O HIPERCENTRO DE UM ANEL

LEILÁ MARIA VASCONCELLOS FIGUEIREDO

DISSERTAÇÃO APRESENTADA

AO

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

DA

UNIVERSIDADE DE SÃO PAULO

PARA OBTENÇÃO DO GRAU DE MESTRE

EM

MATEMÁTICA

ORIENTADOR:

Prof.Dr. Francisco César Polcino Milies

Durante a realização deste trabalho a autora recebeu apoio financeiro do CNPq e FINEP.

- SÃO PAULO, OUTUBRO DE 1978 -

À memória de

L. H. Jacy Monteiro

ÍNDICE

PREFÁCIO

O estudo de condições sob os quais um anel é necessariamente comutativo, integra o campo de abordagem da Teoria de Anéis.

Em 1905, J. Wedderburn obteve o primeiro resultado neste sentido demonstrando que todo anel com divisão finito é comutativo. Quarenta anos mais tarde, N. Jacobson, generalizando esta afirmação provou que um anel R tal que $x^n = x$, para algum inteiro $n = n(x) > 1$ e para todo x em R é comutativo.

Entretanto são poucos os anéis comutativos que verificam as hipóteses do Teorema de Jacobson e por isso tentou-se estender este resultado em outras direções — de modo que as condições impostas sobre o anel, sejam verificadas por todos os anéis comutativos e ainda, que elas forcem a comutatividade dos anéis em questão. Assim, desde o início da década de 50, até os dias de hoje, os Teoremas de Comutatividade vem sendo estudados por I. Herstein, C. Faith, I. Kaplansky e outros.

Do estudo da comutatividade surgiu naturalmente a idéia de se estender o conceito de centro de um anel. Uma destas generalizações que estudaremos em nosso trabalho é o *hipercentro* do anel, que é definido como o conjunto dos elementos do anel, que comutam com uma potência de todos os outros.

No Capítulo 1 apresentamos alguns teoremas de comutatividade que parecem sugerir a gênese do conceito de hipercentro.

No Capítulo 2 introduzimos esta noção e provamos o teorema central deste trabalho: quando um anel não tem ideais nil, seu centro e seu hipercentro coincidem.

No Capítulo 3, damos duas aplicações do teorema do hipercentro, demonstrado no capítulo anterior. Daremos um teorema de comutatividade e estudamos algumas propriedades de anéis radicais sobre subanéis.

Uma questão há muito tempo em aberto na Teoria dos Anéis é a conjectura de Köethe: "se um anel tem um ideal lateral nil não nulo, então este anel tem um ideal bilateral nil não nulo?" Se esta questão estivesse resolvida afirmativamente, os resultados do Capítulo 3 seriam de fácil demonstração. Justamente um dos méritos do teorema do hipercentro consiste em permitir contornar a questão provando essas proposições independentemente da resolução da Cojectura de Köethe.

Queremos agradecer a todas as pessoas que colaboraram na elaboração deste trabalho, em particular, ao Prof. Dr. Francisco César Polcino Milies pela dedicada orientação, ao Prof. Dr. Bernardo Felzenswalb por suas sugestões e aos colegas do grupo de Álgebra do IME, que ouviram pacientemente exposições de partes deste trabalho, dando sugestões e ajudando a resolver nossas dúvidas. Agradeço também ao sr. João Baptista Esteves de Oliveira pela datilografia do trabalho.

Leilã M. V. Figueiredo

CAPÍTULO 0

CONCEITOS BÁSICOS

Neste capítulo introduziremos definições e resultados básicos da Teoria dos Anéis que serão utilizados no texto que se segue. A maioria das demonstrações dos resultados aqui enunciados encontra-se em [7]. Denotaremos sempre por R um anel associativo, não necessariamente com unidade. Usaremos o termo *ideal* para indicar um ideal bilateral de R.

Iniciaremos introduzindo alguns conceitos.

<u>0.1 - DEFINIÇÃO</u> - Seja M um R-módulo (à direita). Chamaremos *anulador de* M ao conjunto

$$A(M) = \{r \in R\colon Mr = (0)\}$$

<u>0.2 - DEFINIÇÃO</u> - Um R-módulo M diz-se *fiel* se $A(M) = (0)$.

Verifica-se sem dificuldade que A(M) é um ideal de R e M é um $\frac{R}{A(M)}$-módulo fiel.

<u>0.3 - DEFINIÇÃO</u> - Um R-módulo M diz-se *irredutível* se $MR \neq (0)$ e se os únicos submódulos de M são (0) e M.

0.4 - DEFINIÇÃO - Um anel R diz-se *primitivo* se existir um R-módulo M irredutível e fiel.

Quando M é um R-módulo irredutível, o anel

$$D = \mathrm{Hom}_R(M,M)$$

é um anel com divisão. Podemos então dar a M uma estrutura de D-espaço vetorial (à esquerda) definindo $dx = d(x)$ para todo $d \in D$ e para todo $x \in R$. Se $E = \mathrm{Hom}_D(M,M)$, definimos a aplicação ϕ: $R \longrightarrow E$ por

$$r \longmapsto \phi_r \text{ por}$$

$$\phi_r: M \longrightarrow M \text{ é tal que}$$

$$\phi_r(x) = xr, \text{ para todo } x \in M.$$

Verifica-se facilmente que a aplicação ϕ é um homomorfismo de anéis.

Se o R-módulo de M for fiel, temos que ϕ é um monomorfismo, já que $\mathrm{Ker}\,\phi = A(M)$. Observamos então que quando R é um anel primitivo, ele é isomorfo a um anel de transformações lineares sobre um espaço vetorial. O Teorema da Densidade (de Jacobson-Chevalley), que enunciamos em continuação, mostra que além disso, toda transformação linear de um subespaço G de M, finitamente gerado sobre D, é a restrição de ϕ_r à G para algum $r \in R$.

0.5 - TEOREMA (Teorema de Densidade) - Seja R um anel primitivo e seja M um R-módulo irredutível e fiel. Se $D = \mathrm{Hom}_R(M,M)$ então, dados $v_1, \ldots, v_n \in M$, linearmente independentes sobre D e dados $w_1,\ldots,w_n \in M$ arbitrários, existe um elemento r em R tal que $v_i r = w_i$ para todo $i=1,\ldots,n$.

Uma consequência do Teorema da Densidade é a seguinte:

0.6 - TEOREMA - Seja R um anel primitivo. Então para algum anel com divisão D, ou R é isomorfo à $M_n(D)$, o anel das matrizes $n \times n$ sobre D, ou dado qualquer inteiro positivo m, existe um subanel S_m de R e um epimorfismo de S_m em $M_m(D)$.

Outro conceito da Teoria de Anéis que usaremos com frequência em nosso trabalho é o de radical de Jacobson de R.

0.7 - DEFINIÇÃO - O *radical de Jacobson* de um anel R, que denotaremos por $J(R)$ é o conjunto de todos os elementos de R que anulam todos os R-módulos irredutíveis. Se R não tem R-módulos irredutíveis colocamos $J(R) = R$.

0.8 - DEFINIÇÃO - Um elemento $x \in R$ é *quase-regular à direita* (*quase regular à esquerda*) se existe $r' \in R$ tal que $r+r'+rr' = 0$ (se existe $r'' \in R$ tal que $r+r''+r''r = 0$). Neste caso chamamos r' de *quase inverso à direita de* r e r'' de *quase inverso à esquerda de* r. Um ideal (ideal à direita, ideal à esquerda) de R é *quase regular à direita* a todos os seus elementos forem quase-regular à direita. De modo análogo definimos ideal (ideal à direita, ideal à esquerda) quase-regular à esquerda.

0.9 - PROPOSIÇÃO - O radical $J(R)$ de R, é um ideal quase-re gular à direita; além disto, todo ideal à direita quase-regular à direita de R está contido em $J(R)$.

Prova-se também que todo elemento de $J(R)$ é quase-regular à esquerda.

Quando o anel R tem unidade, um elemento $x \in R$ é quase-regular à direita (à esquerda) se e somente se $1+r$ é inversível à direita (à esquerda). Se $r \in J(R)$, então $1+r$ é inversível.

O fato acima nos sugere que, mesmo quando R é um anel sem unidade, definamos os símbolos $1+r$ e $(1+r)^{-1}$ quando $r \in J(R)$.

Se $r \in J(R)$, dizemos que $(1+r)$ é "formalmente inversível".

0.10 - DEFINIÇÃO - Sejam R um anel, $r \in J(R)$ e $x \in R$. Definimos $(1+r)x = x + rx$; $x(1+r) = x + xr$; $(1+r)^{-1}x = (1+r')x$; $x(1+r)^{-1} = x(1+r')$ onde r' é o quase-inverso à direita de r (que é igual ao quase-inverso à esquerda de r).

0.11 - PROPOSIÇÃO - Seja R um anel, $r \in J(R)$ e $x \in R$). Então:

(a) $x(1+r)(1+r)^{-1} = x$; $(1+r)^{-1}(1+r)x = x$

(b) $x(1+r)^{-1}(1+r) = (1+r)(1+r)^{-1}x = x$

(c) A aplicação $\phi: R \longrightarrow R$ definida por $\phi(x) = (1+r)x(1+r)^{-1}$ é um automorfismo de R.

0.12 - DEFINIÇÃO - Um elemento $x \in R$ é *nilpotente* se existe um inteiro $n > 0$ tal que $r^n = 0$. Um ideal (ideal à esquerda, ideal à di reita) de R é *nil* de todos os seus elementos forem nilpotentes. Um ideal I de R (ideal à direita, ideal à esquerda) de R é *nilpotente* se existe um inteiro $n > 0$ tal que $I^n = (0)$.

Todo elemento nilpotente de R é quase-regular à direita; logo por (0.9) todo ideal (ideal à direita, ideal à esquerda) nil de R está contido em J(R).

0.13 - DEFINIÇÃO - Um ideal N de R é um radical nil de R se N é nil e se $\frac{R}{N}$ não tem ideais nilpotentes.

