1 = i_2, j_2 = i_3, \ldots j_{n-1} = i_n$, e nesse caso, $E_{i_1 j_1} \ldots E_{i_n j_n} = E_{i_1 j_n}$.

Para fins de simplificação, adotemos a seguinte nomenclatura: Se m é um inteiro positivo então dizemos que uma m-upla de matrizes elementares forma um ciclo se for da forma $(E_{i_1i_2}, E_{i_2i_3}, \ldots, E_{i_mi_1})$, onde $\{i_1, \ldots, i_m\} = \{1, \ldots, m\}$. Assim, unindo as informações obtidas nos parágrafos anteriores, concluímos que

$$G(X, E_{i_1j_1}, \ldots, E_{i_nj_n}) = \begin{cases} \Delta \cdot E_{i_1i_1}, & \text{se } (E_{i_1j_1}, \ldots, E_{i_nj_n}) \text{ forma um ciclo;} \\ 0, & \text{caso contrário} \end{cases}$$

Segue que

$$\mathscr{F}(X, E_{i_1j_1}, \ldots, E_{i_nj_n}) = \begin{cases} \Delta \cdot I, & \text{se } (E_{i_1j_1}, \ldots, E_{i_nj_n}) \text{ forma um ciclo;} \\ 0, & \text{caso contrário} \end{cases}$$

Pelo Lema 3.2.3, $\mathscr{F}(X, Y_1, \ldots, Y_n)$ é uma matriz escalar, quaisquer que sejam $X, Y_1, \ldots, Y_n \in M_n(k)$. Mostremos agora que $\mathscr{F}_n$ não é uma identidade de $M_n(k)$.

Suponha que k seja um corpo infinito e tome n elementos distintos $v_1, \ldots, v_n \in k$. Claramente temos que $\Delta(v_1, \ldots, v_n) \neq 0$. Assim, fazendo $X = v_1E_{11} + \cdots + v_nE_{nn}$, temos que $\mathscr{F}(X, E_{12}, E_{23}, \ldots, E_{n1})$ é uma matriz escalar não nula.

No caso em que k é finito e a característica de k é p, onde p é um primo positivo, observe inicialmente que $M_n(k)$ possui matrizes que são diagonalizáveis como matrizes de $M_n(\overline{k})$, com autovalores em $\overline{k}$ não nulos distintos dois a dois. De fato, tome o polinômio $Q(t)$ dado por

$$Q(t) = \begin{cases} t^n - 1, & \text{se } p \mid n \\ t^n + t - 1, & \text{se } p \nmid n \end{cases}$$

Em qualquer caso, $Q(t)$ é um polinômio cujas n raízes são todas distintas duas a duas, e, portanto, sua matriz companheira tem n autovalores em $\overline{k}$ distintos dois a dois.

Assim, podemos tomar uma matriz $X \in M_n(k)$ com n autovalores em $\overline{k}$ distintos dois a dois e tomar $P \in M_n(\overline{k})$ tal que PXP^{-1} seja diagonal. Fixe $Y_1 = E_{12}, Y_2 = E_{23}, \ldots, Y_n = E_{n1}$ e observe que, pelo caso anterior, $\mathscr{F}(PXP^{-1}, Y_1, Y_2, \ldots, Y_n) \in M_n(\overline{k})$ é uma matriz escalar não nula. Daí:

$$P^{-1}\mathscr{F}(PXP^{-1}, Y_1, \ldots, Y_n)P = \mathscr{F}(X, P^{-1}Y_1P, \ldots, P^{-1}Y_nP) \neq 0.$$

Por outro lado, fazendo $A_1 = P^{-1}Y_1P, \ldots, A_n = P^{-1}Y_nP$, assim como em (3.2.4), existem $a_{ij}^{(m)} \in \overline{k}$, com $1 \leq i, j \leq n$, tais que $A_m = \sum_{1 \leq i,j \leq n} a_{ij}^{(m)} E_{ij}$. Segue que

$$\begin{aligned} \mathscr{F}(X, A_1, \ldots, A_n) &= \mathscr{F}\left(X, \sum_{1 \leq i,j \leq n} a_{ij}^{(1)} E_{ij}, \ldots, \sum_{1 \leq i,j \leq n} a_{ij}^{(n)} E_{ij}\right) \\ &= \sum_{i_1,j_1,\ldots,i_n,j_n} a_{i_1j_1}^{(1)} \ldots a_{i_nj_n}^{(n)} \mathscr{F}(X, E_{i_1j_1}, \ldots, E_{i_nj_n}) \end{aligned} \tag{3.2.7}$$

Como $\mathscr{F}(X, A_1, \ldots, A_n) \neq 0$, pelo menos uma das parcelas de (3.2.7) não é nula, ou seja, existem inteiros positivos $i_1, j_1, \ldots, i_n, j_n \leq n$ tais que $\mathscr{F}(X, E_{i_1 j_1}, \ldots, E_{i_n j_n})$ é uma matriz não nula e escalar, pela construção de $\mathscr{F}$. Está provado assim, que $\mathscr{F}$ é um polinômio central em $M_n(k)$. □

Por fim, encerraremos esta seção com a demonstração de um lema envolvendo polinômios centrais.

Lema 3.2.8 (C. Procesi)**.** *Seja $f(x_1, \ldots, x_m) \in \mathbb{Z}\langle \mathbf{X} \rangle$ um polinômio central em $M_n(R)$, onde R é um anel e $n > 2$ é um inteiro. Segue que f é identidade polinomial de $M_r(R)$, para todo inteiro $2 \leq r < n$.*

Demonstração. Observe que toda matriz $A \in M_r(R)$ possui uma "cópia" em $M_n(R)$ da forma

$$A' = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix},$$

onde cada zero representa uma matriz nula com ordem conveniente. Assim, para quaisquer $A_1, \ldots, A_m \in M_r(R)$:

$$f(A'_1, \ldots, A'_m) = f\left(\begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} A_m & 0 \\ 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} f(A_1, \ldots, A_m) & 0 \\ 0 & 0 \end{pmatrix}$$

Mas, como f é central, $f(A'_1, \ldots, A'_m)$ deve ser uma matriz escalar e, portanto, $f(A_1, \ldots, A_m)$ é a matriz nula. □

3.3 O Teorema de Kaplansky

Assumiremos nesta seção que anéis possuem unidade.

Em 1943, M. Hall [Hal43] mostrou que se D um anel de divisão que satisfaz a identidade polinomial $[[x, y]^2, z] \in \mathbb{Z}\langle \mathbf{X} \rangle$, então D é comutativo ou D é uma álgebra de dimensão 4 sobre seu centro (em outras palavras, uma álgebra de quatérnios sobre seu centro). Em outras palavras, M. Hall mostrou a recíproca de um dos resultados provados por W. Wagner em 1936. Conforme N. Jacobson em [mcd74, p. 4]:

> Durante o verão de 1947, o autor [N. Jacobson] ministrou um curso sobre teoria de estrutura de anéis em Chicago. Durante esta visita, Kaplansky e o autor descobriram o artigo de Hall e levantaram uma questão interessante: Toda álgebra de divisão que satisfaz uma identidade polinomial tem dimensão finita sobre seu centro?[3]

[3]During the summer of 1947, the author lectured on structure theory of rings ar Chicago. During this visit Kaplansky and the author became aware of Hall's paper. This raised an interesting question: Is every PI-division algebra finite dimensional over its center?

No ano seguinte, em 1948, I. Kaplansky demonstra que toda álgebra primitiva à esquerda que satisfaz uma identidade polinomial é isomorfa a uma álgebra de matrizes sobre um anel de divisão de dimensão finita sobre seu centro, o que implica na resposta afirmativa à pergunta de N. Jacobson e I. Kaplansky. Para a demonstração desse resultado, vamos introduzir o conceito de anéis primitivos à esquerda, demonstraremos alguns resultados sobre esse anéis (como o Teorema da Densidade de Jacobson-Chevalley), sobre álgebras centrais simples e sobre subcorpos maximais de anéis de divisão.

3.3.1 Anéis primitivos à esquerda

Seguiremos nesta subseção a exposição de [Lam01, §11].

Um anel não nulo R é dito *primitivo à esquerda* se existe um R-módulo fiel e simples à esquerda. Substituindo as ocorrências da palavra "esquerda" por "direita" na frase anterior obtemos a definição de anéis primitivos à direita. A distinção das duas definições é de fato necessária uma vez que existem anéis primitivos à direita que não o são à esquerda e vice-versa, conforme mostrado por G. Bergman em 1964 [Ber64].

Exemplos 3.3.1.

1. Todo anel simples é um anel primitivo à esquerda e à direita. De fato, como R tem unidade, podemos tomar $\mathfrak{m} \lhd_e R$ maximal. Segue que $M = R/\mathfrak{m}$ é um R-módulo à esquerda simples e, como R é simples, $\operatorname{Ann} M = 0$ e ${}_RM$ é fiel.

2. Um anel comutativo é primitivo à esquerda (resp. à direita) se, e somente se, é um corpo.

3. Se R é um anel e M é um R-módulo à esquerda simples, então $R/\operatorname{Ann}_\ell M$ é um anel primitivo à esquerda, pois M é um $R/\operatorname{Ann}_\ell M$-módulo à esquerda simples e fiel.

4. Seja $D = \mathbb{Q}(x)$ o corpo das funções racionais sobre $\mathbb{Q}$, $\sigma : D \to D$ dada por $\sigma(r(x)) = r(x^2)$ e $R = D[y;\sigma]$. Segue que qualquer subanel de R que contém x e y é primitivo à direita e não é primitivo à esquerda (mais detalhes, ver [Ber64]).

Definição 3.3.2. Se R,S são anéis, então dizemos que o grupo aditivo M é um (R,S)-*bimódulo*, se M é um R-módulo à esquerda, um S-módulo à direita e se, para quaisquer $r \in R$, $s \in S$ e $m \in M$, $r(ms) = (rm)s$.

Para demonstrar o Teorema de Kaplansky usaremos o Teorema da Densidade de Jacobson-Chevalley e, portanto, introduziremos aqui o seguinte conceito. Sejam R,k anéis, V um (R,k)-bimódulo e $E = \operatorname{End} V_k$. Observe que E age em V à esquerda via

$$\begin{aligned} E \times V &\to V \\ (f, v) &\mapsto f(v) \end{aligned}$$

Dizemos que R *age densamente em* V_k se, para todo $f \in E$ e todos $v_1, v_2, \ldots, v_n \in V$ com n inteiro positivo, existe $r \in R$ tal que $rv_i = f(v_i)$ para $i = 1, \ldots, n$.

A nomenclatura justifica-se pela seguinte observação: Seja τ a topologia em E definida pelos abertos básicos

$$\{g \in E \mid g(v_i) = v_i',\ i = 1, 2, \ldots, n\},$$

onde $v_1, \ldots, v_n, v_1', \ldots, v_n \in V$ e n é um inteiro positivo. Considere a função $\varphi : R \to E$ dada por $\varphi(r) = \varphi_r$, onde $\varphi_r : V \to V$ é dada por $\varphi_r(x) = rx$, para todos $r \in R$, $x \in V$. Então $\operatorname{im}\varphi \subseteq E$ é um subespaço topológico denso em E se, e somente se, R age densamente em V_k.

Suponha que R é um anel, V seja um R-módulo à esquerda e considere $k = \operatorname{End}_R V$ visto como anel de operadores à direita em V. Segue que V é um k-módulo via

$$\begin{aligned} V \times k &\to V \\ (v, \phi) &\mapsto v\phi \end{aligned}$$

e adicionalmente, V é um (R, k)-bimódulo.

Lema 3.3.3. *Seja R um anel, ${}_RV$ um R-módulo semissimples, $k = \operatorname{End}_R V$ e $E = \operatorname{End} V_k$. Então qualquer R-submódulo $W \subseteq V$ é um E-submódulo.*

Demonstração. Seja $W' \subseteq V$ tal que $V = W \oplus W'$ e tome $\pi \in k$ a projeção relativa à essa soma direta. Então, para todo $f \in E$, temos que

$$f(W) = f(W\pi) = f(V\pi) = f(V)\pi \subseteq W.$$

Logo, W é um E-submódulo de V. □

Teorema 3.3.4 (da Densidade de Jacobson-Chevalley)**.** *Se R é um anel, ${}_RV$ é um R-módulo semissimples e $k = \operatorname{End}_R V$, então R age densamente em V_k.*

Demonstração. Se n é um inteiro positivo, então $\widetilde{V} = V^n$ é um R-módulo semissimples e

$$\widetilde{k} = \operatorname{End}_R \widetilde{V} = \operatorname{End}_R V^n \simeq M_n(\operatorname{End}_R V) = M_n(k).$$

Como $\widetilde{k}$ age à direita sobre $\widetilde{V}$, por extensão, $M_n(k)$ também age à direita sobre $\widetilde{V}$.

Para todo $f \in E = \operatorname{End} V_k$, defina $\widetilde{f} = (f, \ldots, f) : V^n \to V^n$ e observe que $\widetilde{f} \in \operatorname{End} \widetilde{V}_{\widetilde{k}}$. De fato, se $\widetilde{e} \in \widetilde{k}$, então, tomando $(e_{ij}) \in M_n(k)$ tal que (e_{ij}) represente $\widetilde{e}$, para qualquer $(w_1, \ldots, w_n) \in \widetilde{V}$, segue que

$$\begin{aligned} \widetilde{f}((w_1, \ldots, w_n)\widetilde{e}) &= \widetilde{f}\left(\sum w_i e_{i1}, \ldots, \sum w_i e_{in}\right) \\ &= \left(f\left(\sum w_i e_{i1}\right), \ldots, f\left(\sum w_i e_{in}\right)\right) \\ &= \left(\sum f(w_i) e_{i1}, \ldots, \sum f(w_i) e_{in}\right) \\ &= (\widetilde{f}(w_1, \ldots, w_n))\widetilde{e}. \end{aligned}$$

Se $v_1, \ldots, v_n \in V$ são arbitrários, considere o submódulo $W = R(v_1, \ldots, v_n) \subseteq \widetilde{V}$. Como W é um R-módulo, também é um E-módulo (Lema 3.3.3) e, portanto, $\widetilde{f}(W) \subseteq W$, ou seja, existe $r \in R$ tal que $\widetilde{f}(v_1, \ldots, v_n) = r(v_1, \ldots, v_n)$. □

Corolário 3.3.5. *Sejam R, V, k e $E = \operatorname{End} V_k$ como no Teorema da Densidade. Se V_k é finitamente gerado como um k-módulo à direita, então o homomorfismo $\rho : R \to E$ associado à ação de R em V é sobrejetor.*

Demonstração. Fixe $v_1, \ldots, v_n \in V$ geradores de V como k-módulo à direita e seja $f \in E$. Então, como $f(v_1), \ldots, f(v_n) \in V$, pelo Teorema da Densidade, existe $r \in R$ tal que $rv_i = f(v_i)$, $i = 1, \ldots, n$. Afirmamos que $\rho(r) = f$. De fato, para qualquer $v \in V$, existem $\alpha_1, \ldots, \alpha_n \in k$ tais que $v = v_1\alpha_1 + \cdots + v_n\alpha_n$ e segue que

$$\begin{aligned} rv &= r(v_1\alpha_1 + \cdots + v_n\alpha_n) = (rv_1)\alpha_1 + \cdots + (rv_n)\alpha_n \\ &= f(v_1)\alpha_1 + \cdots + f(v_n)\alpha_n = f(v_1\alpha_1 + \cdots + v_n\alpha_n) = f(v). \end{aligned}$$

□

No caso em que ${}_RV$ é simples, pelo Lema de Schur, $k = \operatorname{End}_R V$ é um anel de divisão e V é um k-espaço vetorial à direita. Isso motiva a seguinte definição:

Definição 3.3.6. Seja R um anel, V um R-módulo à esquerda simples, $k = \operatorname{End}_R V$ e $E = \operatorname{End} V_k$ o conjunto dos operadores lineares do espaço vetorial V_k. Um conjunto $S \subseteq E$ é chamado de *conjunto denso de transformações lineares em V_k* se, para qualquer inteiro positivo n e quaisquer $v_1, \ldots, v_n \in V$ linearmente independentes e $v'_1, \ldots, v'_n \in V$ arbitrários, existe $s \in S$ tal que $s(v_i) = v'_i$, para todo $i = 1, \ldots, n$.