Seja agora N(R) a reunião de todos os ideais nil de um anel R. Temos que N(R) é um ideal, e além disto, N(R) é um nil radical de R.

0.14 - DEFINIÇÃO - Chamamos *radical nil superior de* R ao ideal N(R) obtido como a reunião de todos os ideais nil de R.

O anel $\frac{R}{N(R)}$ não tem ideais nil não nulos, dizemos que um anel R não tem ideais nil quando $N(R) = (0)$.

0.15 - DEFINIÇÃO - Chama-se *ideal comutador* de R ao ideal C(R), gerado pelos elementos da forma $xy - yx$ para todo $x, y \in R$.

É claro que $\frac{R}{C(R)}$ é comutativo e é claro que R é comutativo se e somente se $C(R) = (0)$.

0.16 - DEFINIÇÃO - Um anel R diz-se *semisimples* se $J(R) = (0)$.

0.17 - DEFINIÇÃO - Um anel R é *primo* se $aRb = (0)$, com $a, b \in R$, então $a = 0$ ou $b = 0$.

Pode-se demonstrar que todo anel primitivo é um anel primo. Além disso, temos as seguintes caracterizações dos anéis primos:

0.18 - PROPOSIÇÃO - São equivalentes as seguintes afirmações sobre um anel R:

(1) R é primo.

(2) Se A e B são ideais de R tais que $AB = (0)$ então $A = (0)$ ou $B = (0)$.

(3) O anulador à direita de um ideal à direita não nulo de R é (0).

(4) O anulador à esquerda de um ideal à esquerda não nulo de R é (0).

0.19 - DEFINIÇÃO - Seja R um anel; consideremos o grupo aditivo $(R,+)$. Se existe um inteiro $m > 0$ que seja o máximo do conjunto $\{o(x): x \in (R,+)\}$, m é chamado *característica* de R; caso contrário dizemos que R tem característica *zero*.

0.20 - DEFINIÇÃO - Um anel R é *livre de torção* se $mx = 0$, com m inteiro e $x \in R$, então $m = 0$ ou $x = 0$.

0.21 - PROPOSIÇÃO - Se um anel primo R não é livre de torção, então a característica de R é um número primo.

0.22 - PROPOSIÇÃO - Se R é um anel primo, então o centro Z(R) de R é domínio de integridade, ou é (0).

Utilizaremos ainda a seguinte definição e teoremas.

0.23 - DEFINIÇÃO - Um anel R é *produto subdireto* de uma família de anéis $(R_\alpha)_{\alpha\in I}$ se existe um monomorfismo $\phi:R \longrightarrow \prod_{\alpha\in I} R_\alpha$ tal que $\pi_\alpha\phi(R) = R_\alpha$, onde $\prod_{\alpha\in I} R_\alpha$ indica o produto direto dos anéis R_α, $\alpha\in I$ e π_α é a projeção de $\prod_{\alpha\in I} R_\alpha$ sobre R_α.

<u>0.24 - TEOREMA</u> - Se R é um anel semisimples então R é produto subdireto de anéis primitivos $(R_\alpha)_{\alpha\in I}$.

<u>0.25 - TEOREMA</u> - Se R é um anel sem ideais nil então R é produto subdireto de anéis primos $(R_\alpha)_{\alpha\in I}$. Além disso R_α não tem ideais nil e para todo $\alpha\in I$, existe $c_\alpha\in R_\alpha$ não nilpotente tal que para todo ideal $U_\alpha \neq (0)$ de R_α existe $n=n(U_\alpha) > 0$ tal que $c_\alpha^n \in U_\alpha$.

Finalmente, enunciaremos aqui o Teorema de Levitzki e introduziremos a noção de anel radical sobre um subanel.

<u>0.26 - TEOREMA</u> - (Levitzki) - Seja R uma anel e $0 \neq \rho$ ideal à direita de R, tal que existe um inteiro n verificando $x^n=0$ para todo elemento $x\in\rho$. Então R contém um ideal nilpotente não nulo. (A demonstração deste teorema está em [8], pág. 1 e 2).

<u>0.27 - DEFINIÇÃO</u> - Seja R um anel e A um subanel de R. Então R diz-se *radical sobre* A (ou A-radical) se para todo $r\in R$, existe um inteiro $n = n(r) \geq 1$ tal que $r^n \in A$.

- ✱ -

CAPÍTULO 1

TEOREMAS DE COMUTATIVIDADE

Em 1905 J. Wedderburn provou que todo anel com divisão finito é um corpo comutativo. A demonstração deste resultado serviu como um início para o estudo de condições sob as quais certos anéis são necessariamente comutativos.

Mais tarde, em 1945, N. Jacobson provou que "se R é um anel tal que para todo $x \in R$, existe $n = n(x) > 1$ tal que $x^n = x$, então R é comutativo" ([9]).

O teorema abaixo é uma generalização do teorema de Jacobson. Ele foi demonstrado primeiramente por I. Kaplansky, em 1951, para anéis semisimples ([10]) e generalizado por I. Herstein em 1953 para um anel R qualquer ([3]). A demonstração deste resultado encontra-se em [7], pág. 79-81.

1.1 - TEOREMA - Seja R um anel com centro $Z(R)$ e suponhamos que R é radical sobre $Z(R)$. Então R é comutativo ou o ideal comutador de R é nil.

Uma generalização do Teorema 1.1, que demonstraremos a seguir, terá grande importância nas demonstrações dos teoremas do Capítulo 2.

1.2 - TEOREMA - Seja R um anel tal que dados $x,y \in R$, existe $n=n(x,y) \geq \geq 1$ tal que $xy^n = y^n x$. Então R comutativo ou o ideal comutador de R é nil.

Demonstração - Suponhamos que R não é comutativo. Então o ideal comutador de R, C(R), é não nulo. Vamos então demonstrar que C(R) é nil.

Seja $c \in C(R)$, $c \neq 0$. Então c é da forma:

$$c = \sum_{i=1}^{m} (a_i b_i - b_i a_i) + \sum_{i=1}^{n} r_i (d_i c_i - c_i d_i) + \sum_{i=1}^{p} (f_i g_i - g_i f_i) s_i$$

$$+ \sum_{i=1}^{q} t_i (h_i k_i - k_i h_i) u_i .$$

Seja S o subanel de R gerado por todos os elementos a_i, b_i, $i=1,\ldots,m$; r_i, d_i, e_i, $i=1,\ldots,n$; f_i, g_i, s_i, $i=1,\ldots,p$; t_i, h_i, k_i, u_i, $i=1,\ldots,q$.

Dado $\sigma \in S$, existe n_1 tal que $\sigma^{n_1} a_1 = a_1 \sigma^{n_1}$. Então chamando $\sigma^{n_1} = \sigma_1$, também existe n_2 tal que $\sigma_1^{n_2} a_2 = a_2 \sigma_1^{n_2}$. Se $\sigma_2 = \sigma_1^{n_2}$ é claro que σ_2 comuta com a_1 e a_2. Repetindo este processo, poderemos encontrar $\ell \geq 1$ tal que σ^ℓ comuta com todos os geradores do anel S. Logo σ^ℓ comuta com todos os elementos de S e consequentemente está em Z(S), isto é, S é radical sobre Z(S).

Por (1.1) temos que ou S é comutativo ou o ideal comutador de S é nil. Mas $c \neq 0$ e $c \in C(S)$, então S não é comutativo. Consequentemente C(S) é um ideal nil, logo c é nilpotente o que conclui a demonstração do teorema. ∎

O teorema acima pode ser aplicado (no caso em que R é um anel com divisão) para demonstrar o seguinte resultado de C. Faith (1958).

<u>1.3 TEOREMA</u> - Seja D um anel com divisão e Δ um subanel próprio de D tal que D é radical sobre Δ. Então D é comutativo.

<u>Demonstração</u> - A demonstração deste toerema seguirá como consequência dos lemas a seguir.

Indicaremos por $Z_D(\{x\})$, o centralizador de $x \in D$ em D, isto é $Z_D(\{x\}) = \{d \in D: dx = xd$ para todo $d \in D\}$.

<u>LEMA 1</u> - Seja D um anel com divisão e Δ um subanel com divisão de D, $\Delta \neq D$. Suponhamos que existam elementos $x \in D \backslash \Delta$ e $d \in \Delta$ tais que d não é radical sobre $Z_D(\{x\})$. Então no máximo um elemento do conjunto $\{(x+c)^{-1}d(x+c): c \in Z_D(\{d\}) \cap \Delta\}$ é radical sobre Δ.

<u>Demonstração</u> - Suponhamos que existam $c_1, c_2 \in Z_D(\{d\}) \cap \Delta$ tais que $(x+c_1)^{-1}d(x+c_1)$ e $(x+c_2)^{-1}d(x+c_2)$ sejam distintos e ambos radicais sobre Δ. Então $((x+c_i)^{-1}d(x+c_i))^{k_i} \in \Delta$ para certos inteiros $k_i \geq 1$, $i=1,2$. Se $n = k_1 k_2$, temos que

$$d_1 = (x+c_1)^{-1}d^n(x+c_1) \quad \text{e} \quad d_2 = (x+c_2)^{-1}d^n(x+c_2)$$

são elementos de Δ.

Logo

$$xd_1 + c_1 d_1 = d^n x + d^n c_1 \tag{1}$$

e

$$xd_2 + c_2 d_2 = d^n x + d^n c_2 \tag{2}$$

Subtraindo (2) de (1) temos

$$x(d_2-d_1)+c_2d_2-c_1d_1 = d^n(c_2-c_1)$$

e daí vem que:

$$x(d_2-d_1) = d^n(c_2-c_1)+c_1d_1-c_2d_2 \in \Delta \qquad (3)$$

Se $d_1-d_2 \neq 0$, multiplicando pelo inverso temos que $x \in \Delta$, contra a hipótese. Logo devemos ter $d_1 = d_2$. De (3) obtemos que

$$0 = d^n(c_2-c_1)-(c_2-c_1)d_1 = (c_2-c_1)d^n-(c_2-c_1)d_1 =$$

$$= (c_2-c_1)(d^n-d_1).$$

Como $c_2-c_1 \neq 0$, temos que $d^n=d_1$ donde $d^n=(x+c_1)^{-1}d^n(x+c_1)$; logo $(x+c_1)d^n = d^n(x+c_1)$. Como $c_1 \in Z_D(\{d\})$, temos que $c_1d^n=d^nc_1$, e podemos cancelar os termos correspondentes e temos que $xd^n = d^nx$. Logo $d^n \in Z_D(\{x\})$ e segue que d é radical sobre $Z_D(\{x\})$ contra a hipótese. ∎

<u>LEMA 2</u> - Seja Δ um subanel de um anel D tal que $\Delta \neq D$ e D é radical sobre Δ. Se para todo par x,d, com $x \in D\setminus\Delta$ e $d \in \Delta$ tivermos que d é radical sobre $Z_D(\{x\})$, então se D não tem ideais nil, D é comutativo.

<u>Demonstração</u> - Vamos provar que para todo par $y,z \in D$, z é radical sobre $Z_D(\{y\})$; isto significa que existe um inteiro $s \geq 1$ tal que $z^sy = yz^s$. Daí por (1.2) concluímos que D é comutativo.

Dados $y,z\in D$, $z\in\Delta$ e $y\notin\Delta$, temos por hipótese que z é radical sobre $Z_D(\{y\})$. Restam então dois casos a estudar:

1º caso - Suponhamos que $y,z\in\Delta$. Seja então $a\in D\backslash\Delta$ arbitrário e sejam m,n inteiros tais que $z^n\in Z_D(\{a\})$ e $(z^n)^m\in Z_D(\{y+a\})$. Então se $k=mn$ temos que $z^k\in Z_D(\{y\})$, logo z é radical sobre $Z_D(\{y\})$.

2º caso - Suponhamos que $z\notin\Delta$. Como D é radical sobre Δ, existe um inteiro $n>1$ tal que $z^n\in\Delta$. Agora, se $y\notin\Delta$, por hipótese z^n é radical sobre $Z_D(\{y\})$, donde z é radical sobre $Z_D(\{y\})$; se $y\in\Delta$, pelo primeiro caso concluímos que z^n é radical sobre $Z_D(\{y\})$, consequentemente z também o é. ∎

LEMA 3 - Se D é um anel com divisão radical sobre um subanel Δ, então Δ também é anel com divisão.

Demonstração - Temos que provar que $1\in\Delta$ e que se $d\in\Delta\backslash\{0\}$ então $d^{-1}\in\Delta$.

Do fato de D ser radical sobre Δ, temos que existe um inteiro $n>0$, tal que $1^n=1\in\Delta$. Logo $1\in\Delta$ e $\Delta\neq 0$.

Seja agora $d\in\Delta\backslash\{0\}$. Seja $n>0$ tal que $(d^{-1})^n\in\Delta$. Então $d^{-1}(d^{-1})^{n-1}\ d^{n-1}=d^{-1}\in\Delta$. ∎

Demonstração do teorema (1.3) - Suponhamos que D não seja comutativo; então pelo lema 2, existem $x,d\in D$, com $d\in\Delta$ e $x\notin\Delta$ tais que d não é radical sobre $Z_D(\{x\})$. Então, pelo lema 1, no máximo um elemento do conjunto:

$$\{(x+c)^{-1}d(x+c):\ c\in Z_D(\{d\})\cap\Delta\}$$

é radical sobre Δ. Como o conjunto acima tem pelo menos dois elementos distintos, a saber, $x^{-1}dx$ e $(x+1)^{-1}d(x+1)$, temos que existe pelo menos um elemento de D que não é radical sobre Δ, contra a hipótese. ∎

Uma possível generalização de (1.2) seria a seguinte: "*Se* R *é um anel tal que dados* $x,y\in R$, *existem* $n=n(x,y)\geq 1$ *e* $m=m(x,y)\geq 1$ *tais que* $x^ny^m=y^mx^n$ *então* R *é comutativo ou o ideal comutador de* R *é nil.*"

Este resultado foi logo demonstrado para anéis semisimples. Daremos aqui sua demonstração. Porém, no caso geral, o problema permaneceu em aberto por algum tempo, tendo sido resolvido em 1975 por I.Herstein usando o resultado fundamental do Capítulo 2 deste trabalho.

Começaremos provando o resultado num caso particular.

<u>1.4 Teorema</u> - Se D é um anel com divisão tal que dados $x,y\in D$, existem $n=n(x,y)\geq 1$ e $m=m(x,y)\geq 1$ tais que $x^ny^m=y^mx^n$ então D é comutativo.

<u>Demonstração</u> - Suponhamos que D não seja comutativo. Então por (1.2), existem $x,y\in D$ tais que $xy^n\neq y^nx$ para todo inteiro $n\geq 1$. O conjunto $\Delta=\{t\in D: ty^m=y^mt$ para algum $n=m(t)\geq 1\}$ é um subanel com divisão de D e $\Delta\neq D$ pois $x\notin\Delta$. Entretanto, dado $t\in D$, existe $n=n(t,y)\geq 1$ tal que $t^n\in\Delta$. Logo por (1.3), D

é comutativo.

1.5 - TEOREMA - Seja R um anel semisimples tal que dados $x, y \in R$, existe $n = n(x,y) \geq 1$ e $m = m(x,y) \geq 1$ tais que

$$x^m y^n = y^n x^m \quad (*)$$

Então R é comutativo.

Demonstração - Sendo R semisimples, por (0.15) R é um produto subdireto de anéis primitivos R_α, $\alpha \in I$. Cada um dos anéis R_α for comutativo teremos que R é comutativo. Logo podemos reduzir o problema ao caso em que R é um anel primitivo.

Suponhamos agora que R é um anel primitivo e sejam M um R-módulo irredutível fiel e $D = \mathrm{Hom}_R(M,M)$. Damos à M uma estrutura de D - espaço vetorial e pode acontecer que $\dim_D M = 1$ ou então $\dim_D M > 1$.

Se $\dim_D M = 1$ temos que R é isomorfo à D donde R é um anel com divisão. Neste caso por (1.4), o teorema já está demonstrado.

Se $\dim_D M > 1$ pode acontecer que:

a) $\dim_D M$ é finita. Neste caso, se $\dim_D M = n$ temos que R é isomorfo à $M_n(D)$ (por (0.5)), ou

b) $\dim_D M$ não é finita, o que implica que dado um inteiro n, existe um subanel S_n de R e um epimorfismo de S_n em R (por 0.6).

Tanto no caso a) quanto no caso b) o anel $M_2(D)$ é imagem homomorfa de um subanel de R. Mas $M_2(D)$ não satisfaz à hipótese (*) pois se:

$$x = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad e \quad y = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

temos $x^2 = x$, $y^2 = y$ e portanto $x^n = x$ para todo inteiro m e ainda é fácil ver que $xy \neq yx$.

Assim devemos ter $\dim_D M = 1$ e R é comutativo. ∎

Observemos que da demonstração de (1.5) segue que todo anel primitivo R tal que para todo par de elementos $x, y \in R$, existem $n = n(x,y) \geq 1$ e $m = m(x,y) \geq 1$ verificando

$$x^n y^m = y^m x^n$$

é necessariamente um corpo. ∎

A demonstração do caso geral de (1.5) será dada no Capítulo 3 deste trabalho.

- ∗ -

CAPÍTULO 2

HIPERCENTRO DE UM ANEL

Os resultados do capítulo anterior mostram que no estudo da comutatividade de anéis é útil considerar elementos que comutam com potências de outros. Isto sugere uma forma natural de estender a noção de centro de um anel.

2.1 - DEFINIÇÃO - Chama-se *hipercentro* do anel R ao conjunto

$$T(R) = \{a \in R:\ ax^n = x^n a,\ n = n(a,x) \geq 1,\ \forall x \in R\}$$

As seguintes propriedades do hipercentro decorrem diretamente da definição:

(1) $T(R) \supset Z(R)$

(2) $T(R)$ é um subanel de R

(3) Se ϕ é um automorfismo de R então $\phi(T(R)) \subset T(R)$.

É fácil ver que $T(R)$ não é necessariamente igual à $Z(R)$. Por exemplo, no caso em que R é um anel nil não comutativo temos $T(R) = R$ e $Z(R) \neq R$. Este é o caso do anel R de todas as matrizes X da forma:

$$X = \begin{bmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & c & 0 \end{bmatrix}$$

onde $a,b,c \in \mathbb{Q}$.

Temos que $X^3 = 0$ para todo $x \in R$ e R não é comutativo.

Nosso próximo objetivo é verificar num anel R qualquer, quão próximos estão T(R) e Z(R). O teorema fundamental deste capítulo mostra que na ausência de ideais nil não triviais de R, as noções de centro e hipercentro coincidem. Tudo o que faremos a seguir será com o objetivo de demonstrar este fato.

Começaremos provando o teorema para anéis com divisão; para isto precisamos do seguinte lema:

2.2 - LEMA (Teorema de Brauer-Cartan-Hua) - Seja D um anel com divisão; se Δ é um subanel com divisão de D tal que $x\Delta x^{-1} \subset \Delta$, para todo $x \in D - \{0\}$, então $\Delta = D$ ou $\Delta \subset Z(D)$.

Demonstração - Suponhamos que $\Delta \neq D$ e seja $x_0 \in D$ tal que $x_0 \notin \Delta$. Se $a \in \Delta$, temos que $x_0\, a\, x_0^{-1} = a_1 \in \Delta$ e $(1+x_0)\, a\, (1+x_0)^{-1} = a_2 \in \Delta$. Logo $x_0 a = a_1 x_0$ e $a + x_0 a = a_2 + a_2 x_0$ de onde vem que $a - a_2 = (a_2 - a_1)x_0$.

Se $a_2 - a_1 \neq 0$, então $(a_2-a_1)^{-1} \in \Delta$, logo

$$(a_2-a_1)^{-1}(a-a_2) = (a_2-a_1)^{-1}(a_2-a_1)x_0 = x_0 \in \Delta,$$

contra a hipótese. Portanto, deve ser $a_2 - a_1 = 0$, de onde vem que $a_2 = a_1$ e que $a = a_2$; logo $x_0 a = a x_0$. Provamos então que se $x_0 \notin \Delta$ e $a \in \Delta$ vale $x_0 a = a x_0$.