A próxima proposição relaciona conjuntos densos de transformações lineares e a noção de anterior de densidade.

Proposição 3.3.7. *Sejam R um anel, k um anel de divisão, V um (R, k)-bimódulo, defina $E = \operatorname{End} V_k$ e $\rho : R \to E$ o homomorfismo natural associado à ação de R em V. Então R age densamente no espaço vetorial V_k se, e somente se,* $\operatorname{im}\rho \subseteq E$ *é um conjunto denso de transformações lineares do espaço vetorial V_k.*

Demonstração. Se R age densamente em V_k, então, claramente, $\operatorname{im}\rho$ é um conjunto denso de transformações lineares em V_k.

Suponha que $\operatorname{im}\rho$ seja um conjunto denso de transformações lineares em V_k e tome $v_1, \ldots v_n \in V$ e $f \in E$. Seja $\{w_\lambda\}_{\lambda \in B}$ uma base de V como k-espaço. Podemos obter um inteiro positivo t e $w_1, \ldots, w_t \subseteq \{w_\lambda\}_{\lambda \in B}$ tais que os vetores $v_1, \ldots, v_n$ pertençam ao k-espaço gerado por $\{w_1, \ldots, w_t\}$. Daí, como $\{w_1, \ldots, w_t\}$ é linearmente independente, existe $r \in R$ tal que $rw_i = f(w_i)$, para todo $i = 1, \ldots, t$. Segue, pelo mesmo argumento que o Corolário 3.3.5, que $rv_i = f(v_i)$, para todo $i = 1, \ldots, n$. □

Como aplicação do Teorema da Densidade de Jacobson-Chevalley, mostramos a seguinte consequência, que, às vezes, é chamada de Teorema da Densidade.

Teorema 3.3.8 (Classificação dos Anéis Primitivos à esquerda)**.** *Sejam R um anel primitivo à esquerda e ${}_RV$, um R-módulo simples e fiel, defina $k = \operatorname{End}_R V$ e $E = \operatorname{End} V_k$. Segue que R é (isomorfo a) um anel denso de transformações lineares em V_k e*

- *se R é artiniano à esquerda, então* $\dim_k R = n < \infty$ *e $R \simeq M_n(k)$;*

- *se R não for artiniano à esquerda, então para todo inteiro positivo n, existe um subanel $R_n \subseteq R$ que admite um homomorfismo sobrejetor sobre $M_n(k)$.*

Demonstração. Como ${}_RV$ é fiel, o homomorfismo $\rho : R \to E$ é injetor e $R \simeq \operatorname{im}\rho$. Pelo Teorema da Densidade e pela Proposição 3.3.7, $\operatorname{im}\rho$ é um anel denso de transformações lineares em V_k.

Se $\dim_k R = n < \infty$, então, pelo Corolário 3.3.5, ρ é sobrejetor. Assim, $R \simeq \operatorname{im}\rho = E = \operatorname{End} V_k \simeq M_n(k)$ e, em particular, R é artiniano à esquerda.

Se $\dim_k R = \infty$, então tome $\{v_1, v_2, \dots\} \subseteq V$ um conjunto infinito, enumerável e linearmente independente. (sobre k). Para todo inteiro positivo n, defina V_n o k-espaço gerado por $\{v_1, \dots, v_n\}$, $R_n = \{r \in R \mid rV_n \subseteq V_n\}$ e $\mathfrak{A}_n = \{r \in R \mid rV_n = 0\}$. Observe que, para qualquer inteiro positivo n, R_n é um subanel de R, $\mathfrak{A}_n \lhd_e R$ e $\mathfrak{A}_n \lhd R_n$. Além disso, V_n é um $R_n/\mathfrak{A}_n$-módulo fiel e simples através de

$$(r + \mathfrak{A}_n)v = rv, \quad \forall r \in R_n,\ \forall v \in V_n.$$

Como $\dim(V_n)_k = n$, pelo caso anterior, $R_n/\mathfrak{A}_n \simeq M_n(k)$. Além disso, como R age densamente sobre V_k, existe $r_n \in R$ tal que

$$r_n v_1 = r_n v_2 = \cdots = r_n v_n = 0 \quad \text{e} \quad r_n v_{n+1} = v_{n+1} \neq 0.$$

Logo, $r_n \in \mathfrak{A}_n \setminus \mathfrak{A}_{n+1}$ para todo inteiro positivo n e a cadeia $\mathfrak{A}_1 \supseteq \mathfrak{A}_2 \supseteq \dots$ é estritamente descendente. Segue que R não é artiniano à esquerda. □

3.3.2 Álgebras centrais simples

Para as próximas proposições, seguiremos conforme o exposto em [Her68, p. 89-96]. Se R é um anel simples, tomando seu centro $Z = Z(R)$, temos que RZ é um ideal bilateral de R não nulo, e, portanto, $RZ = R$. Segue que, para qualquer $z \in Z$, existe $a \in R$ tal que $az = za = 1$, ou seja, z é inversível (em R). Por fim, observando que, para todo $r \in R$, $rz^{-1} = z^{-1}(zr)z^{-1} = z^{-1}(rz)z^{-1} = z^{-1}r$, e, assim, para todo $z \in Z$, z é inversível em Z. Provamos assim a

Proposição 3.3.9. *Se R é um anel simples, então Z é um corpo.*

Em particular, no caso acima, R é uma Z-álgebra simples. Tal resultado motiva a seguinte definição:

Definição 3.3.10. Seja k um corpo e A uma k-álgebra. Dizemos que A é uma *álgebra central simples* se A for simples e $Z(A) = k \cdot 1 \subseteq A$.

Concluímos, pela Proposição 3.3.9, que todo anel simples é uma álgebra central simples (sobre seu centro).

Proposição 3.3.11. *Se A é uma k-álgebra central simples e B é uma k-álgebra simples contendo k em seu centro, então $A \otimes_k B$ é simples.*

Demonstração. Seja $\mathfrak{A} \neq 0$ um ideal de $A \otimes_k B$ e fixe $\mathscr{B}$ uma base de B. Tomando $u \in \mathfrak{A}$ não nulo, podemos escrever $v = \sum_{i=1}^{n} a_i \otimes b_i$, com $a_1, \ldots, a_n \in A$ e $b_1, \ldots, b_n \in \mathscr{B}$ únicos e podemos definir o comprimento de v como a quantidade dos a_i's que são não nulos. Fixe $v \in \mathfrak{A}$ não nulo e cujo comprimento seja minimal. Podemos supor, sem perda de generalidade que $v = \sum_{i=1}^{n} a_i \otimes b_i$ com a_i não nulo para todo $i = 1, \ldots, n$ (ou seja, n é comprimento de v).

Suponha que $n > 1$. Como A é simples, $Aa_1A = A$, e daí, existe um inteiro positivo m e existem $r_1, \ldots, r_m, s_1, \ldots, s_m \in A$ tais que $1 = r_1a_1s_1 + \cdots + r_ma_1s_m$. Segue que

$$u = \sum_{i=1}^{m} (r_i \otimes 1)v(s_i \otimes 1) = 1 \otimes b_1 + \sum_{i=2}^{n} a_i' \otimes b_i \in \mathfrak{A}$$

para $a_2', \ldots, a_n' \in A$ convenientes. Observe que, para todo $a \in A$, $(a \otimes 1)u - u(a \otimes 1) = \sum_{i=2}^{n} (aa_i' - a_i'a) \otimes b_i \in \mathfrak{A}$ e $(a \otimes 1)u - u(a \otimes 1)$ tem comprimento menor do que n. Pela minimalidade de n segue que $(a \otimes 1)u - u(a \otimes 1) = 0$ e, como os b_i's são linearmente independentes, segue que $aa_i' = a_i'a$, para todo $i = 2, \ldots, n$ e para todo $a \in A$. Como A é central, temos que $a_2, \ldots, a_n \in Z(A) = k \cdot 1$, e, portanto, existem $\alpha_2, \ldots, \alpha_n \in k$ tais que $\alpha_i \cdot 1 = a_i'$, para todo $i = 2, \ldots, n$. Conclui-se que $u = 1 \otimes b_1 + \sum_{i=2}^{n} a_i' \otimes b_i = 1 \otimes b$, onde $b = b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n$. Como os b_i's são linearmente independentes, $b \neq 0$, e daí, $1 \otimes b$ é um elemento de $\mathfrak{A}$ não nulo com comprimento 1, contradizendo a minimalidade de n.

Concluímos que $n = 1$ e existe $a \otimes b \in \mathfrak{A}$ não nulo com $a \in A$ e $b \in \mathscr{B}$. Assim como anteriormente, existem $r_1, \ldots, r_m, s_1, \ldots, s_m \in A$ tais que $1 = r_1as_1 + \cdots + r_mas_m$ e, portanto, $u = \sum_{i=1}^{m} (r_i \otimes 1)(a \otimes b)(s_i \otimes 1) = 1 \otimes b \in \mathfrak{A}$. Como $b \neq 0$ e B é simples, temos que $BbB = B$ e

$$1 \otimes B = 1 \otimes (Bb_1B) \subseteq (1 \otimes B)(1 \otimes b_1)(1 \otimes B) \subseteq \mathfrak{A}.$$

Como $\mathfrak{A}$ é ideal $(A \otimes 1)(1 \otimes B) \subseteq \mathfrak{A}$, e daí segue que $A \otimes_k B \subseteq \mathfrak{A}$. Conclui-se que $A \otimes_k B$ é simples. □

Corolário 3.3.12 (Extensão de escalares)**.** *Se A é uma álgebra central simples sobre o corpo k e K/k é uma extensão de k, então $A \otimes_k K$ é uma K-álgebra central simples.*

Demonstração. Pelo item anterior, basta demonstrar que o centro de $A \otimes_k K$ é o corpo $K \cdot 1$. Seja $Z = Z(A \otimes_k K)$, tome $z \in Z$ e escreva $z = \sum_{i=1}^{n} a_i \otimes b_i$ onde n é inteiro positivo, $a_1, \ldots, a_n \in A$ e $\{b_1, \ldots, b_n\} \subseteq K$ é um conjunto linearmente independente. Então, para todo $a \in A$, $(a \otimes 1)z - z(a \otimes 1) = 0$, ou seja, $\sum_{i=1}^{n} (aa_i - a_ia) \otimes b_i = 0$. Como os b_i's são linearmente independente, segue que $aa_i - a_ia = 0$, para todo $a \in A$, e, portanto, $a_i \in Z(A)$, para todo $i = 1, \ldots, n$. Como A é central, existem $\alpha_1, \ldots \alpha_n \in k$ tais que $\alpha_i \cdot 1 = a_i$, para todo $i = 1, \ldots, n$, e daí

$$z = \sum_{i=1}^{n} a_i \otimes b_i = 1 \otimes \left(\sum_{i=1}^{n} \alpha_i b_i \right) = \left(\sum_{i=1}^{n} \alpha_i b_i \right) (1 \otimes 1) \in K \cdot 1$$

Logo, $Z(A \otimes_k K) \subseteq K \cdot 1$. Como a inclusão inversa é claramente verdadeira, segue que $Z(A \otimes_k K) = K \cdot 1$ e, portanto, $A \otimes_k K$ é uma K-álgebra central simples. □

Antes de demonstrar o teorema de Kaplansky vamos mostrar um teorema sobre anéis de divisão.

Se D é uma álgebra de divisão, então dizemos que um subcorpo $K \subseteq D$ é maximal se, para todo subcorpo $K \subseteq K' \subseteq D$, temos que $K' = K$. Se K é um subcorpo maximal de D, então K contém o centro de D pois, caso contrário, $KZ(D)$ seria um subcorpo que contém propriamente K. O seguinte teorema é uma aplicação da classificação de anéis primitivos à esquerda que ilustra a importância dos subcorpos maximais para determinar a estrutura de anéis de divisão.

Teorema 3.3.13. *Seja D um anel de divisão de divisão com centro k e $K \subseteq D$ um subcorpo maximal de D. Então $D \otimes_k K$ é um anel denso de transformações lineares em D_K. Além disso,*

- *se $\dim_k K = n < \infty$, então $\dim_K D = n$, $\dim_k D = n^2$ e $D \otimes_k K \simeq M_n(K)$;*
- *se $\dim_k K = \infty$, então $\dim_K D = \infty$.*

Demonstração. Defina

$$\operatorname{End}_+ D = \{\varphi : D \to D \mid \varphi(x+y) = \varphi(x) + \varphi(y),\ \forall x, y \in D\}.$$

O conjunto $\operatorname{End}_+ D$ é um anel com as operações de soma e composição de funções usuais. Além disso, para todo $d \in D$, as funções

$$\begin{aligned} R_d : D &\to D & \qquad L_d : D &\to D \\ x &\mapsto xd & x &\mapsto dx \end{aligned}$$

são tais que $R_d, L_d \in \operatorname{End}_+ D$.

Sejam $D_r = \{R_a \mid a \in D\}$, $K_\ell = \{L_b \mid b \in K\}$ e observe que $D_r, K_\ell \subseteq \operatorname{End}_+ D$ são subanéis e que os elementos de D_r comutam com os elementos de K_ℓ. Considere $R = D_r K_\ell$, o subanel gerado pelos elementos da forma $R_a L_b$, com $a \in D$ e $b \in K$. Observe que $D_r x = \{R_a(x) \mid a \in D\} = D$, para qualquer $x \in D$ não nulo, e, portanto, $Rx = D$, donde segue que D é um R-módulo simples. Se $\varphi \in R$ é tal que $\varphi \cdot x = 0$, para todo $x \in D$, então $\varphi(x) = 0$, para todo $x \in D$, e segue que $\varphi = 0$. Logo, D é um R-módulo à esquerda fiel e simples.

Considere $\Delta = \{\varphi \in \operatorname{End}_+ D \mid \ \varphi\psi = \psi\varphi,\ \forall \psi \in R\}$ e observe que $\Delta = \operatorname{End}_R D$. Como $D_r \subseteq R$, se $\varphi \in \Delta$, então $\varphi R_a = R_a \varphi$, para todo $a \in D$, ou seja, para todos $a, x \in D$:

$$\varphi(xa) = \varphi R_a(x) = R_a \varphi(x) = \varphi(x)a.$$

Em particular, se $\widetilde{a} = \varphi(1) \in D$, então, para todo $x \in D$,

$$\varphi(x) = \varphi(1x) = \varphi(1)x = \widetilde{a}x = L_{\widetilde{a}}(x).$$

Logo, $\Delta \subseteq D_\ell = \{L_a \mid a \in D\}$.

Mas, como $K_\ell \subseteq R$, para qualquer $a \in D$, então $L_a \in \Delta$ e $L_b L_a = L_a L_b$, para todo $b \in K$. Segue que

$$ba = L_b L_a(1) = L_a L_b(1) = ab, \text{ para todo } b \in K,$$

ou seja, a comuta com todos os elementos de K e, daí, $K(a) \subseteq D$ é um corpo que contém K. Como K é maximal, $K(a) = K$, ou seja, $a \in K$. Conclui-se, $\Delta \subseteq K_\ell$.

Claramente vale que $K_\ell \subseteq \Delta$ e, portanto, $K_\ell = \Delta = \mathrm{End}_R D$. Estamos nas hipóteses do Teorema 3.3.8, pois, R é primitivo à esquerda com R-módulo fiel e simples D e $K_\ell = \mathrm{End}_R D$. Segue que R é um anel denso de transformações lineares de D_{K_ℓ}. Como K é comutativo, $K_\ell \simeq K$, e, portanto, por extensão, R é anel denso de transformações lineares de D_K.

Observe, finalmente, que $D \otimes_k K$ é simples, pelo Corolário 3.3.12, e que a função

$$\begin{aligned} f : D \otimes_k K &\to D_r K_\ell \\ \sum_i a_i \otimes b_i &\mapsto \sum_i R_{a_i} L_{b_i} \end{aligned}$$

é um homomorfismo de anéis sobrejetor. Conclui-se que f é um isomorfismo de anéis e que $D \otimes_k K$ é um anel denso de transformações lineares de D_K.

Suponha agora que $[K : k] = n < \infty$ e tome $\{b_1, \ldots, b_n\} \subseteq K$ uma base do k-espaço vetorial K. Segue que $\{1 \otimes b_1, \ldots, 1 \otimes b_n\} \subseteq D \otimes_k K$ é uma base do D-espaço vetorial à esquerda ${}_D(D \otimes_k K)$. Como todo ideal à esquerda de $D \otimes_k K$ é um D-subespaço vetorial, segue que toda cadeia de ideais à esquerda de $D \otimes_k K$ é uma cadeia de subespaços vetoriais de ${}_D(D \otimes_k K)$ e, portanto, estabiliza. Segue que $D \otimes_k K$ é artiniano à esquerda. Assim, pelo Teorema 3.3.8, $D \otimes_k K \simeq M_n(K)$, $[D \otimes_k K : K] = n^2$ e $[D : K] = [K : k] = n$.

Se tivermos $[K : k] = \infty$, então $[D : k] = [D : K][K : k] = \infty$. Se tivéssemos $[D : K] < \infty$, então, pelo Teorema 3.3.8, teríamos que $D \otimes_k K \simeq M_m(K)$, para algum inteiro positivo m, e daí, $[D : k] = [D \otimes_k K : K] = m^2$, contradição. Segue que $[K : D] = [D : k] = \infty$. □

Como uma simples aplicação, observe que se A é uma álgebra de divisão central sobre os reais, então, tomando um subcorpo maximal $K \subseteq A$, temos que $[K : \mathbb{R}]$ é um inteiro positivo, ou seja, K é uma extensão finita de $\mathbb{R}$. Sob isomorfismo, a única extensão finita não trivial de $\mathbb{R}$ é $\mathbb{C}$, logo, $[K : \mathbb{R}] = 1$ ou 2, e $[A : \mathbb{R}] = 1$ ou 4. No caso em que $[A : \mathbb{R}] = 1$, claramente $A \simeq \mathbb{R}$, enquanto que, no caso em que $[A : \mathbb{R}] = 4$, mostra-se (usando, por exemplo, o *Teorema de Noether-Skolem*[4]) que A é isomorfo à álgebra real dos quatérnios (este é o clássico *Teorema de Frobenius*[5]).

Estamos em condições de provar o celebrado Teorema de Kaplansky. Seguiremos a exposição de [DF04, p. 153,154]

[4] *Teorema de Noether-Skolem*: Seja R um anel simples, artiniano à esquerda e com centro k e sejam $A, B \subseteq R$ subálgebras simples de dimensões finitas que contêm k. Se f é um isomorfismo de A em B que é a função identidade nos elementos de k, então existe $x \in R$ inversível tal que $f(a) = x^{-1}ax$.

[5] Embora a demonstração de ambos os resultados sejam simples com as ferramentas aqui desenvolvidas, elas fugiriam de nosso objetivo. As demonstrações pode ser encontradas em [Her68, p. 99, p. 102]

Teorema 3.3.14 (I. Kaplansky, 1948)**.** *Seja R um anel PI primitivo à esquerda. Então $R \simeq M_n(D)$, onde D é uma álgebra de divisão de dimensão finita sobre seu centro. Equivalentemente, R é uma álgebra central simples de dimensão finita.*

Demonstração. Seja $f \in \mathbb{Z}\langle \mathbf{X} \rangle$, uma identidade polinomial satisfeita por R. Podemos supor que f é da forma

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)},$$

para convenientes $a_\sigma \in \mathbb{Z}$, para todo $\sigma \in S_n$, e n inteiro positivo.

Como R é primitivo à esquerda, podemos tomar o R-módulo à esquerda fiel e simples ${}_RM$. Defina $D = \mathrm{End}_R\, M$ e segue que D é um anel de divisão.

Suponha que R não seja artiniano à esquerda. Daí, pelo Teorema 3.3.8, existe um subanel $S \subseteq R$ e um homomorfismo sobrejetor $\varphi : S \to M_n(D)$. Dessa forma, para quaisquer $A_1, \ldots, A_n \in M_n(D)$, existem $r_1, \ldots, r_n \in S$ tais que $\varphi(r_i) = A_i$, para todo $i = 1, \ldots, n$, e temos que $f(A_1, \ldots, A_n) = \varphi(f(r_1, \ldots, r_n)) = 0$. Segue que f é uma identidade polinomial de $M_n(R)$, um absurdo, visto que $\deg f = n$ e, pelo Corolário 3.1.9, $M_n(D)$ não satisfaz identidades polinomiais de grau menor do que $2n$. Assim, R é artiniano à esquerda e $R \simeq M_r(D)$, para algum inteiro positivo r.

Seja $k = Z(D)$ e $K \subset D$ um subcorpo maximal. Como podemos considerar D como um subanel de $M_r(D)$, D satisfaz f. Além disso, $D \otimes_k K$ também satisfaz f. De fato, como $\mathbb{Z}$-álgebra, $D \otimes_k K$ é gerada pelos elementos $T = \{a \otimes b \mid a \in D, b \in K\}$. Assim, se $a_1, \ldots, a_n \in D$, $b_1, \ldots, b_n \in K$ são elementos quaisquer, então

$$\begin{aligned}
f(a_1 \otimes b_1, \ldots, a_n \otimes b_n) &= \sum_{\sigma \in S_n} \alpha_\sigma (a_{\sigma(1)} \otimes b_{\sigma(1)}) \ldots (a_{\sigma(n)} \otimes b_{\sigma(n)}) \\
&= \sum_{\sigma \in S_n} \alpha_\sigma (a_{\sigma(1)} \ldots a_{\sigma(n)}) \otimes (b_{\sigma(1)} \ldots b_{\sigma(n)}) \\
&= \sum_{\sigma \in S_n} \alpha_\sigma (a_{\sigma(1)} \ldots a_{\sigma(n)}) \otimes (b_1 \ldots b_n) \\
&= \left(\sum_{\sigma \in S_n} \alpha_\sigma a_{\sigma(1)} \ldots a_{\sigma(n)} \right) \otimes (b_1 \ldots b_n) \\
&= f(a_1, \ldots, a_n) \otimes (b_1 \ldots b_n) = 0
\end{aligned}$$

Logo, pelo Lema 3.1.10, f é identidade de $D \otimes_k K$.

Pelo Teorema 3.3.13, $D \otimes_k K$ é um anel denso de transformações lineares em D_K e, como anteriormente, $D \otimes_k K$ é artiniano à esquerda e, portanto, finitamente gerado sobre seu centro K e existe inteiro positivo s tal que $[D : k] = [D \otimes_k K : K] = s^2$. □

Como consequência do Teorema de Kaplansky, temos o seguinte corolário.

Teorema 3.3.15. *Se R uma álgebra central simples com $Z(R) = k$, então existe um inteiro positivo n tal que*

(1) $\dim_k R = n^2$;

(2) *R não satisfaz identidades polinomiais de grau menor do que $2n$;*

(3) *$\mathscr{F}_n = \mathscr{F}_n(x, y_1, \ldots, y_n)$ é um polinômio central em R;*

(4) *Para todo inteiro positivo $m > n$, $\mathscr{F}_m = \mathscr{F}(x, y_1, \ldots, y_m)$ é identidade polinomial de R.*

Demonstração. Seja D um anel de divisão e r um inteiro positivo tal que $R \simeq M_r(D)$. Defina $Z = Z(D)$ o centro de D e observe que

$$k = Z(R) \simeq Z(M_r(D)) = Z(D) \cdot I_r \simeq Z$$

Podemos, portanto, considerar que D é uma k-álgebra central simples. Se K é um subcorpo maximal de D que contém k, então existe um inteiro positivo s tal que $D \otimes_k K \simeq M_s(K)$. Segue que

$$R \otimes_k K \simeq M_r(D) \otimes_k K \simeq M_r(D \otimes_k K) \simeq M_r(M_s(K)) \simeq M_{rs}(K)$$

e, portanto, $\dim_k R = \dim_K(R \otimes_k K) = r^2 s^2$. Defina $n = rs$ e temos o item (1) do corolário.

Assim como na demonstração do Teorema de Kaplansky, se f é multilinear e R satisfaz f, então $R \otimes_k K$ satisfaz f. Mas $R \otimes_k K \simeq M_n(R)$, logo, pelo Corolário 3.1.9, $\deg f \geq 2n$.

Para demonstrar os itens (3) e (4) observe que, pelo Teorema 3.2.5, $\mathscr{F}_n$ é um polinômio central em $M_n(F)$, para qualquer corpo F. Daí, temos os seguintes casos dependendo da cardinalidade de k:

- Se k é finito, então D é finito uma vez que D é uma k-álgebra de dimensão finita e, pelo Teorema de Wedderburn[6], segue que D é um corpo e $R \simeq M_n(D)$. Temos, portanto, que $\mathscr{F}_n$ é polinômio central em R.

- Se k é infinito e, por consequência, D é um anel de divisão infinito, então, pelo Teorema 3.1.14, R e $R \otimes_k K \simeq M_n(K)$ satisfazem as mesmas identidades polinomiais em $K\langle \mathbf{X} \rangle$. Em particular, segue que $[\mathscr{F}_n(x, y_1, \ldots, y_n), z]$ é identidade de R, pois é identidade de $M_n(K)$, mas $\mathscr{F}_n$ não é, donde segue que $\mathscr{F}_n$ é polinômio central em R.

Em ambos os casos, temos que R satisfaz as identidades polinomiais de $M_n(F)$ sobre algum corpo F. Se m é um inteiro tal que $n < m$, então $\mathscr{F}_m$ é um polinômio central no anel $M_m(F)$ e, pelo Teorema 3.2.8, é uma identidade polinomial de $M_n(F)$. Segue que $\mathscr{F}_m$ é uma identidade de R para todo inteiro $m > n$, concluindo a demonstração. □

Como simples consequência, mostremos o seguinte resultado demonstrado originalmente em [Wag37]: Se R é uma álgebra simples sobre seu centro k tal que $\dim_k R = 4$, então $[[x, y]^2, z]$ é identidade polinomial de R. Pela demonstração do Teorema 3.3.15, existe um corpo F que estende k e tal que $R \otimes_k F$ satisfaz as identidades polinomiais de $M_n(F)$, onde $n^2 = \dim_k R = 2^2$. Segue que $R \otimes_k F$ satisfaz as identidades polinomiais de $M_2(F)$ e, portanto, satisfaz $[[x, y]^2, z]$. Como podemos identificar R com o subanel $R \otimes 1 \subseteq R \otimes_k F$, temos que R também satisfaz esta identidade polinomial.

[6] *Teorema de Wedderburn:* Todo domínio finito é um corpo [Her68, p. 102]

3.4 Anéis PI primos e semiprimos

O objetivo desta seção é demonstrar que qualquer ideal não nulo de um anel PI semiprimo tem intersecção não nula com o centro. Tal resultado será usado para estudar o radical de Jacobson de anéis de polinômios diferenciais no Capítulo 4. Para auxiliar o estudo de anéis semiprimos, vamos introduzir o conceito de produto subdireto.

O Teorema de Wedderburn-Artin nos fornece uma classificação precisa da classe dos anéis semissimples, uma classe relativamente limitada de anéis; basta observar que existem diversos anéis que não são sequer escritos como um produto direto de ideais não nulos. Aumentar o "alcance" de teoremas como o Teorema de Wedderburn-Artin exige, portanto, generalizar a forma como um anel é escrito em função de outros anéis, preferencialmente em função daqueles que tenham uma estrutura mais familiar. É isso o que temos em mente ao definirmos produtos subdiretos.

Definição 3.4.1. Seja R um anel e $(R_\lambda)_{\lambda\in\Lambda}$ uma família não vazia de anéis. Dizemos que R é um *produto subdireto* de $(R_\lambda)_{\lambda\in\Lambda}$ se existir um homomorfismo injetor

$$\varphi : R \to \prod_{\lambda\in\Lambda} R_\lambda$$

tal que as projeções $\varphi_\lambda : R \to R_\lambda$ (ou seja, as respectivas composições da função φ com as projeções associadas ao produto $\prod_{\lambda\in\Lambda} R_\lambda$) são sobrejetoras para todo $\lambda \in \Lambda$.

A função φ também é chamada de representação subdireta de R. Facilmente verifica-se que, na notação da definição anterior, R é produto subdireto de $(R_\lambda)_{\lambda\in\Lambda}$ se, e somente se, para cada $\lambda \in \Lambda$ existirem homomorfismos sobrejetores $\varphi_\lambda : R \to R_\lambda$ tais que $\bigcap_{\lambda\in\Lambda} \ker\varphi_\lambda = 0$.

Conforme veremos após a demonstração do próximo lema, representações subdiretas são úteis para estudar anéis semiprimos e anéis semiprimitivos.

Lema 3.4.2. *Se R é um anel com unidade, então* $\operatorname{rad} R$ *é a intersecção dos ideais $\mathfrak{A} \subseteq R$ tais que $R/\mathfrak{A}$ é primitivo à esquerda.*

Demonstração. Pelo Corolário 2.2.2, é suficiente mostrar que o conjunto dos ideais $\mathfrak{A}$ tais que $R/\mathfrak{A}$ é primitivo à esquerda é igual ao conjunto dos anuladores de R-módulos à esquerda simples.

Tome um ideal $\mathfrak{A}$ tal que $R/\mathfrak{A}$ seja primitivo à esquerda e considere M um $R/\mathfrak{A}$-módulo à esquerda fiel e simples. Segue que M é um R-módulo simples com estrutura dada por

$$r \cdot m = (r + \mathfrak{A})m,$$

para todo $r \in R$ e todo $m \in M$. Além disso, $r \in \operatorname{Ann}_\ell({}_R M)$ se, e somente se, para todo $m \in M$, $(r + \mathfrak{A})m = rm = 0$. Como ${}_{R/\mathfrak{A}}M$ é um módulo fiel, segue que $r \in \operatorname{Ann}_\ell({}_R M)$ se, e somente se, $r + \mathfrak{A} = 0 + \mathfrak{A}$, ou seja, $r \in \mathfrak{A}$. Temos, portanto, que $\mathfrak{A} = \operatorname{Ann}_\ell({}_R M)$, ou seja, $\mathfrak{A}$ é o anulador de um R-módulo à esquerda simples.

Tome agora M, um R-módulo à esquerda simples e $\mathfrak{A} = \operatorname{Ann}_\ell({}_RM)$. Podemos considerar M como um $R/\mathfrak{A}$-módulo à esquerda através da estrutura dada por

$$(r + \mathfrak{A}) \cdot m = rm,$$

para todo $r \in R$ e todo $m \in M$. Tal estrutura está bem definida, uma vez que, se $r, r' \in R$ são tais que $r + \mathfrak{A} = r' + \mathfrak{A}$, então $r - r' \in \mathfrak{A}$ e $(r + \mathfrak{A}) - (r' + \mathfrak{A}) = (r - r') + \mathfrak{A} = 0 + \mathfrak{A}$. Além disso, ${}_{R/\mathfrak{A}}M$ é um módulo fiel e simples, donde segue que $R/\mathfrak{A}$ é primitivo à esquerda. □

Teorema 3.4.3. *Se R é um anel, então:*

- *R é semiprimo se, e somente se, R é produto subdireto de anéis primos;*
- *se adicionalmente R tem unidade, R é semiprimitivo se, e somente se, R é produto subdireto de anéis primitivos à esquerda.*

Demonstração. Suponha que R seja um anel semiprimo (respectivamente, semiprimitivo, no caso em que R é anel com unidade) e considere a família $(\mathfrak{A}_\lambda)_{\lambda\in\Lambda}$ de todos os ideais de R tais que $R/\mathfrak{A}_\lambda$ é um anel primo (respectivamente, é um anel primitivo à esquerda). Definindo, para todo $\lambda \in \Lambda$, $\varphi_\lambda : R \to R/\mathfrak{A}_\lambda$ como as projeções canônicas, temos que $\bigcap_{\lambda\in\Lambda} \ker\varphi_\lambda = \bigcap_{\lambda\in\Lambda} \mathfrak{A}_\lambda = 0$, pois

$$\bigcap_{\lambda\in\Lambda} \mathfrak{A}_\lambda = \operatorname{nil} R \quad \left(\text{respectivamente, } \bigcap_{\lambda\in\Lambda} \mathfrak{A}_\lambda = \operatorname{rad} R\right).$$

Portanto, R é representação subdireta da família $(R/\mathfrak{A}_\lambda)_{\lambda\in\Lambda}$ de ideais primos (respectivamente, primitivos à esquerda).