Dado $x \in \Delta$, como $x_0 \notin \Delta$, temos que $x + x_0 \notin \Delta$. Seja $a \in \Delta$, então $a(x+x_0) = (x+x_0)a$ e $ax_0 = x_0 a$; logo $ax = xa$.

Assim se $a \in \Delta$ então $ax = xa$ para todo $x \in D$ o que implica que $a \in Z(D)$. ∎

<u>2.3 - TEOREMA</u> - Se D é um anel com divisão então $T(D) = Z(D)$.

<u>Demonstração</u> - É fácil ver que quando D é um anel com divisão, $T(D)$ é um subanel com divisão de D. Como $T(D)$ é invariante sob qualquer automorfismo de D, temos em particular que $d^{-1}T(D)d \subset T(D)$ para todo $d \in D - \{0\}$. Então por (2.2) concluímos que $T(D) \subset Z(D)$ ou $T(D) = D$. No primeiro caso, concluímos que $T(D) = Z(D)$.

Se $T(D) = D$, temos que dados $x, y \in D$, existe $n = n(x,y) \geq 1$ tal que $xy^n = y^n x$. Neste caso D é comutativo por (1.2) e temos $T(D) = D = Z(D)$. ∎

Outro caso particular que provaremos a seguir é aquele em que R é um anel semisimples.

<u>2.4 - TEOREMA</u> - Se R é um anel semisimples então $T(R) = Z(R)$.

<u>Demonstração</u> - Sendo R semisimples, R é produto subdireto de anéis primitivos R_α, $\alpha \in I$. É fácil ver que se $T(R_\alpha) = Z(R_\alpha)$ para todo $\alpha \in I$ então $T(R) = Z(R)$; assim, sem perda de generalidade, podemos assumir que R é primitivo.

Se R é primitivo, seja M um R-módulo (à direita) ir redutível e fiel e $D = Hom_R(M,M)$. Damos à M de modo natural, uma estrutura de D-espaço vetorial (à esquerda) e pelo Teorema de Densidade (0.5) temos que dados $v_1,\ldots,v_n \in M$ linearmente independentes sobre D e $w_1,\ldots,w_n \in M$, existe um elemento $r \in R$ tal que $v_i r = w_i$ para todo $i=1,\ldots,n$.

Se $\dim_D M = 1$ então R é isomorfo à D, e por (2.3) tem se $T(R) = Z(R)$.

Suponhamos então que $\dim_D M > 1$.

Demonstraremos primeiramente que se $v \in M$ e $t \in T(R)$ então v e vt são linearmente dependentes sobre D. Para isto, suponhamos por absurdo que existam $v \in M$ e $t \in T(R)$ tais que v e vt sejam linearmente independentes sobre D. Temos então, pelo Teorema da Densidade que existe $x \in R$ tal que $vx=0$ e $vtx = vt$. Consequentemente $vtx^m = vt$ para todo $m \geq 1$. Como $t \in T(R)$ e $x \in R$, existe $n = n(x,t) \geq 1$ tal que $tx^n = x^n t$. Logo $vt = vtx^n = vx^n t = 0$. Se $vt = 0$ é claro que v e vt não podem ser linearmente independentes sobre D.

Dados $v \in M$ e $t \in T(R)$, temos que $vt = \lambda(v)v$ onde $\lambda(v) \in D$. Fixamos então $t \in T(D)$ e vamos provar que dados $v,w \in M$, linearmente independentes sobre D tem-se que $\lambda(v) = \lambda(w)$.

De fato, temos $vt = \lambda(v)v$, $wt = \lambda(w)w$ e $(v+w)t = \lambda(v+w)(v+w)$ o que implica que, $\lambda(v)v + \lambda(w)w - \lambda(v+w)v - \lambda(v+w)w = 0$ e de onde obtemos que $(\lambda(v) - \lambda(v+w))v + (\lambda(w) - \lambda(v+w))w = 0$. Como v e w são linearmente independentes sobre D vem que $\lambda(v) = \lambda(v+w) = \lambda(w)$.

Como $\dim_D M > 1$ temos que $\lambda(v) = \lambda$ para todo $v \in M$, pois λ é constante sobre elementos linearmente independentes de M sobre D.

Podemos agora concluir a demonstração do teorema. Seja $x \in R$ e $t \in T(R)$. Se $v \in M$, $vx \in M$, e temos $(vx)t = \lambda(vx)$. Por outro lado, $vt = \lambda t$, e então $(vt)x = (\lambda v)x$. Logo $v(xt-tx) = 0$, o que implica que $M(xt-tx) = (0)$. Como M é R-módulo fiel vem que $tx-xt = 0$. Daí segue que $t \in Z(R)$. ∎

A demonstração de que $T(R) = Z(R)$ para um anel R sem ideais nil, será consequência de uma série de proposições e teoremas que demonstraremos a seguir. Entretanto os fatos que provaremos também tem interesse intrínseco e revelam mais algumas propriedades de $T(R)$.

Quando um elemento $a \in Z(R)$ é nilpotente é claro que aR é um ideal à direita nil de R. A proposição seguinte mostra que é suficiente termos $a \in T(R)$ para que a mesma conclusão seja verdadeira.

<u>2.5 - PROPOSIÇÃO</u> - Seja R um anel e a um elemento de $T(R)$. Se a é nilpotente então aR é um ideal à direita nil de R.

<u>Demonstração</u> - Seja $a \neq 0$ um elemento nilpotente de $T(R)$. Queremos provar que se $x \in R$ então ax é nilpotente.

Como a é nilpotente, existe um inteiro $n > 1$ tal que $a^n = 0$ e $a^{n-1} \neq 0$. Como $a^{n-1} \in T(R)$ e $x \in R$, existe um inteiro $m \geq 1$ tal que $(ax)^m a^{n-1} = a^{n-1}(ax)^m = 0$.

Seja então $S = \{i \in N : (ax)^u a^i = 0$ para algum $u \geq 1\}$. Temos que $S \neq \emptyset$ pois $n-1 \in S$; seja então i o menor elemento de S. Então $(ax)^u a^i = 0$ para algum $u \geq 1$. Se $i = 1$ temos que $(ax)^u a = 0$ e, consequentemente que $(ax)^{u+1} = 0$ e logo ax é nilpotente.

Se $i = 2$, temos que $(ax)^u a^2 = 0$ para algum $u \geq 1$, consequentemente $0 = x(ax)^u a \cdot a = (xa)^{u+1} a$. Mas $a \in T(R)$ logo existe $t \geq 1$ tal que $a((xa)^{u+1})^t = ((xa)^{u+1})^t a = 0$. Se $v = (u+1)t$, temos $a(xa)^v = 0$ o que implica que $(ax)^{v+1} = 0$, logo ax é nilpotente. Vamos então provar que $i \leq 2$.

Suponhamos que $i > 2$. Então, $x(ax)^u a \cdot a^{i-1} = 0$, ou seja $(xa)^{u+1} a^{i-1} = 0$; mas $a^{i-1} \in T(R)$, logo existe $s \geq 1$ tal que $0 = ((xa)^{u+1})^s a^{i-1} = a^{i-1}((xa)^{u+1})^s$. Se $r = (u+1)s$, então $a^{i-1}(xa)^r = 0$, logo $a^{i-2} a(xa)^r x = 0$, ou seja $a^{i-2}(ax)^{r+1} = 0$.

Como $a^{i-2} \in T(R)$ existe $v \geq 1$ tal que $a^{i-2}((ax)^{r+1})^v = ((ax)^{r+1})^v a^{i-2} = 0$; mas então $i-2 \in S$ contrariando a minimilidade de i. ∎

<u>2.6 - LEMA</u> - Seja R um anel e T(R) seu hipercentro. Então o conjunto $N = \{x \in T(R) : x$ é nilpotente$\}$ é um ideal de T(R). Além disso $N \subset J(R)$.

<u>Demonstração</u> - Dados $x, y \in T(R)$, existe $n = n(x,y) \geq 1$ tal que $xy^n = y^n x$. Então por (1.2), T(R) é comutativo ou o ideal comutador de T(R) é nil. Se T(R) for comutativo, é claro que N é ideal de T(R). Suponhamos então que T(R) não é comutati

vo, e seja C o ideal comutador de T(R).

O anel $\frac{T(R)}{C}$ é comutativo, e então $\bar{N} = \{\bar{x} \in \frac{T(R)}{C} \mid \bar{x}$ é nilpotente$\}$ é um ideal de $\frac{T(R)}{C}$. É claro que $\frac{N}{C} \subset \bar{N}$. Por outro lado, se $\bar{x} = x+C \in \bar{N}$, existe um inteiro $n \geq 1$ tal que $x^n \in C$; como C é nil, existe $m \geq 1$ tal que $(x^n)^m = 0$, o que implica que $x \in N$. Logo $\bar{x} \in \frac{N}{C}$ e $\bar{N} \subset \frac{N}{C}$.

Temos então $\bar{N} = \frac{N}{C}$. Pelo Teorema da correspondência, N é um ideal de T(R).

Vamos agora provar que $N \subset J(R)$. Seja $a \in N$. Consideremos que $\rho = \mathbb{Z}a + aR$; mostraremos que ρ é um ideal à direita nil de R. A verificação de que ρ é ideal é imediata, ainda, se $y \in \rho$, ele é da forma $y = ma + ax$, $m \in \mathbb{Z}$ e $x \in R$. Como a é nilpotente, ma é nilpotente, logo existe um inteiro $m \geq 1$ tal que $(ma)^n = 0$; então $y^n = (ma+ax)^n = (ma)^n + z = z$ onde $z \in aR$. Por (2.5), aR é nil, e existe um inteiro $k \geq 1$ tal que $z^k = 0$, logo $(y^n)^k = z^k = 0$ e y é nilpotente.