Reciprocamente, suponha que R seja produto subdireto da família $(R_\lambda)_{\lambda\in\Lambda}$ de anéis primos (respectivamente, primitivos à esquerda). Para cada $\lambda \in \Lambda$, podemos tomar um homomorfismo sobrejetor $\varphi_\lambda : R \to R_\lambda$ de forma que $\bigcap_{\lambda\in\Lambda} \ker\varphi_\lambda = 0$. Assim, $R/\ker\varphi_\lambda \simeq R_\lambda$ é um anel primo (respectivamente, primitivo à esquerda) e

$$\operatorname{nil} R \subseteq \bigcap_{\lambda\in\Lambda} \ker\varphi_\lambda = 0, \quad \left(\text{respectivamente, } \operatorname{rad} R \subseteq \bigcap_{\lambda\in\Lambda} \ker\varphi_\lambda = 0\right),$$

donde segue que R é semiprimo (respectivamente, semiprimitivo). □

Também vale observar que, se R é um anel PI que é produto subdireto da família $(R_\lambda)_{\lambda\in\Lambda}$, então cada R_λ é um anel PI. De fato, tome, para cada $\lambda \in \Lambda$, um homomorfismo $\varphi_\lambda : R \to R_\lambda$ sobrejetor. Daí, como φ_λ é um homomorfismo de anéis, em particular é um homomorfismo de grupos abelianos, ou seja, de $\mathbb{Z}$-módulos. Suponha agora que $p(x_1, \ldots, x_n) \in \mathbb{Z}\langle\mathbf{X}\rangle$ seja uma identidade de R e $a_1, \ldots, a_n \in R_\lambda$ são arbitrários. Como φ_λ é sobrejetora, existem $r_1, \ldots, r_n \in R$ tais que $\varphi_\lambda(r_i) = a_i$, para todo $i = 1, \ldots, n$. Segue que

$$\begin{aligned} p(a_1, \ldots, a_n) &= p(\varphi_\lambda(r_1), \ldots, \varphi_\lambda(r_n)) \\ &= \varphi_\lambda(p(r_1, \ldots, r_n)) = \varphi_\lambda(0) = 0 \end{aligned}$$

Voltando ao contexto de anéis PI, provaremos que a conjectura de Köthe (Problema 2.1.2) é verificada nesta classe. Se R é um anel PI, defina o *PI-grau* de R como o menor grau de uma identidade satisfeita por R. Em vista do Teorema 3.1.6, podemos assumir que todo anel PI satisfaz uma identidade multilinear cujo grau é o PI-grau do anel. Se R é um anel PI não nulo, então o menor PI-grau possível é 2 e, nesse caso, existe um inteiro m tal que R satisfaz $xy - myx = 0$.

Lema 3.4.4. *Seja R é um anel primo, $\mathfrak{A} \lhd_e R$ e considere* $\operatorname{Ann}_r \mathfrak{A} = \{r \in R \mid \mathfrak{A}r = 0\}$. *Segue que*

(1) $M = \mathfrak{A} \cap \operatorname{Ann}_r \mathfrak{A}$ *é um ideal de* $\mathfrak{A}$*;*

(2) $\mathfrak{A}/M$ *é um anel primo.*

Demonstração. (1) $\mathfrak{A}M = 0$, pois $M \subseteq \operatorname{Ann}_r \mathfrak{A}$ e, portanto, $\mathfrak{A}M \subseteq M$. Além disso, $\mathfrak{A}(M\mathfrak{A}) = 0$ e, portanto, $M\mathfrak{A} \subseteq \operatorname{Ann}_r \mathfrak{A}$. Como claramente $M\mathfrak{A} \subseteq \mathfrak{A}$, segue que $M\mathfrak{A} \subseteq \mathfrak{A} \cap \operatorname{Ann}_r \mathfrak{A} = M$. Logo, M é ideal de $\mathfrak{A}$.

(2) Sejam I, J ideais de $\mathfrak{A}$ tais que $IJ \subseteq M$. Daí, $\mathfrak{A}I + \mathfrak{A}IR$ e $\mathfrak{A}J + \mathfrak{A}JR$ são ideais de R e

$$(\mathfrak{A}I + \mathfrak{A}IR)(\mathfrak{A}J + \mathfrak{A}JR) \subseteq \mathfrak{A}IJ + \mathfrak{A}IJR \subseteq \mathfrak{A}M + \mathfrak{A}MR = 0.$$

Como R é primo, podemos sem perda de generalidade supor que $\mathfrak{A}I + \mathfrak{A}IR = 0$ e segue que $I \subseteq M$. Conclui-se que $\mathfrak{A}/M$ é um anel primo. □

Teorema 3.4.5 (J. Levitzki)**.** *Se R é um anel PI primo não nulo, então R não tem ideais à esquerda nil.*

Demonstração. Procederemos por indução sobre o PI-grau. Suponha que R seja um anel com PI-grau igual a 2, ou seja, $xy - myx$ é identidade de R para algum inteiro m. Seja um ideal à esquerda nil $\mathfrak{A} \neq 0$ e seja $a \in \mathfrak{A}$ tal que $a^2 = 0$ e $a \neq 0$. Se $Ra = 0$, então $\mathbb{Z}a$ é um ideal à esquerda não nulo e nilpotente de R. Se $Ra \neq 0$, então $aRa = na^2R = 0$ e $Ra + \mathbb{Z}a$ é um ideal à esquerda não nulo e nilpotente de R. De qualquer forma, existe ideal à esquerda $\mathfrak{B} \subseteq R$ nilpotente não nulo, um absurdo, visto que R é primo. Logo, R não tem ideais à esquerda nil.

Suponha um inteiro $n \geq 2$ tal que todo anel PI primo com PI-grau menor ou igual a n não tenha ideais à esquerda nil. Tome R um anel PI primo com PI-grau $n+1$ e suponha que exista $N \lhd_e R$ não nulo e nil. Segue que existe $a \in N$ não nulo e tal que $a^2 = 0$. Defina $\mathfrak{A} = Ra$ e, pelo Lema 3.4.4, temos que $R_1 = \mathfrak{A}/(\mathfrak{A} \cap \operatorname{Ann}_r \mathfrak{A})$ é um anel primo. Mostremos que R_1 é um anel PI com PI-grau igual a n. Seja $f(x_1, \ldots, x_{n+1}) \in \mathbb{Z}\langle \mathbf{X} \rangle$ uma identidade multilinear de R de grau $n+1$. Existem $g(x_2, \ldots, x_{n+1}), h(x_1, \ldots, x_{n+1}) \in \mathbb{Z}\langle \mathbf{X} \rangle$ multilineares tais que

$$f(x_1, \ldots, x_{n+1}) = x_1 g(x_2, \ldots, x_{n+1}) + h(x_1, \ldots, x_{n+1}),$$

g é mônico e os monômios de h não começam com a indeterminada x_1. Dessa forma, para quaisquer $r_1, \ldots, r_{n+1} \in R$,

$$\begin{aligned} 0 = f(ar_1, r_2a, \ldots, r_{n+1}a) &= ar_1g(r_2a, \ldots, r_{n+1}a) + h(ar_1, r_2a, \ldots, r_{n+1}a) \\ &= ar_1g(r_2a, \ldots, r_{n+1}a), \end{aligned}$$

uma vez que, como nenhum dos monômios de h começa com x_1, sempre ocorre o produto a^2 nas parcelas de $h(ar_1, r_2a, \ldots, r_{n+1}a)$. Segue que $aRg(a_1, \ldots, a_n) = 0$, para quaisquer $a_1, \ldots, a_n \in \mathfrak{A}$. Substituindo ar_1 por a, temos também que $ag(a_1, \ldots, a_n) = 0$, para quaisquer $a_1, \ldots, a_n \in \mathfrak{A}$. Lembrando que o ideal gerado pelo elemento $b \in R$ é dado por

$$\mathrm{id}\langle b\rangle = RbR + Rb + bR + \mathbb{Z}b,$$

concluímos que, para quaisquer $a_1, \ldots, a_n \in gtA$, $\mathrm{id}\langle a\rangle\,\mathrm{id}\langle g(a_1, \ldots, a_n)\rangle = 0$. Como R é primo e $a \neq 0$, temos que $g(a_1, \ldots, a_n) = 0$, para quaisquer $a_1, \ldots, a_n \in \mathfrak{A}$. Segue que $\mathfrak{A}$ é PI com PI-grau menor ou igual a n e, por consequência, R_1 também o é.

Se R_1 fosse não nulo, pela hipótese de indução, R_1 não tem ideais à esquerda nil. Por outro lado, como $\mathfrak{A} \subseteq N$, $\mathfrak{A}$ é nil e, portanto, R_1 também é nil. Segue que $R_1 = 0$ e $\mathfrak{A} \subseteq \mathrm{Ann}_r\,\mathfrak{A}$. Assim, $0 = \mathfrak{A}^2 = RaRa$ e, como R é um anel primo, $Ra = 0$, donde segue que $\mathrm{id}\langle a\rangle^2 = 0$. Como R é primo, segue que $a = 0$, uma contradição. Concluímos que R não possui ideais nil à esquerda não nulos.

Pelo princípio da indução finita, concluímos a demonstração do teorema. □

Corolário 3.4.6. *Se R é um anel PI e semiprimo, então R não tem ideais à esquerda nil não nulos.*

Demonstração. Seja $(R_\lambda)_{\lambda\in\Lambda}$ uma família de anéis primos tais que R seja um produto subdireto de $(R_\lambda)_{\lambda\in\Lambda}$ e considere os homomorfismos sobrejetores associados $\phi_\lambda : R \to R_\lambda$, $\lambda \in \Lambda$. Se $\mathfrak{A}$ é um ideal à esquerda de R, então, para todo $\lambda \in \Lambda$, $\phi_\lambda(\mathfrak{A})$ é um ideal à esquerda nil de R_λ e, pelo Teorema 3.4.5, segue que $\phi_\lambda(\mathfrak{A}) = 0$. Logo, $\mathfrak{A} \subseteq \bigcap_{\lambda\in\Lambda} \ker\phi_\lambda = 0$ e, portanto, $\mathfrak{A} = 0$. □

Corolário 3.4.7. *Se R é um anel PI e $\mathfrak{A} \subseteq R$ é um ideal à esquerda nil, então $\mathfrak{A} \subseteq \mathrm{nil}\,R$. Em particular, se $\mathfrak{A}, \mathfrak{B} \subseteq R$ são ideais à esquerda nil, então $\mathfrak{A} + \mathfrak{B}$ é um ideal à esquerda nil, ou seja, R satisfaz a conjectura de Köthe.*

Demonstração. Se $\mathfrak{A} \lhd_e R$ é nil, então $\mathfrak{A}' = \mathfrak{A} + \mathrm{nil}\,R$ é um ideal à esquerda nil que contêm $\mathrm{nil}\,R$. Se $\mathfrak{A}'$ contém propriamente $\mathrm{nil}\,R$, então $R/\mathrm{nil}\,R$ possui ideais à esquerda nil não nulos. Como $R/\mathrm{nil}\,R$ é um anel PI semiprimo, isto não pode acontecer e, portanto, $\mathfrak{A}+\mathrm{nil}\,R = \mathrm{nil}\,R$, ou seja, $\mathfrak{A} \subseteq \mathrm{nil}\,R$.

Para a segunda parte, basta observar que, se $\mathfrak{A}, \mathfrak{B} \subseteq R$ são ideais à esquerda nil, então $\mathfrak{A} + \mathfrak{B} \subseteq \mathrm{nil}\,R$ e, portanto, $\mathfrak{A} + \mathfrak{B}$ é nil. □

Em suma, se R é um anel PI, então $\mathrm{nil}\,R$ é um ideal nil que contém todos os ideais à esquerda nil. Segue o seguinte corolário:

Corolário 3.4.8. *Se R é um anel PI, então* $\operatorname{nil} R$ *é um ideal nil maximal que é igual à soma dos ideais à esquerda nil de R (alternativamente, à direita). Em particular,* $\operatorname{nil} R \supseteq \operatorname{Nil} R$*, ou seja,* $\operatorname{nil} R = \ell\text{-rad}\, R = \operatorname{Nil} R$.

Como consequência, um anel PI é semiprimo se, e somente se, não possui ideais nil não nulos. Antes de prosseguir, lembremos a seguinte definição.

Definição 3.4.9. Se R é um anel e t uma indeterminada que comuta com os elementos de R, então definimos $R[[t]]$, o *anel das séries de potências formais*, como o anel dos elementos $a_0 + a_1t + a_2t^2 + \ldots$, com adição e multiplicação compatível com o (sub)anel de polinômios $R[t] \subseteq R[[t]]$.

Lema 3.4.10. (1) *Se R é um anel comutativo com unidade e $R[t]$ é o anel de polinômios na indeterminada central t, então um polinômio $p(x) = a_0 + a_1t + \cdots + a_nt^n$ é inversível se, e somente se, a_0 é inversível e a_i é nilpotente, para $i = 1, \ldots, n$;*

(2) *Se R é um anel com unidade, e $a_0, a_1, \ldots a_n \in R$ comutam entre si, então o polinômio $p(x) = a_0 + a_1t + \cdots + a_nt^n$ é inversível se, e somente se, a_0 é inversível e a_i é nilpotente, para $i = 1, \ldots, n$.*

Demonstração. Se a e u são elementos de um anel comutativo qualquer tais que a é nilpotente e u é inversível, então $a + u$ é inversível. De fato, como a é nilpotente, a pertence ao radical de Jacobson e $1 + au^{-1}$ é inversível, donde segue que $a + u = u(1 + au^{-1})$ é inversível.

Suponha que R seja um anel comutativo e com unidade e que os elementos $a_0, a_1, \ldots, a_n \in R$ são tais que a_0 é inversível e a_i é nilpotente para $i = 1, \ldots, n$. Daí, cada elemento $a_1t, a_2t^2 \ldots, a_nt^n$ é nilpotente e, como $R[t]$ é comutativo, $a_1t + a_2t^2 + \cdots + a_nt^n$ é nilpotente, donde segue que $p(t) = a_0 + a_1t + \cdots + a_nt^n$ é inversível aplicando o parágrafo anterior com $a = a_0$ e $u = a_1t + \cdots + a_nt^n$.

Para a recíproca, consideramos inicialmente o caso em que R é um domónio de integridade. Neste caso, demonstrar que os elementos inversíveis de $R[t]$ são os elementos inversíveis de R. Assim, tome um polinômio $p(t) = a_0 + a_1t + \cdots + a_nt^n \in R[t]$ inversível e seja $q(t) = b_0b_1t + \cdots + b_mt^m$, $b_m \neq 0$, o inverso de $p(t)$. De $p(t)q(t) = 1$ obtemos imediatamente que $a_0b_0 = 1$ e $a_nb_m = 0$, donde segue que a_0 é inversível e $a_n = 0$, pois $b_m \neq 0$. Novamente, de $p(t)q(t) = 1$ segue que $a_{n-1}b_m = 0$ e, portanto, $a_{n-1} = 0$. Prosseguindo dessa forma, temos que $a_1, \ldots, a_n = 0$ e, portanto, segue o resultado.

Suponha agora que R seja um anel comutativo arbitrário e tome um polinômio $p(t) = a_0 + a_1t + \cdots + a_nt^n$ que seja inversível. Tomando $\mathfrak{p} \subseteq R$ um ideal primo de R, temos que o anel $\overline{R} = R/\mathfrak{p}$ é um anel primo comutativo e, portanto, é um domínio de integridade. Definindo $\overline{a_i} = a_i + \mathfrak{p} \in R/\mathfrak{p}$, temos que o polinômio $\overline{p}(t) = \overline{a_0} + \overline{a_1}t + \cdots + \overline{a_n}t^n \in \overline{R}[t]$ é inversível e, pelo parágrafo anterior, segue que $\overline{a_i} = \overline{0}$ para $i = 1, \ldots, n$. Provamos, portanto, que $a_1, \ldots, a_n \in \mathfrak{p}$ para todo ideal primo $\mathfrak{p} \subseteq R$, ou seja, $a_1, \ldots, a_n \in \operatorname{nil} R$, donde segue que $a_1, \ldots, a_n$ são nilpotentes, completando a demonstração de (1).

Para demonstrar a afirmação (2), suponha que R seja um anel com unidade arbitrário e que $a_0, a_1, \ldots, a_n \in R$ são elementos que comutam entre si. Defina o polinômio $p(t) = a_0 + a_1t + \cdots + a_nt^n$ e suponha que $p(t)$ seja inversível em $R[t]$. Como feito anteriormente,

podemos concluir que a_0 é inversível. Defina R_0 o subanel de R gerado pelos elementos $a_0, a_0^{-1}, a_1, \ldots, a_n$. Claramente, R_0 é um anel comutativo e $p(t) \in R_0[t] \subseteq R_0[[t]]$. Como a_0 é inversível, temos que $p(t)$ é inversível em $R_0[[t]]$. De fato, observe que, fazendo $q(t) = \sum_{i=0}^{\infty} b_i t^i \in R[[t]]$, e supondo $p(t)q(t) = 1$, obtemos as equações:

$$\begin{aligned}
a_0 b_0 = 1 &\iff b_0 = a_0^{-1} \\
a_0 b_1 + a_1 b_0 = 0 &\iff b_1 = -a_0^{-1} a_1 b_0 \\
a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 &\iff b_2 = -a_0^{-1}(a_1 b_1 + a_2 b_0) \\
&\cdots \\
a_0 b_\ell + a_1 b_{\ell-1} + \cdots + a_\ell b_0 = 0 &\iff b_\ell = -a_0^{-1}(a_1 b_{\ell-1} + a_2 b_{\ell-2} + \cdots + a_\ell b_0)
\end{aligned}$$

Daí, definindo b_ℓ para todo inteiro $\ell \geq 0$ recursivamente como acima, temos que $q(t) \in R_0[[t]]$ e $p(t)q(t) = 1$.

Segue que, $q(t) = (p(t))^{-1} \in R_0[[t]] \cap R[t] = R_0[t]$, ou seja, $p(t)$ é inversível em $R_0[t]$. Como $R_0[t]$ é comutativo, segue pelo item (1) que a_0 é inversível e $a_1, \ldots, a_n$ são nilpotentes.

Como a implicação inversa é trivial, temos o resultado estabelecido. □

Teorema 3.4.11 (S. A. Amitsur [Ami56])**.** *Se R é um anel com unidade tal que* $\operatorname{Nil} R = 0$ *(ou seja, R não possui ideais nil não nulos), então o anel de polinômios $R[t]$ é semiprimitivo.*

Demonstração. Assumindo que $R[t]$ é semiprimitivo, isto é, $\operatorname{rad}(R[t]) \neq 0$, mostraremos que R possui um ideal nil não nulo, donde teremos que $\operatorname{Nil} R \neq 0$. Se n é o menor inteiro positivo tal que existe um polinômio de grau n em $\operatorname{rad}(R[t])$, então considere o conjunto

$$\mathfrak{A} = \{a \in R \mid \text{existe polinômio de grau } n \text{ em } \operatorname{rad}(R[t]) \text{ com coeficiente líder } a\} \cup \{0\}.$$

Temos que $\mathfrak{A}$ é um ideal de R. Tome $a \in \mathfrak{A}$ e um polinômio $p(t) = at^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \operatorname{rad}(R[t])$. Como $ap(t)$ e $p(t)a$ são polinômios de $\mathfrak{A}$ cujos graus são menores ou iguais a n e que contêm o monômio $a^2 t^n$, temos que $[a, p(t)] = ap(t) - p(t)a \in \mathfrak{A}$ é um polinômio de grau menor do que n. Portanto, $[a, p(t)] = \sum_{i=0}^{n-1} [a, a_i] t^i = 0$ e concluímos que $aa_i = a_i a$, para cada $i = 0, 1, \ldots, n-1$. Pelo mesmo argumento, para todo $i = 0, 1, \ldots, n-1$, o polinômio $[a_i, p(t)]$ tem grau menor do que n e pertence a $\operatorname{rad}(R[t])$, donde segue que $a_i a_j = a_j a_i$, para todos $i, j = 0, 1, \ldots, n-1$. Como $p(t)$ é um elemento do radical, segue que $1 - tp(t)$ é inversível em $R[t]$ e satisfaz as condições do item (2) do Lema 3.4.10, donde segue que a é nilpotente. Concluímos que $\mathfrak{A}$ é um ideal nil de R. Por contraposição, segue o resultado desejado. □

Pelo Corolário 3.4.6, podemos aplicar o Teorema 3.4.11 para anéis PI semiprimos, donde obtemos o seguinte corolário:

Corolário 3.4.12. *Se R é um anel PI, com unidade e semiprimo, então $R[t]$ é um anel semiprimitivo.*

Teorema 3.4.13. *Se R é um anel PI semiprimo, então todo ideal não nulo de R tem intersecção não nula com seu centro.*

Demonstração. Mostremos inicialmente que podemos reduzir a demonstração para o caso em que R é um anel com unidade. Suponha demonstrado o teorema para esse caso e tome S um anel PI sem unidade. Existe, como construído na demonstração do Lema 2.5.1, uma multiplicação sobre o grupo aditivo $S^{\#} = S \oplus \mathbb{Z}$ de forma que $S^{\#}$ seja um anel com unidade, S é um ideal de $S^{\#}$ e $S^{\#}/S$ é isomorfo a $\mathbb{Z}$. Daí:

- *$S^{\#}$ satisfaz uma identidade polinomial:* Se $p(x_1, \ldots, x_n)$ é identidade de S, então $p([x_1, y_1], \ldots, [x_n, y_n])$ é identidade polinomial de $S^{\#}$, pois, para quaisquer $s_1, s_2 \in S^{\#}$, $[s_1 + S, s_2 + S] = [s_1, s_2] + S = 0 + S$. Portanto, se $r_1, \ldots, r_n, s_1, \ldots, s_n \in S^{\#}$, então $[r_1, s_1], \ldots, [r_n, s_n] \in S$ e $p([r_1, s_1], \ldots, [r_n, s_n]) = 0$;

- *$S^{\#}$ não tem ideais nil não nulos:* Se existir $\mathfrak{A}^{\#} \subseteq S^{\#}$ ideal nil, então $(\mathfrak{A}^{\#} + S)/S$ é um ideal nil de $S^{\#}/S$ e, como $\mathbb{Z}$ não tem ideais nil não nulos, segue que $\mathfrak{A}^{\#} \subseteq S$. Assim, segue que $\mathfrak{A}^{\#} = 0$, pois S não possui ideais nil não nulos.

Segue que $S^{\#}$ satisfaz as hipóteses do teorema. Se $\mathfrak{A}$ é um ideal de S, então verifica-se facilmente que $\mathfrak{A} \oplus 0$ é um ideal de $S^{\#}$ e, portanto, segue que $(\mathfrak{A} \oplus 0) \cap Z(S^{\#}) \neq 0$. Tomando $(x, 0) \in (\mathfrak{A} \oplus 0) \cap Z(S^{\#})$ não nulo, temos que $x \in \mathfrak{A}$ é um elemento não nulo tal que, para todo $y \in S$,

$$(xy, 0) = (x, 0)(y, 0) = (y, 0)(x, 0) = (yx, 0) \Rightarrow xy = yx$$

Segue que $x \in Z(S)$ e temos demonstrado o teorema no caso geral.

Em suma, podemos assumir que R é um anel PI, com unidade e semiprimo. Vamos agora reduzir a demonstração para o caso em que R é um anel PI, com unidade e é adicionalmente semiprimitivo.

Suponha demonstrado o teorema para anéis semiprimitivos e considere R um anel PI, com unidade e semiprimo com centro Z e tome $\mathfrak{A}$ um ideal não nulo de R. Segue que $R[t]$ é um anel com unidade que satisfaz uma identidade polinomial (Corolário 3.1.11), semiprimitivo (Corolário 3.4.12), com centro $Z[t]$ e tal que $\mathfrak{A}[t]$ é um ideal de $R[t]$. Assim, $(\mathfrak{A} \cap Z)[t] = \mathfrak{A}[t] \cap Z[t]$ é não nulo e, portanto, $\mathfrak{A} \cap Z \neq 0$, demonstrando o teorema como originalmente enunciado.

Iremos supor, portanto, que R é um anel semiprimitivo com unidade e que satisfaz uma identidade polinomial de grau d. Seja $\phi : R \to \prod_{\lambda \in \Lambda} R_\lambda$ uma representação subdireta de R, onde R_λ é um anel primitivo à esquerda para todo $\lambda \in \Lambda$. Cada R_λ é uma álgebra central simples de dimensão ${n_\lambda}^2$, pelo Corolário 3.3.15. Ainda pelo Corolário 3.3.15, temos que $2n_\lambda \leq d$, para todo $\lambda \in \Lambda$, ou seja, o conjunto dos inteiros n_λ, com $\lambda \in \Lambda$, é limitado superiormente.

Tome $\mathfrak{A} \subseteq R$ um ideal e observe que as projeções relativas à representação subdireta $\phi_\lambda : R \to R_\lambda$, $\lambda \in \Lambda$, são sobrejetoras e, portanto, $\phi_\lambda(\mathfrak{A})$ é um ideal de R_λ para todo $\lambda \in \Lambda$. Como cada R_λ é simples, temos que $\phi_\lambda(\mathfrak{A})$ é igual a 0 ou igual a R_λ. Tome n o maior inteiro n_λ dentre aqueles tais que $\phi_\lambda(\mathfrak{A}) = R_\lambda$ e considere o polinômio central $\mathscr{F}_n \in \mathbb{Z}\langle \mathbf{X} \rangle$ do Teorema 3.2.5. Pelo Teorema 3.3.15, $\mathscr{F}_n$ é um polinômio central em todas as álgebras centrais simples de dimensão n^2. Analisando a imagem do polinômio $\mathscr{F}_n$ quando avaliado em valores de $\phi_\lambda(\mathfrak{A}) \subseteq R_\lambda$, para todo $\lambda \in \Lambda$, temos os seguintes casos:

- $n_\lambda < n$: A imagem é zero, pois $\mathscr{F}_n$ é identidade polinomial de R_λ (item (4) do Teorema 3.3.15);
- $n_\lambda = n$: Os elementos da imagem são todos centrais em R_λ;
- $n_\lambda > n$: A imagem é zero, pois, pela maximalidade de n, $\phi_\lambda(\mathfrak{A}) = 0$.

Podemos concluir que os valores do polinômio $\mathscr{F}_n$ quando avaliado em $\phi(\mathfrak{A})$ são todos centrais em $\phi(R)$ e, como ϕ é injetora, concluímos que os valores de $\mathscr{F}_n$ quando avaliado em $\mathfrak{A}$ são todos centrais em R. Além disso, se $\lambda \in \Lambda$ é tal que $\phi_\lambda(\mathfrak{A}) = R_\lambda$, então, como $\mathscr{F}_n$ é central em R_λ, existem elementos centrais não nulos de $\mathscr{F}_n$ quando avaliada em valores de R_λ e, portanto, existem valores centrais não nulos de $\mathscr{F}_n$ quando avaliada em valores de $\mathfrak{A}$. Tais valores são elementos não nulos de $\mathfrak{A} \cap Z(R)$, donde segue que $\mathfrak{A} \cap Z(R) \neq 0$. □

O Teorema 3.4.13 é central na demonstração do Teorema 4.1.1 e é a principal motivação para os tópicos da teoria de anéis PI aqui selecionados.

Capítulo 4

O radical de Jacobson do anel de polinômios diferenciais

No Teorema 2.5.3, mostramos que se R é um anel e δ é um derivação, então o radical de $R[x;\delta]$ é igual a $N[x;\delta]$, onde N é um ideal de R tal que $\delta(N) \subseteq N$. No artigo original de M. Ferrero et al, os autores mostram que no caso em que R é um anel comutativo, então N é um ideal nil. Se $\delta = 0$, então, pelo teorema de Amitsur, N é um ideal nil. É sabido [Smo15], no entanto, que existe R tal que N não é um ideal nil. O objetivo desta seção é estudar o ideal N em alguns casos particulares. Na Seção 4.1, demonstramos que o ideal N é nil quando R satisfaz uma identidade polinomial. Em seguida, abordamos o problema de mostrar que $R[x;\delta]$ é localmente nilpotente quando R é localmente nilpotente e satisfaz uma identidade polinomial. Na Seção 4.2 fazemos uma abordagem ingênua, sem a hipótese de que R é um anel PI, de modo a motivar algumas definições da Seção 4.3, onde desenvolvemos algumas noções combinatórias, e concluímos a resolução do problema na Seção 4.4. Se $\delta = 0$ e R é comutativo, pelo Teorema de Snapper[1], N é igual ao radical de Köthe. Encerrando a Seção 4.4, mostramos com um exemplo que não é possível generalizar este teorema para $R[x;\delta]$, onde R é um anel PI, e mostramos que se R é um anel PI e adicionalmente é uma álgebra sobre um corpo de característica zero, então $\operatorname{rad}(R[x;\delta]) = (\operatorname{Nil} R)[x;\delta]$.

4.1 Anéis de polinômios diferenciais sobre anéis PI

Teorema 4.1.1. *Se R é um anel PI e $\delta : R \to R$ é um derivação de R, então $S = R \cap \operatorname{rad}(R[x;\delta])$ é um ideal nil de R tal que $\delta(S) \subseteq S$ e $\operatorname{rad}(R[x;\delta]) = S[x;\delta]$.*

Demonstração. Pelo Teorema 2.5.3, basta provar que S é um ideal nil ou, equivalentemente, que $S \subseteq N$, onde $N = \operatorname{Nil} R$. Notando adicionalmente que o anel semiprimo R/N não tem ideais nil não nulos, mostrar que S é nil é equivalente a mostrar que $\overline{S} = (S+N)/N$ é o ideal nulo.

[1] *Teorema*[E. Snapper][Lam01, 5.1, p. 67] Se R um anel comutativo com unidade, então $\operatorname{rad}(R[t]) = (\operatorname{Nil} R)[t] = \operatorname{Nil}(R[t])$.

Suponha por contradição que $\overline{S}$ não é o ideal nulo. Pelo Teorema 3.4.13, podemos tomar um elemento não nulo $a \in S \setminus N$ tal que $a \in Z(R/N)$. Mostraremos que a é nilpotente, donde seguirá que o conjunto $(a\mathbb{Z} + aR + N)/N$ será um ideal nil não nulo de R/N, um absurdo.

Como $a \in S$, temos que $ax \in \mathrm{rad}(R[x;\delta])$ e, portanto, existe $f(x) \in R[x;\delta]$ tal que

$$f(x) + ax + f(x)ax = 0 \tag{4.1.2}$$
$$f(x) + ax + axf(x) = 0 \tag{4.1.3}$$

Escrevendo $f(x) = \sum_{i=0}^{n} b_i x^i$, de (4.1.2) concluímos que $b_0 = 0$. Além disso, de (4.1.3), temos que

$$\begin{aligned} 0 &= \sum_{i=0}^{n} b_i x^i + ax + ax\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} b_i x^i + ax + \sum_{i=0}^{n} a(xb_i)x^i \\ &= \sum_{i=0}^{n} b_i x^i + ax + \sum_{i=0}^{n} a\delta(b_i)x^i + \sum_{i=1}^{n+1} ab_{i-1}x^i \\ &= b_0 a\delta(b_0) + (b_1 + a + a\delta(b_1) + ab_0)x + \sum_{i=2}^{n}(b_i + a\delta(b_i) + ab_{i-1})x^i + ab_n x^{n+1} \end{aligned}$$

Igualando os coeficientes, obtemos as seguintes equações:

$$ab_n = 0 \tag{4.1.4}$$
$$b_i + a\delta(b_i) + ab_{i-1} = 0,\ i = 2, \ldots, n \tag{4.1.5}$$
$$b_1 + a + a\delta(b_1) = 0 \tag{4.1.6}$$

Para mostrar que $a \in N$, provaremos o seguinte passo intermediário:

$$a^j b_{n-j+1} \in N,\ j = 1, \ldots, n.$$

Mostremos por indução sobre j (definindo $a^j b_{n-j+1} = 0$, se $j > n$). Se $j = 1$, então $ab_n = 0 \in N$. Da mesma forma, se $j > n$, então $a^{j+1}b_{n-j+2} = 0 \in N$. Para tratar o caso $1 < j \leq n$, tome $m \in \{2, \ldots, n\}$, suponha que $a^j b_{n-j+1} =\in N$ para todo $j < m$ e provemos que $a^m b_{n-m+1} \in N$.