Como J(R) contém todos os ideais à direita nil de R, temos $\rho \subset J(R)$, logo $a \in \rho \subset J(R)$. ∎

2.7 - TEOREMA - Seja R um anel primo sem ideais nil. Então T(R) não tem elementos nilpotentes.

Demonstração - Vamos considerar

$$N = \{x \in T(R) \mid x \text{ é nilpotente}\}.$$

Por (2.6) já sabemos que N é um ideal de T(R) e $N \subset J(R)$.

Vamos supor que $N \neq (0)$ e chegar assim a uma contradição. A demonstração será feita em vários passos.

<u>1º Passo</u> - Se $x \in J(R)$ então $(1+x)N(1+x)^{-1} \subset N$.

Se $x \in J(R)$, a aplicação $\phi: R \longrightarrow R$ definida por $\phi(\chi) = (1+x)y(1+x)^{-1}$ é um automorfismo de R. Como T(R) é invariante sob automorfismos de T(R), temos que $\phi(T(R)) \subset T(R)$, e consequentemente $\phi(N) \subset N$, donde $(1+x)N(1+x)^{-1} \subset N$.

<u>2º Passo</u> - Se $a \in N$ é tal que $a^2 = 0$, então $aRa \subset N$.

Se $x \in R$, por (2.5) ax é nilpotente e $ax \in J(R)$. Logo $(1+ax)a(1+ax)^{-1} \in N$; mas $(1+ax)^{-1} = 1 - ax + (ax)^2 - \ldots \pm (ax)^n$ para algum $n \geq 1$. Como $a^2 = 0$ temos que

$$(1+ax)a(1+ax)^{-1} = (1+ax)a \in N.$$

Desde que $a \in N$ e N é ideal de T(R) temos que $axa \in N$, para todo $x \in R$, logo $aRa \subset N$.

<u>3º Passo</u> - Se $a \in N$ é tal que $a^2 = 0$ e $b \in N$, então $abaJ(R) \subset N$.

Se $y \in J(R)$ e $b \in N$ então

$$(by-yb)(1+y)^{-1} = by(1+y)^{-1} - yb(1+y)^{-1} + b(1+y)^{-1} - b(1+y)^{-1} =$$
$$= b - (1+y)b(1+y)^{-1} \in N$$

já que $b \in N$ e $(1+y)b(1+y)^{-1} \in N$.

Se $x \in R$, então $-ax \in J(R)$ e $(axb-bax)(1-ax)^{-1} \in N$, logo $a(axb-bax)(1-ax)^{-1} \in N$ e como $a^2 = 0$, vem que $abax(1-ax)^{-1} \in N$.

Notamos agora que todo elemento $w \in J(R)$ pode ser es crito na forma $w = x(1-ax)^{-1}$, para algum $x \in R$. Com efeito, basta tomar $x = (wa+1)^{-1}w$ pois calculando temos $(wa+1)x = w$, donde vem que $w - wax = x$ e então $w = x(1-ax)^{-1}$.

Como $abax(1-ax)^{-1} \in N$ para todo $x \in R$, temos então que $abaw \in N$ para todo $w \in J(R)$ donde segue que $abaJ(R) \subset N$.

<u>4º Passo</u> - Se $a \in N$ e $a^2 = 0$ então $aNa = (0)$.

Se $y \in J(R)$ e $b \in N$ então

$$(1+y)abaJ(R)(1+y)^{-1} \subset (1+y)N(1+y)^{-1} \subset N.$$

Mas $J(R)(1+y)^{-1} \subset J(R)$ e se $z \in J(R)$, $z = z(1+y)(1+y)^{-1} \in J(R)(1+y)^{-1}$. Logo $J(R) = J(R)(1+y)^{-1}$, donde vem que $(1+y)abaJ(R) \subset N$.

Como $abaJ(R) \subset N$, temos $yabaJ(R) \subset N$ para todo $y \in J(R)$, logo $J(R)abaJ(R) \subset N$. Mas $J(R)abaJ(R)$ é ideal de R e como está contido em N tem que ser nil. Ainda, como R não tem ideais nil temos que $J(R)abaJ(R) = (0)$.

Mas $J(R)RabaRJ(R) \subset J(R)abaJ(R)$, como R é primo e $J(R) \neq (0)$ temos que $RabaR = (0)$. Consideremos então o conjunto $abaRaba$; do fato de $RabaR = (0)$ vem que $abaRaba$ é um ideal nil de R; logo $abaRaba = (0)$ e como R é primo vem que $aba = 0$.

<u>5º Passo</u> - Se $a \in N$, com $a^2 = 0$ e se $x \in J(R)$ então $axa = 0$ ou $a(1+x)^{-1}a = 0$.

Se b é outro elemento de N tal que $b^2 = 0$, pelo 2º passo temos que $bRb \subset N$. Ainda, dado $a \in N$ tal que $a^2 = 0$, então $abRba \subset aNa = (0)$.

Como R é primo temos $ab = 0$ ou $ba = 0$. Em particular, dado $x \in J(R)$, temos que o elemento $b = (1+x)a(1+x)^{-1} \in N$ e $b^2=0$, mas $ab = 0$ implica que $a(1+x)a(1+x)^{-1} = 0$ de onde vem que $axa = 0$. De $ba = 0$ vem que $(1+x)a(1+x)^{-1}a = 0$ o que implica que $a(1+x)^{-1}a = 0$.

<u>6º Passo</u> - Se $a \in N$, com $a^2 = 0$ e se $x \in J(R)$ é nilpotente então $axa = 0$.

Do 5º passo vem que $axa = 0$ ou $a(1+x)^{-1}a = 0$. Se x é nilpotente, existe $n \geq 1$ tal que $x^n = 0$ e portanto $(1+x)^{-1} = 1 - x + x^2 - \ldots \pm x^{n-1}$.

Faremos a demonstração por indução sobre o índice de nilpotência de x.

Se $x^2 = 0$ então $(1+x)^{-1} = 1 - x$, logo se $a(1+x)a = 0$, como $a^2 = 0$ vem que $axa = 0$.

Suponhamos agora $x \in J(R)$ tal que $x^n = 0$. Se $i > 1$, x^i tem índice de nilpotência menor que n, assim, pela hipótese de indução vem que $ax^ia = 0$.

De $a(1+x)^{-1}a = 0$, vem que $a(1+x+x^2-\ldots\pm x^{(n-1)})a = 0$. Logo $axa = 0$.

<u>7º Passo</u> - Se $a \in N$ e $a^2 = 0$, então $a = 0$.

Sejam $a, b \in N$ tais que $a^2 = b^2 = 0$. Se $x \in R$, por (2.5), $br \in J(R)$ e br é nilpotente, logo $abra = 0$ pelo 6º passo. Então $abRa=0$ e como R é primo vem que $ab = 0$ ou $a = 0$.

Dado $x \in J(R)$, tomamos $b = (1+x)a(1+x)^{-1}$, então $b \in N$ e $b^2=0$. De $ab=0$ vem que $axa(1+x)^{-1}=0$, donde $axa=0$. Logo $aJ(R)a=$

$= 0$ e como R é primo e $J(R) \neq (0)$ temos que $a \neq 0$.

A demonstração do teorema está então concluída, pois supusemos $N \neq (0)$ e tomamos $a \in N$, $a \neq 0$, com $a^2 = 0$, o que é uma contradição com a conclusão obtida no 7º passo, isto é, que $a = 0$. ∎

2.8 - PROPOSIÇÃO - Seja R um anel primo sem ideais nil. Então $T(R)$ é comutativo e um elemento não nulo de $T(R)$ não é um divisor do zero em R.

Demonstração - Dados $x, y \in T(R)$ temos que $xy^n = y^n x$ para algum $n \geq 1$. Por (2.7) temos que $T(R)$ não contém elementos nilpotentes, logo de (1.2) vem que $T(R)$ é comutativo.

Seja agora a um elemento não nulo de $T(R)$ e suponhamos que $au = 0$ para algum elemento $u \in R$. Dado x arbitrário em R o elemento $y = uxa$ é tal que $y^2 = (uxa)(uxa) = 0$ e $ay = a(uxa) = 0$. Mas

$$(1+y)a(1+y)^{-1} = (1+y)a(1-y) = a + ya - ay - yay = a + ya \in T(R).$$

Como $a \in T(R)$ vem que $ya \in T(R)$, mas $(ya)^2 = 0$ e como $T(R)$ não tem elementos nilpotentes temos que $ya = 0$. Ainda como $ya = 0$ e $y = uxa$, vem que $uxa^2 = 0$, para todo $x \in R$, logo $uRa^2 = (0)$.

Como R é um anel primo e $a^2 \neq 0$ vem que $u = 0$. ∎

Sabemos que se R é um anel primo, $Z(R)$ é um domínio de integridade ou é (0). Entretanto, o mesmo não ocorre com $T(R)$. De fato, no caso em que R é um anel primo nil, $T(R) = R$ e obviamente não é um domínio de integridade.

O exemplo abaixo mostra que existem anéis primos nil, e portanto a hipótese do anel R não ter ideais nil, é essencial nas demonstrações de (2.7) e (2.8).

2.9 - EXEMPLO - Seja G o grupo $\mathbb{Z}^{(\mathbb{N})}$ isto é, G é uma soma direta enumerável de cópias de $(\mathbb{Z},+)$. Consideremos uma base B de G, e vamos enumerá-la da seguinte maneira:

$$B = \{b_0, b_1, b_{-1}, \dots, b_n, b_{-n}, \dots\}.$$

Para cada inteiro positivo i, definimos $\mathbb{Z}$-homomorfismos $u_i \colon G \longrightarrow G$, tais que

$$u_i(b_j) = \begin{cases} 0 & \text{se } j \equiv 0 \pmod{2^i} \\ b_{j-1} & \text{se } j \not\equiv 0 \pmod{2^i} \end{cases}$$

Seja R o subanel de $\mathrm{Hom}_{\mathbb{Z}}(G,G)$ gerado por

$$\{u_1, u_2, \dots, u_n, \dots\}.$$

Então todo elemento de R é da forma $x = \sum_{j=1}^{k} x_j$, onde cada somando é da forma

$$x_j = \pm u_{j_{m(j)}} u_{j_{m(j)-1}} \dots u_{j_1} u_{j_0} \quad \text{com } m(j) \geq 0$$

Prova-se, sem dificuldade, por indução sobre m que:

$$(*) \quad u_{i_m} \dots u_{i_1} u_{i_0}(b_j) = \begin{cases} 0 & \text{se } j \equiv n \pmod{2^{i_n}} \text{ para algum} \\ & n \text{ com } 0 \leq n \leq m \\ b_{j-m-1} & \text{se } j \not\equiv n \pmod{2^{i_n}} \text{ para} \\ & \text{todo } n \text{ com } 0 \leq n \leq m \end{cases}$$

Vamos provar que R é um anel primo e nil.

(1) *R é um anel primo*

Para provar este fato faremos a demonstração em vá rios passos.

1º PASSO - Observemos inicialmente que se $x \in R$, $x \neq 0$ e existe $b_\ell \in B$ tal que $x(b_\ell) \neq 0$, então existe $\ell_1 < \ell$ tal que $x(b_{\ell_1}) \neq 0$. De fato:

(a) Começamos considerando um elemento $x \in R$ da forma $x = u_j$, tal que $u_j(b_\ell) \neq 0$, para algum $b_\ell \in B$. Então $\ell \not\equiv 0 \pmod{2^j}$, isto é, $2^j \nmid \ell$. Se $j_1 \geq j$ então $2^j \nmid \ell - 2^{j_1}$, já que $2^j | 2^{j_1}$. Logo se $u_j(b_\ell) \neq 0$ e $\ell_1 = \ell - 2^{j_1}$, temos $u_j(b_{\ell_1}) \neq 0$ e $\ell_1 < \ell$.

(b) Suponhamos agora que x é da forma $x = u_{i_m} \ldots u_{i_0}$ e se $x(b_\ell) \neq 0$ então $\ell \not\equiv n \pmod{2^{i_n}}$ para todo n com $0 \leq n \leq m$. Seja $s = \max\{i_0, \ldots, i_m\}$ e seja $s_1 \geq s$. Tomemos $\ell_1 = \ell - 2^{s_1}$; $2^{i_n} \nmid \ell - 2^{s_1}$, para todo n, $0 \leq n \leq m$, já que $2^{i_n} | 2^{s_1}$. Temos então $x(b_{\ell_1}) \neq 0$ e $\ell_1 < \ell$.

(c) Finalmente, seja x da forma $x = \sum_{i=1}^{k} \alpha_i x_i$, com $x_i \neq x_j$ se $i \neq j$, $\alpha_i \in \mathbb{Z}$, $\alpha_i \neq 0$ e $x_i = u_{i_{m(i)}} \ldots u_{i_1} u_{i_0}$, para cada i=1,...,k. Seja $b_\ell \in B$ tal que $x(b_\ell) \neq 0$ e seja ainda

$$C = \{i,\ 1 \leq i \leq k:\ x_i(b_\ell) \neq 0\}$$

Então,

$$x(b_\ell) = \sum_{i \in C} \alpha_i b_{\ell - m(i) - 1}$$

Para cada $i \in C$, seja $s_i = \max\{i_0, \ldots, i_{m(i)}\}$ e seja

$s = \max\{s_i : i \in C\}$. Se $t \geq s$ e $\ell_1 = \ell - 2^t$, temos que $x_i(b_{\ell_1}) \neq 0$ para cada $i \in C$, logo $x(b_{\ell_1}) = \sum_{i \in C} \alpha_i b_{\ell_1 - m(i) - 1}$

Afirmamos que $x(b_{\ell_1}) \neq 0$. Para isto basta que observemos que $x(b_\ell) \neq 0$ e que sempre que $\ell_1 = m(i) - 1 = \ell_1 - m(j) - 1$ temos que $\ell - m(i) - 1 = \ell - m(j) - 1$.

2º PASSO - Sejam $y \in R$ e $b_j \in B$ tais que $y(b_j) = \sum_{i=1}^{n} \gamma_i \, b_{j_i} \neq 0$, com $j_1 < j_2 < \ldots < j_n$. Seja $s = j_n - j_1$. Afirmamos que para cada k, com $1 \leq k \leq n$, existe uma potência t_k de u_s tal que

$$u_s^{t_k}(b_{j_k}) = 0.$$

De fato, se $j_k = \pm 2^s$, temos $u_s(b_{j_k}) = 0$. Se $j_k > 2^s$, tomamos $t^k = j_k - 2^s + 1$ e se $j_k < 2^s$ tomamos $t^k = j_k + 2^s + 1$. É consequência de (*) que $u_s^{t_k}(b_{j_k}) = 0$.

Seja agora m a menor potência de u_s tal que $u_s^m(b_{j_k}) = 0$ para algum k, com $0 \leq k \leq r$. Mostraremos que se $h \neq k$, com $0 \leq h \leq r$, $u_s^m(b_{j_h}) \neq 0$.

Em caso contrário, por (*) ter-se-ia que $2^s | j_k - m$ e $2^s | j_h - m$, pois m é a menor potência de u_s que anula algum b_{j_k}. Logo $2^s | j_k - j_h$, o que não é possível, já que $|j_k - j_h| \leq s$ e $2^s > s$.

3º PASSO - Sejam $y \in R$ e $b_j \in B$ tais que

$$y(b_j) = \sum_{i=1}^{n} \gamma_i b_{j_i} \neq 0, \text{ com } j_1 < \ldots < j_n.$$

Afirmamos que existe $r \in R$ tal que $ry(b_j) = \gamma b_t$, para algum $b_t \in B$

e $\gamma \in \mathbb{Z}$ não nulo.

Faremos a demonstração por indução sobre n.

Se $n = 1$, temos $y(b_j) = \gamma_1 b_{j_1} \neq 0$. Tomemos neste caso $r = u_i$, de modo que $2^i \mid j_1$. Então temos

$$ry(b_j) = u_i y(b_j) = u_i(\gamma_1 b_{j_1}) = \gamma_1 b_{j_1 - 1} \neq 0.$$

Suponhamos então que $n > 1$ e suponhamos que o resultado seja verdadeiro para $n - 1$.

Temos então $y(b_j) = \sum_{i=1}^{n} \gamma_i b_{j_i} \neq 0$ com $j_1 < \ldots < j_r$. Se tomarmos s e m como no 2º passo temos $u_s^m(y(b_j)) = \sum_{i=1}^{n-1} \gamma_{j_i} b_{\ell_i}$. Mas, pela hipótese de indução, existe $r_1 \in R$ tal que

$$r_1 u_s^m(y(b_j)) = \gamma b_t.$$

Tomando então $r = r_1 u_s^m$ temos $ry(b_j) = \gamma b_t \neq 0$.

4º PASSO - Suponhamos agora que x e y são elementos não nulos de R e vamos provar que $xRy \neq (0)$.

Como $y \neq 0$, existe $b_j \in B$ tal que $y(b_j) \neq 0$. Então

$$y(b_j) = \sum_{i=1}^{n} \gamma_i b_{j_i}, \qquad \gamma_i \in \mathbb{Z} \text{ e } j_1 < \ldots < j_n.$$

Pelo 3º passo, existe $r \in R$ tal que $ry(b_j) = \gamma b_t \neq 0$.

Como $x \neq 0$, existe $b_\ell \in B$ tal que $x(b_\ell) \neq 0$. Pode acontecer que $\ell < t$ ou $\ell \geq t$. Se a segunda possibilidade ocorrer, pelo 1º passo, podemos encontrar $\ell_1 < \ell$, e a fortiori, $\ell_1 < t$ tal que $x(b_{\ell_1}) \neq 0$. Podemos assim sempre supor que $\ell < t$.

Então $t = \ell+h$, $h > 0$. Podemos escolher k tal que $2^k \nmid \ell+h-i$, com $0 \leq i \leq h-1$. Então se $u = u_k^h$, temos por (*) que

$$u(b_t) = b_{\ell+h-h} = b_\ell .$$

Consequentemente temos:

$$xury(b_j) = xur\left(\sum_{i=1}^{r} \gamma_i b_{j_i}\right) = xu(\gamma b_t) = x\gamma(b_\ell) = \gamma x(b_\ell) \neq 0.$$

Logo $xRy \neq (0)$ e R é um anel primo.

(2) R *é um anel nil.*

Seja $x \in R$, então $x = \sum_{i=1}^{k} x_i$, onde $x_i = \pm u_{i_{m(i)}} \ldots u_{i_0}$, com $m_i \geq 0$. Seja

$$h = \max\{2^{i_n},\ 1 \leq i \leq k,\ 0 \leq n \leq m(i)\}.$$

Afirmamos que qualquer produto de u_{i_n}, com $0 \leq i \leq k$, $0 \leq n \leq m(i)$, com pelo menos h elementos é nulo.

De fato, seja $u_{j_{h-1}} \ldots u_{j_1} u_{j_0}$ um tal produto e $j \in \mathbb{Z}$; temos que $j \equiv n \pmod h$ para algum n, com $0 \leq n \leq h$. Como $2^{j_n} | h$ sempre, temos que $u_{j_{n-1}} \ldots u_{j_1} u_{j_0}(b_j) = 0$.

Temos então que $x^h = 0$, já que $x^h = \sum_{i=1}^{m} y_i$, onde cada y_i contém pelo menos h dos u_{i_n}, $1 \leq i \leq h$, $0 \leq n \leq m(i)$.

2.10 - EXEMPLO - Seja R o anel do exemplo anterior e consideremos $\bar{R}$ como sendo o anel gerado por R e a aplicação identidade de R. É claro que todo elemento de $\bar{R}$ é da forma $r = x + mI$, onde $x \in R$, $m \in \mathbb{Z}$ e $I: G \longrightarrow G$ é a identidade.

É fácil ver que $\bar{R}$ é um anel primo, e que R é um ideal nil de $\bar{R}$. Além disso temos que $R \neq \bar{R}$.