Tomando (4.1.5) com $i = n - m + 2$ e multiplicando à esquerda por a^{m-1}, temos que

$$\begin{aligned} &\underbrace{a^{m-1}b_{n-m+2}}_{\in N} + a^m\delta(b_{n-m+2}) + a^m b_{n-m+1} = 0 \in N \Rightarrow \\ &\Rightarrow a^m\delta(b_{n-m+2}) + a^m b_{n-m+1} \in N \end{aligned} \tag{4.1.7}$$

Para provar o resultado, é suficiente mostrar que $a^m\delta(b_{n-m+2}) \in N$. De (4.1.2) e (4.1.3) obtemos que $xaf(x) = f(x)xa$ e, usando a equação (1.0.3), temos que

$$0 = f(x)ax - axf(x) = \left(\sum_{i=0}^{n} b_i x^i ax\right) - \left(\sum_{i=0}^{n} axb_i x^i\right)$$
$$= \left(\sum_{i=0}^{n} b_i x^i ax\right) - \left(\sum_{i=0}^{n} a\delta(b_i)x^i + \sum_{i=1}^{n+1} ab_{i-1}x^i\right)$$
$$0 = \sum_{i=0}^{n}\sum_{\ell=0}^{i} \binom{i}{\ell} b_i \delta^{\ell}(a) x^{i-\ell+1} - \left(\sum_{i=0}^{n} a\delta(b_i)x^i + \sum_{i=1}^{n+1} ab_{i-1}x^i\right) \tag{4.1.8}$$

Igualando em (4.1.8) os coeficientes que acompanham x^{n-m+2}, temos que:

$$0 = \left(\sum_{i=n-m+1}^{n} \binom{i}{i-(n-m)-1} b_i \delta^{i-(n-m)-1}(a)\right) - (a\delta(b_{n-m+2}) + ab_{n-m+1})$$
$$= b_{n-m+1}a + \binom{n-m+2}{2} b_{n-m+2}\delta(a) + \cdots +$$
$$+ \binom{n-1}{m-2} b_{n-1}\delta^{m-2}(a) + \binom{n}{m-1} b_n \delta^{m-1}(a) - a\delta(b_{n-m+2}) - ab_{n-m+1} \tag{4.1.9}$$

Observe que a primeira e a última parcela de (4.1.9) formam o termo $[b_{n-m+1}, a]$ e, como $a + N \in Z(R/N)$, temos que $[b_{n-m+1}, a] \in N$. Além disso, pela hipótese de indução, $a^{m-1}b_n, a^{m-1}b_{n-1}, \ldots, a^{m-1}b_{n-m+2} \in N$, e portanto, multiplicando (4.1.9) por a^{m-1} à esquerda, segue que $a^m\delta(b_{n-m+2}) \in N$. Usando isso e (4.1.7) provamos como desejado que $a^m b_{n-m+1} \in N$.

Multiplicando (4.1.6) por a^n à esquerda e observando que $a^n b_1 = a^j b_{n-j+1}$ para $j = n$, donde segue que $a^n b_1 \in N$, temos que

$$\underbrace{a^n b_1}_{\in N} + a^{n+1} + a^{n+1}\delta(b_1) = 0 \in N \Rightarrow$$
$$\Rightarrow a^{n+1} + a^{n+1}\delta(b_1) \in N$$

e, por fim, resta provar que $a^{n+1}\delta(b_1) \in N$. Para tal, igualando os coeficientes que acompanham x em (4.1.8), temos que:

$$0 = \left(\sum_{i=1}^{n} b_i \delta^i(a)\right) - (a\delta(b_1) + ab_0)$$
$$= b_1\delta(a) + b_2\delta^2(a) + \cdots + b_n\delta^n(a) - a\delta(b_1) \tag{4.1.10}$$

Multiplicando (4.1.10) por a^n à esquerda, e usando o fato que $a^n b_1, a^n b_2, \ldots, a^n b_n \in N$, segue que

$$\underbrace{a^n b_1}_{\in N}\delta(a) + \underbrace{a^n b_2}_{\in N}\delta^2(a) + \cdots + \underbrace{a^n b_n}_{\in N}\delta^n(a) - a^{n+1}\delta(b_1) \in N \Rightarrow$$
$$\Rightarrow a^{n+1}\delta(b_1) \in N$$

Temos, portanto, que $a^{n+1} \in N$ e, em particular, segue que a é um elemento nilpotente. □

Como caso particular do Teorema 4.1.1, temos a seguinte proposição originalmente demonstrada em [TWC07, p. 976]:

Corolário 4.1.11. *Se R é um anel PI com* $\operatorname{Nil} R = 0$ *e $\delta : R \to R$ é uma derivação, então* $\operatorname{rad}(R[x;\delta]) = 0$.

4.2 Anéis de polinômios diferenciais sobre anéis localmente nilpotentes: abordagem ingênua

Suponha que R seja um anel PI localmente nilpotente e $\delta : R \to R$ seja uma derivação. Para provar que $R[x;\delta]$ é um anel localmente nilpotente basta tomar um inteiro positivo m, um conjunto arbitrário $S = \{p_1(x), \ldots, p_m(x)\} \subseteq R[x;\delta]$ e provar o subanel gerado por S é nilpotente. Para isso, é suficiente mostrar que existe um inteiro não negativo N tal que $S^{N+1} = 0$, ou seja, que qualquer produto de $N+1$ elementos de S é igual a zero. Tome k o maior grau de todos os polinômios de S. Como cada elemento de $R[x;\delta]$ se escreve de maneira única da forma

$$c_0 + c_1 x + \cdots + c_r x^r,$$

onde $c_0, c_1 \ldots, c_r \in R$ e $0 \leq r \leq k$ é um inteiro, existe um inteiro positivo t e um conjunto $T = \{a_1, \ldots, a_t\} \subset R$, de forma que

$$S \subseteq T + Tx + \cdots + Tx^k.$$

Dessa forma, para provar que $S^{N+1} = 0$, é suficiente provar que

$$(T + Tx + \cdots + Tx^k)^{N+1} = 0,$$

ou seja, é suficiente mostrar que

$$a_{i_0} x^{d_1} a_{i_1} x^{d_2} \ldots a_{i_N} x^{d_{N+1}} = 0,$$

para quaisquer inteiros positivos $d_1, \ldots, d_{N+1} \leq k$ e quaisquer inteiros positivos $i_0, \ldots, i_k \leq t$.

Usando (1.0.3), temos que, para quaisquer inteiros positivos $d_1, \ldots, d_{N+1} \leq k$ e quaisquer inteiros positivos $i_0, \ldots, i_N \leq t$, o produto $a_{i_0} x^{d_1} a_{i_1} x^{d_2} \ldots a_{i_N} x^{d_{N+1}}$ é escrito como uma $\mathbb{Z}$-combinação linear de elementos da forma

$$a_{i_0} \delta^{j_1}(a_{i_1}) \ldots \delta^{j_N}(a_{i_N}) x^M, \tag{4.2.1}$$

onde M é algum inteiro positivo e $j_1, \ldots, j_N$ são inteiros positivos que satisfazem as seguintes relações:

$$\begin{aligned} &j_1 \leq d_1; \\ &j_2 \leq d_1 + d_2 - j_1; \\ &\quad \cdots \\ &j_N \leq d_1 + \cdots + d_N - j_1 - \cdots - j_{N-1}. \end{aligned}$$

Podemos escrever essas inequações como

$$\begin{aligned} j_1 &\leq d_1 \leq k; \\ j_2 + j_1 &\leq d_1 + d_2 \leq 2k; \\ &\cdots \\ j_N + \cdots + j_2 + j_1 &\leq d_1 + d_2 + \cdots + d_N \leq nk. \end{aligned}$$

Somando as últimas inequações, temos que:

$$j_N + 2j_{N-1} + \cdots + (N-1)j_2 + Nj_1 \leq \sum_{i=1}^{N} ki = k\binom{N+1}{2}. \tag{4.2.2}$$

Guardemos essa importante observação que motivará uma definição mais a seguir e nos voltemos novamente para os produtos da forma (4.2.1).

Para provar que $S^{N+1} = 0$, é suficiente mostrar que os produtos da forma (4.2.1) são todos nulos. Nestas condições, é conveniente definir, para todo inteiro não negativo n, o conjunto

$$T_n = T \cup \delta(T) \cup \cdots \cup \delta^n(T).$$

Como T_n é finito, para todo inteiro não negativo n, existe um inteiro positivo b_n tal que $T_n^{b_n} = 0$. Podemos definir a sequência $\mathbf{b} = (b_0, b_1, \dots)$ de números inteiros positivos e separar o problema nos seguintes casos:

Caso 1. Existe um inteiro positivo n tal que, existam b_n índices consecutivos $j_{r+1}, \dots, j_{r+b_n} \leq n$ dentre os índices de (4.2.1). Aqui, temos que

$$\begin{aligned} \delta^{j_{r+1}}(a_{i_{r+1}}), \delta^{j_{r+2}}(a_{i_{r+2}}), \dots, \delta^{j_{r+b_n}}(a_{i_{r+b_n}}) \in T_n \Rightarrow \\ \delta^{j_{r+1}}(a_{i_{r+1}})\delta^{j_{r+2}}(a_{i_{r+2}}) \dots \delta^{j_{r+b_n}}(a_{i_{r+b_n}}) \in T_n^{b_n} \Rightarrow \\ a_{i_0}\delta^{j_1}(a_{i_1})\delta^{j_2}(a_{i_2}) \dots \delta^{j_N}(a_{i_N}) = 0 \end{aligned}$$

Em particular, neste caso, a expressão (4.2.1) é igual a zero.

Caso 2. Para qualquer inteiro positivo n, quaisquer b_n índices consecutivos dentre $j_1, \dots, j_N$, existe um deles que é maior do que n.

Observe que o Caso 2 não é contemplado pela argumentação anterior e sugere uma abordagem combinatória, conforme será visto nas próximas seções. Tal abordagem pretende tirar proveito da identidade polinomial satisfeita pelos elementos do anel R.

4.3 Combinatória em palavras

Considere um conjunto A e defina A^+ como o semigrupo livre sobre A, ou seja, A^+ é conjunto das sequências finitas formadas por elementos de A. A essas sequências daremos o nome de

palavras e aos elementos de A daremos o nome de *letras*. O conjunto A^+ é um semigrupo considerando a operação como a concatenação de palavras.

Se $u, v \in A^+$, então dizemos que u é *prefixo* de v se existe palavra $w \in A^+$ tal que $v = uw$, ou seja, a palavra v é formada da palavra u concatenada à palavra w à direita. Dizemos que u é *sufixo* de v se existe palavra $w \in A^+$ tal que $v = wu$.

Se $u, v \in A^+$, dizemos que v é *subpalavra* de u se existem palavras $w, x \in A^+$ (possivelmente vazias) tais que $u = wvx$.

Uma palavra $u \in A^+$ não vazia tem *comprimento* $\ell(u) = n$, onde n é um inteiro positivo, se existem $u_1, \ldots, u_n \in A$ tais que $u = u_1 \ldots u_n$. Definimos o comprimento de uma palavra vazia como $\ell(\emptyset) = 0$.

Fixemos por um instante $A = \mathbb{N} = \{0, 1, 2, 3, \ldots\}$. Considere $u = u_1 \ldots u_n \in \mathbb{N}^+$ uma palavra, com $u_1, \ldots, u_n \in \mathbb{N}$. Definimos o *peso* de u como

$$\omega(u) = \min_{\sigma \in S_n} \left\{ \sum_{k=1}^{n} (n-k+1) u_{\sigma(k)} \right\}$$

Exemplo 4.3.1. Sejam $u = 2\ 1\ 4$, $v = 2\ 1\ 2$ e $w = 2\ 2\ 1$. Os possíveis resultados para $\sum_{k=1}^{n}(n-k)u_{\sigma(k)}$ são:

$$\begin{aligned}
3.2 + 2.1 + 1.4 &= 12 \\
3.2 + 2.4 + 1.1 &= 15 \\
3.1 + 2.2 + 1.4 &= 11 \\
3.1 + 2.4 + 1.2 &= 13 \\
3.4 + 2.1 + 1.2 &= 14 \\
3.4 + 2.2 + 1.1 &= 17
\end{aligned}$$

Segue que o peso de u é $\omega(u) = 11$. Como v e w são compostos das mesmas letras, temos que $\omega(v) = \omega(w) = 9$.

Se k é um inteiro positivo, dizemos que $u \in \mathbb{N}^+$ é uma palavra *k-válida* se

$$\omega(u) \leq \binom{k}{2}.$$

Assim como o conceito de peso de uma palavra de $\mathbb{N}^+$, a definição de palavra k-válida é motivada pela propriedade (4.2.2). Podemos, portanto, formalizar no seguinte lema algumas das conclusões da seção anterior:

Lema 4.3.2. *Seja R um anel arbitrário, $\delta : R \to R$ uma derivação de R, n, m, k inteiros positivos e $T = \{a_1, a_2, \ldots, a_m\} \subseteq R$ um subconjunto. Para quaisquer inteiros positivos $d_1, d_2, \ldots, d_{n+1} \leq k$ e quaisquer inteiros positivos $i_0, i_1, \ldots, i_n \leq m$, o produto de elementos de $R[x; \delta]$*

$$a_{i_0} x^{d_1} a_{i_1} x^{d_2} a_{i_2} \ldots x^{d_n} a_{i_n} x^{d_{n+1}}$$

é escrito como uma $\mathbb{Z}$-combinação linear de elementos da forma

$$a_{i_0}\delta^{j_1}(a_{i_1})\delta^{j_2}(a_{i_2})\dots\delta^{j_n}(a_{i_n})x^M$$

onde M é um inteiro positivo e $j_1, j_2, \dots, j_n \leq k$ são inteiros positivos tais que $j_1 j_2 \dots j_n \in \mathbb{N}^+$ é uma palavra k-válida.

Intuitivamente, podemos interpretar uma palavra k-válida como uma palavra cujas letras não são "demasiadamente maiores do que k".

Agora definiremos termos que nos auxiliarão a tratar o caso descrito no último parágrafo da seção anterior. Fixe uma sequência infinita $\mathbf{b} = (b_0, b_1, \dots)$ de inteiros positivos. Uma palavra $u \in \mathbb{N}^+$ é dita $\mathbf{b}$-*limitada* se, para todo m inteiro não negativo, toda subpalavra de u cujo comprimento seja b_m (se existir) contém uma letra maior do que m.

Exemplo 4.3.3. Sejam $u = 3\ 2\ 7\ 2$, $v = 1\ 2\ 2\ 7$ palavras de $\mathbb{N}^+$ e seja a sequência de naturais $\mathbf{b} = (1, 2, 3, 4, \dots)$. A palavra v não é $\mathbf{b}$-limitada, pois admite a subpalavra $1\ 2\ 2$ de tamanho $b_2 = 3$ mas não possui uma letra maior do que 2. Já a palavra u é $\mathbf{b}$-limitada. Note que existem sequências que não admitem palavras limitadas, como, por exemplo, a sequência $(1, 1, 1, \dots)$.

Seja B um conjunto arbitrário e $<$ uma ordem parcial sobre B. Podemos definir uma ordem parcial $\prec$ sobre B^+ da seguinte forma:

- Se $u, v \in \mathbb{N}^+$ são palavras distintas tais que u é prefixo de v ou vice-versa, então u e v são incomparáveis;
- Caso contrário, considere que $u \prec v$ segundo a ordem lexicográfica.

Dizemos que a sequência finita $(v_1, v_2, \dots, v_d)$ de palavras de B^+ é *d-decrescente* se

$$v_1 \succ v_2 \succ \dots \succ v_d$$

Dizemos que uma palavra $u \in B^+$ admite *subpalavra d-decrescente*, onde d é um inteiro positivo, se existirem $w, v_1, v_2, \dots, v_d, x \in B^+$ tais que $u = wv_1v_2\dots v_dx$ e $(v_1, v_2, \dots, v_d)$ é d-decrescente.

Conforme afirmado na seção anterior, almejamos tirar proveito de alguma identidade polinomial satisfeita por R. Para tal, será necessária a demonstração da seguinte proposição:

Proposição 4.3.4. *Sejam k, d inteiros positivos, $\mathbf{b} = (b_0, b_1, b_2, \dots)$ uma sequência de naturais e $\varepsilon \in [0, 1[$. Então existem inteiros positivos $N = N(d, \mathbf{b}, k, \varepsilon)$ e $M = M(d, \mathbf{b}, k, \varepsilon)$ tais que, para toda palavra $u \in \mathbb{N}^+$ com $\ell(u) \geq N$, k-válida e $\mathbf{b}$-limitada, existem $w \in \mathbb{N}^+$ e uma sequência d-decrescente $(v_1, v_2, \dots, v_d)$ tais que a subpalavra das últimas $\lfloor \varepsilon n \rfloor$ letras seja $wv_1v_2\dots v_d$ e, para todo $i = 1, 2, \dots, d$, a letra inicial de v_i é menor do que M.*

Demonstração. Procedemos por indução sobre d.

O caso em que $d = 1$ é trivial, e é suficiente tomar $M(1, \mathbf{b}, k, \varepsilon) = N(1, \mathbf{b}, k, \varepsilon) = 1$.

Suponha agora que $d \geq 1$ seja um inteiro positivo tal que a proposição seja válida e tome

$$M_1 = M(d, \mathbf{b}, k, \varepsilon/2) \quad \text{e} \quad N_1 = N(d, \mathbf{b}, k, \varepsilon/2)$$

Daí, fixe um número inteiro positivo M_2 tal que

(i) $M_2 > M_1$

(ii) $M_2 > 8(b_{M_1})^2 k\varepsilon^{-2}$

Daí temos que

$$M_2\binom{((\varepsilon n/2)-1)/b_{M_1}}{2} = \frac{M_2}{2}\left(\frac{\frac{\varepsilon n}{2}-1}{b_{M_1}}\right)\left(\frac{\frac{\varepsilon n}{2}-1}{b_{M_1}}-1\right)$$
$$\overset{n}{\sim} \frac{M_2}{2b_{b_{M_1}}^2}\frac{\varepsilon^2 n^2}{2^2} = \frac{M_2 n^2}{8b_{M_1}\varepsilon^{-2}} \geq kn^2$$

Logo, como $kn^2 > k^{\frac{n(n+1)}{2}} = k\binom{n+1}{2}$, podemos tomar inteiro positivo N_2 tal que, se $n > N_2$ então

$$M_2\binom{((\varepsilon n/2)-1)/b_{M_1}}{2} > k\binom{n+1}{2}$$

Seja $u \in \mathbb{N}^+$ uma palavra k-válida, **b**-limitada e cujo comprimento seja $n \geq N_2$. Escreva $u = vwx$, onde $v, w, x \in \mathbb{N}^+$ são palavras tais que

- wx tenha comprimento $\lfloor \varepsilon n \rfloor$;
- x tenha comprimento $\lfloor \varepsilon n/2 \rfloor$.

Decomponha w como $w = y_1 y_2 \dots y_j y_{j+1}$ de forma que cada subpalavra $y_1, y_2, \dots, y_j$ tenha comprimento b_{M_1} e a palavra y_{j+1} tenha comprimento não negativo e menor do que b_{M_1}.

Por construção,

$$j = \left\lfloor \frac{\lfloor \varepsilon n \rfloor - \lfloor \varepsilon n/2 \rfloor}{b_{M_1}} \right\rfloor$$

Observe que

- $\lfloor \varepsilon n \rfloor = \varepsilon n - \delta_{\varepsilon n}$, com $0 \leq \delta_{\varepsilon n} < 1$;
- $\lfloor \varepsilon n/2 \rfloor = \varepsilon n/2 - \delta_{\varepsilon n}$, com $0 \leq \delta_{\varepsilon n/2} < 1$.

Daí, temos que

$$\frac{\lfloor \varepsilon n \rfloor - \lfloor \varepsilon n/2 \rfloor}{b_{M_1}} = \frac{1}{b_{M_1}}\left(\frac{\varepsilon n}{2} + (\delta_{\varepsilon n} - \delta_{\varepsilon n/2})\right) \geq \frac{1}{b_{M_1}}\left(\frac{\varepsilon n}{2} - 1\right) \tag{4.3.5}$$

Se necessário, podemos alterar N_2 de forma que, se $n \geq N_2$, então $\frac{1}{b_{M_1}}\left(\frac{\varepsilon n}{2} - 1\right) > 1$. assim, podemos assumir que j é um inteiro positivo.

Se $m \in \{1, 2, \dots, j\}$, então, y_m tem comprimento b_{M_1} e, portanto, existe letra em y_m digamos, $a_m \in \mathbb{N}$, tal que $a_m > M_1$.

Afirmamos que existe $m \in \{1, 2, \ldots, j\}$ tal que $a_m < M_2$. De fato, caso contrário, teríamos que a palavra u teria ao menos j letras maiores ou iguais a M_2. Daí, teríamos que

$$\omega(u) \geq \omega(w) \geq jM_2 + (j-1)M_2 + \ldots + M_2 = M_2\binom{j+1}{2}$$

De (4.3.5), temos que

$$j+1 = \left\lfloor \frac{\lfloor \varepsilon n \rfloor - \lfloor \varepsilon n/2 \rfloor}{b_{M_1}} \right\rfloor + 1 > \frac{\lfloor \varepsilon n \rfloor - \lfloor \varepsilon n/2 \rfloor}{b_{M_1}} \geq \frac{1}{b_{M_1}} \left(\frac{\varepsilon n}{2} - 1 \right)$$

e, portanto,

$$\omega(u) \geq M_2\binom{j+1}{2} > M_2\binom{((\varepsilon n/2) - 1)/b_{M_1}}{2} > k\binom{n+1}{2},$$

um absurdo, visto que a palavra u tem comprimento n e é k-válida.

Logo, existe letra $a \in \mathbb{N}$ da palavra w tal que $M_1 < a < M_2$. Tome palavras $b, c \in \mathbb{N}^+$ tais que $w = bc$ e a letra inicial de c seja a.

Por hipótese de indução, existem palavras $p, v_1, v_2, \ldots, v_d \in \mathbb{N}^+$ tais que $x = pv_1 \ldots v_d$, $\{v_1, \ldots, v_d\}$ seja subsequência d-decrescente de x e todas as letras iniciais de $v_1, \ldots, v_d$ são menores do que M_1.

Segue que $u = vb(cp)v_1 \ldots v_d$, e, por construção,

$$cp \succ v_1 \succ v_2 \succ \ldots \succ v_d$$

é uma sequência $(d+1)$-decrescente em que cada uma das palavras $cp, v_1, v_2, \ldots, v_d$ começa com uma letra menor do que M_2.

O resultado desejado segue, portanto, tomando

$$M(d+1, \mathbf{b}, k, \varepsilon) = M_2 \quad \text{e} \quad N(d+1, \mathbf{b}, k, \varepsilon) = N_2 \qquad \square$$

Corolário 4.3.6. *Sejam k, d inteiros positivos e $\mathbf{b} = (b_0, b_1, b_2, \ldots)$ uma sequência de naturais. Existe inteiro positivo $N = N(d, \mathbf{b}, k)$ tal que toda palavra $u \in \mathbb{N}^+$ com $\ell(u) \geq N$, k-válida e $\mathbf{b}$-limitada contém uma subpalavra d-decrescente.*

Demonstração. O resultado segue aplicando a Proposição 4.3.4, fazendo $N = N(d, \mathbf{b}, k) = N(d, \mathbf{b}, k, 1)$. $\square$

4.4 Anéis de polinômios diferenciais sobre anéis localmente nilpotentes: abordagem combinatória

Agora estamos nas condições para mostrar o resultado original de [BMS15]:

Teorema 4.4.1. *Seja R um anel localmente nilpotente e $\delta : R \to R$ uma derivação em R. Então $R[x; \delta]$ é um anel localmente nilpotente.*

Demonstração. Como R é um anel PI, podemos supor que exista um inteiro positivo d e existam $c_\sigma \in \mathbb{Z}$, para qualquer $\sigma \in S_d \setminus \{Id\}$, tais que

$$x_1 \dots x_d - \sum_{\substack{\sigma \in S_d \\ \sigma \neq Id}} c_\sigma x_{\sigma(1)} \dots x_{\sigma(d)} \in \mathbb{Z}\langle \mathbf{X} \rangle \tag{4.4.2}$$

é identidade polinomial de R. Na mesma notação da Seção 4.2, fixe para o resto da demonstração $N = N(d, \mathbf{b}, k)$.

Continuando o desenvolvimento da Seção 4.2, observe que os dois últimos parágrafos podem ser reescritos na nova nomenclatura como:

Caso 1. A palavra $u = j_1 \dots j_N \in \mathbb{N}^+$ não é **b**-limitada; então existe um inteiro positivo n e uma subpalavra de u cujo comprimento seja b_n, digamos, $j_{r+1}, \dots, j_{r+b_n} \leq n \in \mathbb{N}^+$. Nesse caso, como mostrado anteriormente, o produto $a_{i_0}\delta^{j_1}(a_{i_1}) \dots \delta^{j_N}(a_{i_N})$ é nulo para quaisquer inteiros positivos $i_0, i_1, \dots, i_N \leq t$;

Caso 2. A palavra $u = j_1 \dots j_N \in \mathbb{N}^+$ é **b**-limitada.

Para completar a demonstração, basta tratar os casos em que $u = j_1 \dots j_N \in \mathbb{N}^+$ é uma palavra com $\ell(u) = N$, k-válida e **b**-limitada.

Suponha, por contradição, que exista uma palavra $u = j_1 \dots j_N \in \mathbb{N}^+$ com $\ell(u) = N$, k-válida, **b**-limitada e inteiros positivos $i_0, i_1, \dots, i_N \leq t$ tais que $a_{i_0}\delta^{j_1}(a_{i_1}) \dots \delta^{j_N}(a_{i_N}) \neq 0$. Podemos tomar u minimal com tais propriedades para $i_0, i_1, \dots, i_N \leq t$ fixados. Para toda subpalavra $y = j_r \dots j_{r+s}$, com $r, s \in \mathbb{Z}$ convenientes, defina

$$f(y) = \delta^{j_r}(a_{i_r}) \dots \delta^{j_{r+s}}(a_{i_{r+s}}).$$

Pelo Corolário 4.3.6, podemos tomar subpalavras $v, w_1, w_2, \dots, w_d, z \in \mathbb{N}^+$ tais que $j_1 j_2 \dots j_N = v w_1 w_2 \dots w_d z$ e

$$w_1 \succ w_2 \succ \dots \succ w_d$$

Fazendo em (4.4.2), $x_1 = f(w_1), \dots, x_d = f(w_d)$, temos que

$$f(w_1) \dots f(w_d) = \sum_{\substack{\sigma \in S_d \\ \sigma \neq Id}} c_\sigma f(w_{\sigma(1)}) \dots f(w_{\sigma(d)}) \tag{4.4.3}$$

Multiplicando (4.4.3) à esquerda por $a_{i_0} f(v)$ e à direita por $f(z)$, temos que

$$a_{i_0} f(v) f(w_1) \dots f(w_d) f(z) = \sum_{\substack{\sigma \in S_d \\ \sigma \neq Id}} c_\sigma a_{i_0} f(v) f(w_{\sigma(1)}) \dots f(w_{\sigma(d)}) f(z) \tag{4.4.4}$$

Observe daí que, para toda permutação $\sigma \in S_d \setminus \{Id\}$ existe uma permutação $\tau \in S_N \setminus \{Id\}$ tal que

$$a_{i_0} f(v) f(w_{\sigma(1)}) \dots f(w_{\sigma(d)}) f(z) = a_{i_0} \delta^{j_{\tau(1)}}(a_{i_{\tau(1)}}) \dots \delta^{j_{\tau(N)}}(a_{i_{\tau(N)}})$$

Consideremos inicialmente as permutações τ tais que a palavra $j_{\tau(1)} \dots j_{\tau(N)} \in \mathbb{N}^+$ não seja **b**-limitada. Neste caso, temos que $a_{i_0}\delta^{j_{\tau(1)}}(a_{i_{\tau(1)}}) \dots \delta^{j_{\tau(N)}}(a_{i_{\tau(N)}}) = 0$.

Considere agora o caso onde a permutação τ seja tal que a palavra $j_{\tau(1)} \dots j_{\tau(N)} \in \mathbb{N}^+$ seja **b**-limitada. Claramente, o peso da palavra $j_{\tau(1)} \dots j_{\tau(N)}$ é igual ao peso da palavra $j_1 \dots j_N$ e, portanto, segue que $j_{\tau(1)} \dots j_{\tau(N)}$ é uma palavra de comprimento N, k-válida e **b**-limitada. Observe que, pela construção de τ, existe uma permutação não trivial $\mu \in S_d$ tal que $j_{\tau(1)} \dots j_{\tau(N)} = vw_{\mu(1)} \dots w_{\mu(d)}z$. Como a sequência $(w_1, \dots, w_d)$ foi tomada d-decrescente, temos que

$$j_1 \dots j_N = vw_1 \dots w_d z \succ vw_{\mu(1)} \dots w_{\mu(d)}z = j_{\tau(1)} \dots j_{\tau(N)}$$

Mas daí, pela minimalidade de $j_1 \dots j_N$, temos que

$$a_{i_0}\delta^{j_{\tau(1)}}(a_{i_{\tau(1)}}) \dots \delta^{j_{\tau(N)}}(a_{i_{\tau(N)}}) = 0.$$

Concluímos que, para toda permutação $\sigma \in S_d$ não trivial,

$$a_{i_0}f(v)f(w_{\sigma(1)}) \dots f(w_{\sigma(d)})f(z) = 0,$$

donde segue, por (4.4.4), que

$$a_{i_0}\delta^{j_1}(a_{i_1}) \dots \delta^{j_N}(a_{i_N}) = a_{i_0}f(v)f(w_1) \dots f(w_d)f(z) = 0,$$

um absurdo.

Conclui-se que, para toda palavra $u = j_1 \dots j_N \in \mathbb{N}^+$ com $\ell(u) = N$, vale que

$$a_{i_0}\delta^{j_1}(a_{i_1}) \dots \delta^{j_N}(a_{i_N}) = 0$$

para quaisquer inteiros positivos $i_0, i_1, \dots, i_N \leq t$. Em particular, pelo desenvolvimento da Seção 4.2, temos que $S^{N+1} = 0$. □

Observe que não é possível provar um resultado análogo ao Teorema 4.4.1 para o caso de anéis de polinômios com automorfismo:

Exemplo 4.4.5. Se k é um corpo qualquer e $T = \{t_i \mid i \in \mathbb{Z}\}$ é um conjunto enumerável de indeterminadas, então podemos considerar no anel de polinômios $k[T]$ o ideal $k^\times[T]$ gerado pelas indeterminadas t_i, com $i \in \mathbb{Z}$. Em outras palavras, $k^\times[T]$ é o ideal dos polinômios nas variáveis de T que possuem termo constante zero. Por sua vez, $k^\times[T]$ contém $\mathrm{id}\langle {t_i}^2 \mid i \in \mathbb{Z}\rangle \lhd k[T]$, o ideal gerado em $k[T]$ pelos polinômios ${t_i}^2$, com $i \in \mathbb{Z}$. Mostremos que o anel $R = k^\times[T]/\,\mathrm{id}\langle {t_i}^2 \mid i \in \mathbb{Z}\rangle$ é um anel localmente nilpotente.

Tomando $S \subseteq R$ um conjunto finito, temos que existe um inteiro positivo N tal que S está contido no subanel R_N gerado pelos elementos $\bar{t}_i \in R$, com $-N \leq i \leq N$ e, portanto, o subanel gerado por S está contido em R_N. Conclui-se que é necessário e suficiente demonstrar que R_N é um conjunto nilpotente. Um elemento arbitrário de R_N é da forma

$$a_{-N}\bar{t}_{-N} + \dots + a_N\bar{t}_N,$$

onde cada $a_i \in k$, para $-N \leq i \leq N$. Como R_N é comutativo, vale o teorema binomial e, segue que o produto de $2N+1$ elementos de R_N é uma k-combinação linear de elementos da forma

$$t_{i_1}\bar{t}_{i_2}\cdots\bar{t}_{i_{2N+1}},\ \text{onde}\ -N \leq i_1, i_2, \ldots, i_{2N+1} \leq N \tag{4.4.6}$$

Segue pelo princípio da casa dos pombos que existem dois índices iguais dentre $i_1, \ldots, i_{2N+1}$ e, portanto, sempre ocorre em (4.4.6) o termo $\bar{t}_j{}^2 = 0$ para algum inteiro positivo $-N \leq j \leq N$. Segue que $\bar{t}_{i_1}\bar{t}_{i_2}\cdots\bar{t}_{i_{2N+1}} = 0$ para quaisquer índices e concluímos que ${R_N}^{2N+1} = 0$. Portanto, R_N é nilpotente como desejado.