Neste caso temos que $T(\bar{R}) = \bar{R}$ e $Z(\bar{R}) = \mathbb{Z}I$.

Observamos que a presença de ideais nil não nulos em $\bar{R}$, torna falsas as conclusões de (2.7) e (2.8).

<u>2.11 - LEMA</u> - Seja R um anel primo sem ideais nil e tal que $\operatorname{car} R \neq 2$. Se um elemento a de R comuta $ax - xa$ para todo x em R, então a pertence à $Z(R)$.

<u>Demonstração</u> - Sejam x e y elementos arbitrários em R; temos que

$$a(a(xy) - (xy)a) = (a(xy) - (xy)a)a \tag{1}$$

Mas $a(xy) - (xy)a = a(xy) - xay + xay - (xy)a$ donde vem que

$$a(xy) - (xy)a = (ax-xa)y + x(ay-ya) \tag{2}$$

Substituindo (2) em (1) e usando que a comuta com $ax - xa$ e $ay - ya$ vem que

$$(ax-xa)ay + ax(ay-ya) = (ax-xa)ya + xa(ay-ya)$$

e daí vem que $2(ax-xa)(ay-ya) = 0$ e como $\operatorname{car} R \neq 2$ temos

$$(ax-xa)(ay-ya) = 0 \tag{3}$$

Seja x um elemento arbitrário de R e seja

$$\rho = (ax-xa)R;$$

ρ é um ideal à direita de R; vamos provar que ρ é nilpotente.

Para isto, observemos inicialmente que a comuta com todo elemento de ρ. De fato:

$$a[(ax-xa)r] - [(ax-xa)r]a = (ax-xa)ar - (ax-xa)ra =$$
$$= (ax-xa).(ar-ra) = 0 \qquad \text{(por (3))}$$

Logo

$$a(ax-xa)r = (ax-xa)ra \text{ para todo } r \in R \qquad (4)$$

Sejam agora $(ax-xa)r$ e $(ax-xa)s$ dois elementos de ρ; vamos provar que $(ax-xa)r(ax-xa)s = 0$.

Mas

$$(ax-xa)r(ax-xa)s = (ax-xa)raxs - (ax-xa)rxas.$$

Usando (4) temos

$$(ax-xa)r(ax-xa)s = a(ax-xa)raxs - (ax-xa)rxas =$$
$$= (ax-xa)arxs - (ax-xa)rxas =$$
$$= (ax-xa)(a(rx)-(rx)a)s = 0 \qquad \text{por (3)}$$

Logo ρ é um ideal à direita nilpotente de R. Se $\rho \neq 0$, então R tem um ideal nilpotente não nulo, contra a hipótese.

Logo $\rho = (0)$ e então $ax - xa = 0$ o que implica que $ax = xa$ e $a \in Z(R)$. ∎

<u>2.12 - TEOREMA</u> - Seja R um anel primo, sem ideais nil e tal que $J(R) = R$. Então $T(R) = Z(R)$.

<u>Demonstração</u> - Seja a um elemento não nulo de $T(R)$ e x e z elementos de R tais que $za = az$ e $zx = xz$. Como $(1+x)a\ (1+x)^{-1}$ e $(1+zx)a\ (1+zx)^{-1}$ estão em $T(R)$ temos que:

$$(1+x)a = a_1(1+x) \tag{1}$$

$$(1+zx)a = a_2(1+zx) \tag{2}$$

Multiplicando (1) à direita por z e subtraindo (2) obtemos:

$$za - a = a_1z - a_2 + (a_1-a_2)zx.$$

Por (2.8), $T(R)$ é comutativo e como a, a_1, $a_2 \in T(R)$ e $za = az$ temos que $a_1z = a_2$ comuta com a.

De (3) concluímos então que $(a_1-a_2)zx$ comuta com a, donde vem que $(a_1-a_2)z(xa-ax) = 0$.

Como $a_1-a_2 \in T(R)$, por (2.8) temos que se $a_1-a_2 \neq 0$, então não é divisor de zero em R, e vem que $z(ax-xa) = 0$.

Se $a_1-a_2 = 0$, de (3) temos que $(a_1-a_2)(1-z) = 0$, logo $0 = (a-a_1)(1-z)(1-z)^{-1} = a-a_1$. De (1) temos que $ax = xa$, logo também neste caso vale que $z(ax-xa) = 0$.

Então, se z é um elemento de R que comuta com $a \in T(R)$ e $x \in R$, temos que $z(ax-xa) = 0$.

Agora, se $a \neq 0$ está em $T(R)$ e $x \in R$, então $ax^n = x^na$, para algum $n = n(a,x) \geq 1$. Tomando $z = x^n$, temos $za=az$ e $zx=xz$, logo $x^n(ax-xa) = 0$ e $x^n(ax-xa)(1+x)^{-1} = 0$.

Como $(xa-ax)(1+x)^{-1} = a-(1+x)a(1+x)^{-1} \in T(R)$, se for não nulo, não é divisor do zero em R.

Logo, se $ax-xa \neq 0$, então $x^n = 0$. Consequentemente a comuta com todos os elementos não nilpotentes de R.

Seja y um elemento de R tal que $ay-ya \neq 0$; então, como $0 \neq (ay-ya)(1+y)^{-1} \in T(R)$ não é divisor do zero em R, temos que $(ay-ya)$ não é divisor do zero em R, logo $ay-ya$ não pode ser nilpotente. Consequentemente $a(ay-ya) = (ay-ya)a$. Logo

$$(ax-xa)a = a(ax-xa) \text{ para todo } x \in R.$$

Se $\text{car} R \neq 2$, por (2.11) temos que $a \in Z(R)$. Assim, se $\text{car} R \neq 2$, $T(R) \subset Z(R)$, logo $T(R) = Z(R)$.

Se $\text{car} R = 2$, temos $a(ax+xa) = (ax+xa)a$ para todo $x \in R$, o que implica que $a^2 x = xa^2$ para todo $x \in R$, logo $a^2 \in Z(R)$.

Tomando $z = a^2$, temos que z comuta com a e x; logo $a^2(ax-xa) = 0$. Como a não é divisor do zero em R, $ax = xa$ para todo $x \in R$, logo $a \in Z(R)$ também neste caso. Temos então que $T(R) \subset Z(R)$ e consequentemente $T(R) = Z(R)$. ∎

Estamos agora em condições de demonstrar o teorema central deste capítulo.

<u>2.13 - TEOREMA</u> - Seja R um anel sem ideais nil. Então $T(R) = Z(R)$.

<u>Demonstração</u> - Como R é um anel sem ideais nil, R é produto subdireto de anéis primos sem ideais nil. Conforme já observamos na demonstração de (2.4) podemos supor sem perda de generalidade que R é um anel primo sem ideais nil.

Se $J(R) = (0)$, então R é semisimples e por (2.4), $T(R) = Z(R)$. Podemos então supor que $J(R) \neq (0)$.

Vamos verificar que mais algumas reduções podem ainda ser feitas, para se demonstrar o teorema.

Observemos inicialmente que se R é anel primo sem ideais nil, como $J(R) \neq (0)$ e se $Z_R(J(R))$ é o centralizador de $J(R)$ em R, i.e., o conjunto

$$Z_R(J(R)) = \{r \in R: rx=xr \text{ para todo } x \in J(R)\},$$

podemos provar que $Z_R(J(R)) \subset Z(R)$.

Com efeito, tomemos $r \in Z_R(J(R))$ e y arbitrário em R. Dado um elemento x em $J(R)$, temos que

$$(ry-yr)x = ryx - yrx = yxr - yxr = 0;$$

logo $(ry-yr)J(R) = (0)$ e como R é primo e $J(R) \neq (0)$ vem que $ry-yr = 0$ donde $r \in Z(R)$.

Da observação anterior vem que para obtermos $T(R) = Z(R)$ é suficiente provar que $T(R)$ centraliza $J(R)$. Afirmamos que para isto será suficiente provar que $T(R) \cap J(R) \subset Z(R)$.

De fato, vamos assumir que $T(R) \cap J(R) \subset Z(R)$ e suponhamos que existam $a \in T(R)$ e $x \in J(R)$ tais que $ax-xa \neq 0$.

Então

$$0 \neq (ax-xa)(1+x)^{-1} = a - (1+x)a(1+x)^{-1} \in T(R),$$

logo tanto $a(ax-xa)(1+x)^{-1}$ quanto $a\,(ax-xa)(1+x)^{-1}$ pertencem à $T(R) \cap J(R)$; logo pertencem à $Z(R)$. Vamos provar que isto implica que a também pertence à $Z(R)$.

De fato, seja $b = (ax-xa)(1+x)^{-1}$; temos que $b \in Z(R)$ e $ab \in Z(R)$. Se $a \notin Z(R)$, existe $y \in R$ tal que $ay-ya \neq 0$. Então

$$b(ay-ya) = bay - bya = aby - yba = aby - yab = 0.$$

Logo $b(ay-ya) = 0$ e $(ay-ya) \neq 0$.

Agora $bR(ay-ya) = Rb(ay-ya) = (0)$; como R é primo, isto é uma contradição.

Logo, devemos ter $ax = xa$ para todo $x \in J(R)$ e para todo $a \in T(R)$.

Agora, para provarmos que $T(R) \cap J(R) \subset Z(R)$ basta observar que, sendo R um anel primo sem ideais nil, J(R) é um anel primo sem ideais nil. Então por (2.12) temos que

$$T(J(R)) = Z(J(R)).$$

Logo

$$T(R) \cap J(R) \subset T(J(R)) = Z(J(R)) \subset Z_R(J(R)) \subset Z(R).$$

Uma consequência imediata de (2.13) é o seguinte teorema:

2.14 - TEOREMA - Seja R um anel e T(R) seu hipercentro. Se $a \in T(R)$ e $x \in R$, então $ax-xa$ gera um ideal nil de R. Em particular, $ax-xa$ é nilpotente para todo $x \in R$.