Podemos definir sobre R um automorfismo $\sigma : R \to R$ dado por $\sigma(\bar{t}_i) = \bar{t}_{i+1}$, $i \in \mathbb{Z}$, e, com esse automorfismo, o anel $R[x;\sigma]$ não é sequer nil, pois $\bar{t}_0 x \in R[x;\sigma]$ não é nilpotente. De fato, para cada inteiro $N > 1$, temos que

$$\begin{aligned}(\bar{t}_0x)^N &= (\bar{t}_0x)(\bar{t}_0x)\ldots(\bar{t}_0x)\\ &= (\bar{t}_0\bar{t}_1x^2)(\bar{t}_0x)\ldots(\bar{t}_0x)\\ &= (\bar{t}_0\bar{t}_1\bar{t}_2x^3)\ldots(\bar{t}_0x)\\ &\ldots\\ &= (\bar{t}_0\bar{t}_1\ldots\bar{t}_N)x^{N+1}.\end{aligned}$$

Como $t_0\ldots t_N \notin \operatorname{id}\langle {t_i}^2 \mid i \in \mathbb{Z}\rangle$, segue que $(\bar{t}_0x)^N \neq 0$ para todo inteiro positivo N. Em suma, mesmo que R seja um anel comutativo e localmente nilpotente, $R[x;\sigma]$ não necessariamente será um anel localmente nilpotente.

Conforme provado no Teorema 4.1.1, o radical de Jacobson do anel $R[x;\delta]$ é o anel de polinômios diferenciais com coeficientes em algum ideal nil de R. Se R for um anel comutativo com unidade e $\delta = 0$, então temos que $N = \operatorname{Nil} R$ [Lam01, 5.1, p. 67]. Segundo o próximo exemplo, não podemos generalizar este resultado para anéis de polinômios diferenciais sobre R, mesmo quando R satisfaz uma identidade polinomial.

Exemplo 4.4.7. Seja $p \in \mathbb{Z}$ um primo positivo, K_p um corpo com p elementos e $K_p[t]$ o anel de polinômios sobre a indeterminada t. Daí, se $I = \operatorname{id}\langle t^p\rangle$, segue que está bem definida uma derivação do anel $R = K_p[t]/\operatorname{id}\langle t^p\rangle$ determinada por:

$$\begin{aligned}&\delta : K_p[t]/I \to K_p[t]/I\\ &\quad a(t+I)^n \mapsto an(t+I)^{n-1}, \quad n \in \mathbb{Z}, n > 0\end{aligned}$$

e estendida para soma por linearidade. Esta derivação é tal que $\delta(t+I) = 1+I$ e, portanto, se N é um ideal tal que $\delta(N) \subseteq N$, então $N = 0$ ou $N = R$. Pelo Teorema 2.5.3, devemos ter que $\operatorname{rad} R[x;\delta] = 0$.

Por outro lado, conforme veremos no Teorema 4.4.9, podemos determinar o ideal N, desde que R seja uma álgebra sobre um corpo de característica zero. Antes disso, mostraremos o seguinte lema:

Lema 4.4.8. *Seja R uma álgebra com unidade sobre um corpo de característica zero e $\delta : R \to R$ uma derivação, então $\delta(\operatorname{Nil} R) \subseteq \operatorname{Nil} R$.*

Demonstração. Se $a \in \operatorname{Nil} R$, então é suficiente mostrar que $R\delta(a)R \subseteq \operatorname{Nil} R$. Para isso, se $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$, então mostraremos que $\sum_{i=1}^{t} r_i\delta(a)s_i \in \operatorname{Nil} R$. Observe inicialmente que $\sum_{i=1}^{t} r_i a s_i \in \operatorname{Nil} R$ e, para todo inteiro positivo n, temos que

$$\left(\sum_{i=1}^{t} r_i a s_i\right)^n = \sum\nolimits_I r_{i_1} a s_{i_1} \ldots r_{i_n} a s_{i_n},$$

onde a última soma percorre todos os multi-índices do conjunto $I = \{(i_1, \ldots, i_n) \mid i_1, \ldots, i_n \in \mathbb{Z}, 1 \leq i_1, \ldots, i_n \leq t\}$. Aplicando δ^n em ambos os lados, temos

$$\delta^n\left(\left(\sum_{i=1}^{t} r_i a s_i\right)^n\right) = \sum \delta^n(r_{i_1} a s_{i_1} \ldots r_{i_n} a s_{i_n}).$$

Observe que, para qualquer $i = 1, \ldots, n$,

$$\delta(r_i a s_i) = (\delta(r_i) a s_i + r_i \delta(a) s_i + r_i a \delta(s_i)) \in r_i\delta(a)s_i + \operatorname{Nil} R.$$

Analogamente, existe um inteiro $m = m(n)$ tal que, para quaisquer $1 \leq i_1, i_2, \ldots, i_n \leq t$, temos que

$$\delta^n(r_{i_1} a s_{i_1} \ldots r_{i_n} a s_{i_n}) \in m(r_{i_1}\delta(a)s_{i_1} \ldots r_{i_n}\delta(a)s_{i_n}) + \operatorname{Nil} R$$

e, portanto,

$$\delta^n\left(\left(\sum_{i=1}^{t} r_i a s_i\right)^n\right) \in m\left(\sum\nolimits_I r_{i_1}\delta(a)s_{i_1} \ldots r_{i_n}\delta(a)s_{i_n}\right) + \operatorname{Nil} R,$$

para algum inteiro positivo m. Mas como $\sum_{i=1}^{t} r_i a s_i \in \operatorname{Nil} R$, existe um inteiro positivo n tal que $(\sum_{i=1}^{n} r_i a s_i)^n = 0$ e, portanto, existe inteiro positivo m tal que

$$m\left(\sum\nolimits_I r_{i_1}\delta(a)s_{i_1} \ldots r_{i_n}\delta(a)s_{i_n}\right) \in \operatorname{Nil} R.$$

Como R é uma álgebra sobre um corpo de característica positiva, segue que

$$\left(\sum_{i=1}^{t} r_i\delta(a)s_i\right)^n = \sum\nolimits_I r_{i_1}\delta(a)s_{i_1} \ldots r_{i_n}\delta(a)s_{i_n} \in \operatorname{Nil} R.$$

E, portanto, para quaisquer $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$, $\sum_{i=1}^{t} r_i\delta(a)s_i \in \operatorname{Nil} R$. Concluímos que $R\delta(a)R \subseteq \operatorname{Nil} R$ e, em particular, $\delta(a) \in \operatorname{Nil} R$. □

Teorema 4.4.9 ([BMS15]). *Se k é um corpo de característica zero, R é uma k-álgebra com unidade que satisfaz uma identidade polinomial de $\mathbb{Z}\langle \mathbf{X}\rangle$ e $\delta : R \to R$ é uma derivação de R, então o ideal $N = \operatorname{Nil} R$ é tal que $\delta(N) \subseteq N$ e $\operatorname{rad}(R[x;\delta]) = N[x;\delta]$. Em particular, $N = \operatorname{rad}(R[x;\delta]) \cap R$.*

Demonstração. Como N é nil, é em particular localmente nilpotente. Além disso, pelo Lema 4.4.8, $\delta(N) \subseteq N$. Adicionalmente, como R satisfaz uma identidade polinomial, N também satisfaz uma identidade polinomial de $\mathbb{Z}\langle \mathbf{X}\rangle$. Assim, está bem definido o conjunto $N[x;\delta]$, que é um ideal de $R[x;\delta]$ e é localmente nilpotente, pelo Teorema 4.4.1. Segue que $N[x;\delta] \subseteq \operatorname{rad}(R[x;\delta])$.

Para provar a inclusão inversa, observe que o anel $\overline{R} = R/N$ é um anel sem ideais nil que satisfaz uma identidade polinomial de $\mathbb{Z}\langle \mathbf{X}\rangle$. Podemos definir a função $\overline{\delta} : \overline{R} \to \overline{R}$ dada por $\overline{\delta}(r+N) = \delta(r) + N$, que está bem definida uma vez que $\delta(N) \subseteq N$. Além disso, $\overline{\delta}$ é uma derivação de $\overline{R}$. Segue, pelo Corolário 4.1.11, que $\operatorname{rad}((R/N)[x;\overline{\delta}]) = 0$. Por outro lado, a projeção natural de R em R/N induz um homomorfismo sobrejetor do anel $R[x;\delta]$ para o anel $(R/N)[x;\overline{\delta}]$ cujo núcleo é o ideal $N[x;\delta]$. Segue, portanto, que

$$0 = \operatorname{rad}((R/N)[x;\overline{\delta}]) \simeq \operatorname{rad}(R[x;\delta]/N[x;\delta]) = \operatorname{rad}(R[x;\delta])/N[x;\delta],$$

onde a última igualdade segue pois $N[x;\delta] \subseteq \operatorname{rad}(R[x;\delta])$ e, portanto, é válida a Proposição 2.2.5. Podemos concluir, portanto, que $\operatorname{rad}(R[x;\delta])/N[x;\delta] = 0$ e por consequência $\operatorname{rad}(R[x;\delta]) \subseteq N[x;\delta]$.

Concluímos pelos dois últimos parágrafos que $\operatorname{rad}(R[x;\delta]) = N[x;\delta]$. □

4.5 Comentários finais

Esperamos com este trabalho ter feito um texto auto-contido para as demonstrações dos resultados do Capítulo 4. Como mencionado na introdução, o problema de expandir o teorema de Amitsur para anéis de polinômios diferenciais tem resposta negativa, como conferido em [Smo15]. Alguns problemas relacionados continuam abertos, no entanto. Se R não tem ideais nil não nulos, então o radical de Jacobson de $R[x;\delta]$ é igual a zero? Se $R[x;\delta]$ é nil, então $R[x]$ é nil?

Índice Remissivo

Referências Bibliográficas

[Ami56] S. A. Amitsur. Radicals of polynomial rings. *Canad. J. Math.*, 8:355–361, 1956.

[Ami58] S. A. Amitsur. The radical of field extensions. *Bull. Res. Council Israel. Sect. F*, 7F:1–10, 1957/1958.

[Bae43] R. Baer. Radical ideals. *Amer. J. Math.*, 65:537–568, 1943.

[Ber64] G. M. Bergman. A ring primitive on the right but not on the left. *Proc. Amer. Math. Soc.*, 15:473–475, 1964.

[BG12] J. Bergen and P. Grzeszczuk. Jacobson radicals of ring extensions. *J. Pure Appl. Algebra*, 216(12):2601–2607, 2012.

[BMP87] J. Bergen, S. Montgomery, and D. S. Passman. Radicals of crossed products of enveloping algebras. *Israel J. Math.*, 59(2):167–184, 1987.

[BMS15] J. Bell, B. Madill, and F. Shinko. Differential polynomial rings over rings satisfying a polynomial identity. *J. Algebra*, 423:28–36, 2015.

[CL06] C-L Chuang and T-K Lee. Semiprime rings with prime ideals invariant under derivations. *J. Algebra*, 302(1):305–312, 2006.

[Cox04] D. Cox. *Galois theory*. Pure and Applied Mathematics (New York). Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2004.

[Deh22] M. Dehn. Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme. volume 85, pages 184–194. 1922.

[DF04] V. Drensky and E. Formanek. *Polynomial identity rings*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2004.

[dni06] Dniester notebook: unsolved problems in the theory of rings and modules. In *Non-associative algebra and its applications*, volume 246 of *Lect. Notes Pure Appl. Math.*, pages 461–516. Chapman & Hall/CRC, Boca Raton, FL, 2006. Translated from the 1993 Russian edition [MR1310114] by Murray R. Bremner and Mikhail V. Kochetov and edited by V. T. Filippov, V. K. Kharchenko and I. P. Shestakov.

[FKM83] M. Ferrero, K. Kishimoto, and K. Motose. On radicals of skew polynomial rings of derivation type. *J. London Math. Soc. (2)*, 28(1):8–16, 1983.

[For72] E. Formanek. Central polynomials for matrix rings. *J. Algebra*, 23:129–132, 1972.

[GW04a] B. J. Gardner and R. Wiegandt. *Radical theory of rings*, volume 261 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 2004.

[GW04b] K. R. Goodearl and R. B. Warfield, Jr. *An introduction to noncommutative Noetherian rings*, volume 61 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 2004.

[Hal43] M. Hall. Projective planes. *Trans. Amer. Math. Soc.*, 54:229–277, 1943.

[Hal83] P. Halpin. Central and weak identities for matrices. *Communications in Algebra*, 11(19):2237–2248, 1983.

[Her68] I. N. Herstein. *Noncommutative rings*. The Carus Mathematical Monographs, No. 15. Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York, 1968.

[Jac45a] N. Jacobson. The radical and semi-simplicity for arbitrary rings. *Amer. J. Math.*, 67:300–320, 1945.

[Jac45b] N. Jacobson. Structure theory of simple rings without finiteness assumptions. *Trans. Amer. Math. Soc.*, 57:228–245, 1945.

[Jor75] D. A. Jordan. Noetherian Ore extensions and Jacobson rings. *J. London Math. Soc. (2)*, 10:281–291, 1975.

[Kap70] I. Kaplansky. "Problems in the theory of rings" revisited. *Amer. Math. Monthly*, 77:445–454, 1970.

[Kem91] A. R. Kemer. *Ideals of identities of associative algebras*, volume 87 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1991. Translated from the Russian by C. W. Kohls.

[Köt30] G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.

[Kre72] J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.

[Lam01] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lev43] J. Levitzki. On the radical of a general ring. *Bull. Amer. Math. Soc.*, 49:462–466, 1943.

[Mad14] B. W. Madill. On the Jacobson radical of skew polynomial extensions of rings satisfying a polynomial identity. *ArXiv e-prints*, August 2014.

[mcd74] *Ring theory*. Marcel Dekker, Inc., New York, 1974. Edited by Bernard R. McDonald, Andy R. Magid and Kirby C. Smith, Lecture Notes in Pure and Applied Mathematics, Vol. 7.

[MR87] J. C. McConnell and J. C. Robson. *Noncommutative Noetherian rings*. Pure and Applied Mathematics (New York). John Wiley & Sons, Ltd., Chichester, 1987. With the cooperation of L. W. Small, A Wiley-Interscience Publication.

[NI14] A. Nasr-Isfahani. Jacobson radicals of skew polynomial rings of derivation type. *Canad. Math. Bull.*, 57(3):609–613, 2014.

[Ram84] J. Ram. On the semisimplicity of skew polynomial rings. *Proc. Amer. Math. Soc.*, 90(3):347–351, 1984.

[Raz73] Yu. P. Razmyslov. On a problem of Kaplansky. *Izvestiya: Mathematics*, 7(3):479–496, 1973.

[Rom08] S. Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.

[Row88] L. H. Rowen. *Ring theory. Vol. II*, volume 128 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1988.

[Smo15] A. Smoktunowicz. How far can we go with Amitsur's theorem? *ArXiv e-prints*, April 2015.

[SZ14] A. Smoktunowicz and M. Ziembowski. Differential polynomial rings over locally nilpotent rings need not be Jacobson radical. *J. Algebra*, 412:207–217, 2014.

[TWC07] Y-T Tsai, T-Y Wu, and C-L Chuang. Jacobson radicals of Ore extensions of derivation type. *Comm. Algebra*, 35(3):975–982, 2007.

[vdW85] B. L. van der Waerden. *A history of algebra*. Springer-Verlag, Berlin, 1985. From al-Khwārizmī to Emmy Noether.

[Wag37] W. Wagner. Über die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme. *Math. Ann.*, 113(1):528–567, 1937.