Demonstração - Seja $a \in T(R)$ e $x \in R$ e seja I o ideal gerado por $ax-xa$. Seja N(R) o radical nil superior de R. Então $\frac{R}{N(R)}$ é um anel sem ideais nil. Consequentemente

$$T\left(\frac{R}{N(R)}\right) = Z\left(\frac{R}{N(R)}\right).$$

Se $a \in T(R)$, então $a + N(R) \in T\left(\frac{R}{N(R)}\right)$, portanto $a + N(R) \in T\left(\frac{R}{N(R)}\right)$.

Se $x \in R$, $x + N(R) \in \frac{R}{N(R)}$; logo

$$(a+N(R))(x+N(R)) - (x+N(R))(a+N(R)) = N(R);$$

logo $ax-xa \in N(R)$. Assim $ax-xa$ é nilpotente e o ideal de R gerado por $ax-xa$ é nil. ∎

<u>2.15 - EXEMPLO</u> - A recíproca do Teorema 2.12 não é em geral verdadeira, isto é, se $a \in R$ é tal que $ax-xa$ gera um ideal nil de R, para todo $x \in R$, a não está necessariamente em $T(R)$.

Para isto, consideremos o anel

$$R = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \middle| \alpha,\beta,\gamma \in \mathbb{Z} \right\}.$$

Seja

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \quad x = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}.$$

Então

$$ax - xa = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} - \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha & \beta+\gamma \\ 0 & \gamma \end{pmatrix} - \begin{pmatrix} \alpha & \alpha+\beta \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} 0 & \gamma-\alpha \\ 0 & 0 \end{pmatrix}$$

que é nilpotente e gera um ideal nil de R. Entretanto, se

$$y = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

temos $y^2 = y$ e $ay \neq ya$, logo $ay^n \neq y^n a$ para todo inteiro $n \geq 1$. Logo $a \notin T(R)$. ∎

CAPÍTULO 3

APLICAÇÕES

§1 - UM TEOREMA DE COMUTATIVIDADE

No Capítulo 1 afirmamos que o seguinte resultado é verdadeiro: "*Se* R *é um anel sem ideais nil tal que dados* $x,y \in R$ *existem inteiros* $n=n(x,y) \geq 1$ *e* $m=m(x,y) \geq 1$ tais que $x^n y^m = y^m x^n$ *então* R *é comutativo.*" e provamos este resultado no caso em que R é semisimples.

Vamos passar agora à demonstração do teorema do caso geral.

3.1 - OBSERVAÇÃO - Se R é um anel tal que dados $x,y \in R$, existem inteiros $n=n(x,y) \geq 1$ e $m=m(x,y) \geq 1$ tais que $x^n y^m = y^m x^n$, podemos supor que $n=m$. Com efeito, basta tomarmos $s=mn$ e temos $s \geq 1$ e $x^s y^s = y^s x^s$. ∎

3.2 - OBSERVAÇÃO - Se R é um anel sem ideais nil então R é produto subdireto de anéis primos $(R_\alpha)_{\alpha \in I}$, sem ideais nil com a propriedade de que existe $c_\alpha \in R_\alpha$ não nilpotente tal que qual quer que seja U_α ideal de R_α, $U_\alpha \neq (0)$, existe $t=t(U_\alpha)\geq 1$ tal que $c_\alpha{}^t \in U_\alpha$. Se R satisfaz à hipótese de que dados $x,y\in R$ existe $n=n(x,y)\geq 1$ tal que $x^n y^n = y^n x^n$, cada R_α preserva também esta hipótese e se provarmos que cada R_α é comutativo teremos que R é comutativo. Podemos então, sem perda de generalidade, assumir que:

(1) R é um anel primo,

(2) R não tem ideais nil,

(3) Existe $c\in R$ não nilpotente tal que para todo ideal $U\neq(0)$ de R, existe $t(U)\geq 1$ tal que $c^{t(U)}\in U$.

<u>3.3 - LEMA</u> - Seja R um anel satisfazendo as hipóteses (1), (2), (3) acima. Se $J(R)\neq(0)$, então $J(R)$ é um subanel de R que também satisfaz à (1), (2), (3).

<u>Demonstração</u> - (1) $J(R)$ é um anel primo

Suponhamos que $aJ(R)b=(0)$ com $a,b\in J(R)$ e suponhamos que $a\neq 0$. Então $aJ(R)\neq(0)$ pois R é primo e $J(R)\neq(0)$. Mas $aJ(R)$ é ideal à direita de R e como $aJ(R)b=(0)$ vem que $b=0$ pois R é primo. Logo $J(R)$ é primo.

(2) $J(R)$ não contém ideais nil

Suponhamos que $A\neq(0)$ é um ideal nil de $J(R)$. Como $J(R)$ é primo, temos que $J(R)AJ(R)\neq(0)$ e também é um ideal nil já que $J(R)AJ(R)\subset A$. Logo $J(R)AJ(R)$ é ideal nil de R, o que não pode ocorrer já que R não tem ideais nil.

(3) $J(R)$ verifica a condição (3)

Como $J(R) \neq (0)$ é ideal de R, existe $t \geq 1$ tal que tal que $d = c^t \in J(R)$. Mostraremos que d está nas condições de (3).

Seja então $A \neq (0)$ um ideal de $J(R)$. Temos que $J(R)AJ(R) \subset A$ é um ideal não nulo de R. Logo existe $k \geq 1$ tal que $c^k \in J(R)AJ(R)$. Temos então que $d^k = (c^t)^k = (c^k)^t \in A$.

<u>3.4 - LEMA</u> - Seja R um anel primo como $J(R) \neq (0)$. Se $J(R)$ é comutativo então R é comutativo.

<u>Demonstração</u> - Sendo $J(R)$ comutativo, temos que $Z(J(R)) = J(R)$. Como R é primo, $Z_R(J(R)) \subset Z(R)$ (ver demonstração de (2.13)). Temos então que $J(R) = Z(J(R)) \subset Z_R(J(R)) \subset Z(R)$. Logo $J(R) \subset Z(R)$.

Se $x,y \in R$ e $r \in J(R)$, temos que $(xy-yx)r = xyr-yxr$. Como $yr, r \in J(R)$ temos $(xy-yx)r = yrx-yrx = 0$. Logo $(xy-yr)J(R) = (0)$. Como R é primo vem que $xy = yx$.

Seja R um anel tal que: (*) dados $x,y \in R$, existe $n = (x,y) \geq 1$ com $x^n y^n = y^n x^n$

(1) R é primo

(2) R não tem ideais nil

(3) existe $c \in R$ não nilpotente tal que qualquer que seja $U \neq (0)$ ideal de R, existe $t(U) \geq 1$ tal que $c^{t(U)} \in U$

(4) $R = J(R)$.

Por (3.1), (3.2), (3.3) e (3.4) temos que se provarmos o teorema para aneis nestas condições então o teorema estará demonstrado em geral.

Daqui em diante R será um anel que satisfaz (*), (1), (2), (3) e (4).

3.5 - PROPOSIÇÃO - Se R não tem divisores do zero então R é comutativo.

Demonstração - Suponhamos que R não seja comutatico. Então existe $x \in R$ tal que $x \notin Z(R)$, e consequentemente, por (2.13), $x \notin T(R)$. Então existe $a \in R$ tal que $ax^m \neq x^m a$ para todo $m \geq 1$. Pela hipótese (*) temos que existe $n \geq 1$ tal que

$$(1+x)a^n(1+x)^{-1}a^n = a^n(1+x)a^n(1+x)^{-1}$$

e

$$(1+ax)a^n(1+ax)^{-1}a^n = a^n(1+ax)a^n(1+ax)^{-1}$$

Seja

$$a_1 = (1+x)a^n(1+x)^{-1} \quad \text{e} \quad a_2 = (1+ax)a^n(1+ax)^{-1}$$

Logo

$$a_1(1+x) = (1+x)a^n \qquad \text{(I)}$$

$$a_2(1+ax) = (1+ax)a^n \qquad \text{(II)}$$

Multiplicando (I) à esquerda por a e subtraindo (II) temos:

$$a^n(a-1) = aa_1 - a_2 + (aa_1-a_2a)x \qquad \text{(III)}$$

Como a, a_1, a_2, a^n comutam com a^n, de (III) vem que

$$(aa_1-a_2a)xa^n = a^n(aa_1-a_2a)x$$

de onde vem que $(aa_1-a_2a)(xa^n-a^nx) = 0$. Como $xa^n \neq a^nx$ e R não tem divisores do zero, temos $aa_1 = a_2a$.

Então (III) reduz-se à

$$a^n(a-1) = aa_1 - a_2 = a_2(a-1).$$

Como $R = J(R)$, $a-1$ é formalmente inversível, logo $a^n = a_2 = a_1$. Mas se $a_1 = a^n$, temos $xa^n = a^nx$, o que é uma contradição. ∎

Com isto o teorema está demonstrado no caso em que R não tem divisores do zero, podemos agora adicionar a hipótese (5) R tem divisores do zero.

O próximo lema vale para anéis primos em geral.

3.6 - LEMA - Se R é um anel primo que tem divisores do zero não triviais, então R tem um elemento nilpotente não trivial.

Demonstração - Existem $b,c \in R$, $b,c \neq 0$ tais que $bc = 0$; como R é primo, temos que $cRb \neq (0)$. Logo existe $r \in R$ tal que $crb \neq 0$; se $a = crb$, temos $a^2 = 0$ e $a \neq 0$. ∎

3.7 - PROPOSIÇÃO - Se $a^2 = 0$, $a \neq 0$, então aR é um ideal à direita nil de R.

Demonstração - Seja x um elemento de R, vamos provar que o elemento ax é nilpotente.

Pela hipótese (*) existe $n \geq 1$ tal que

$$(1+a)(ax)^n(1+a)^{-1} \quad \text{e} \quad (ax)^n$$

comutam.

Como $a^2 = 0$, $(1+a)^{-1} = 1-a$, donde vem que:

$$(1+a)(ax)^n(1-a)(ax)^n = (ax)^n(1+a)(ax)^n(1-a).$$

Desenvolvendo ambos os produtos e cancelando segue que

$$(ax)^{2n} = (ax)^{2n}(1-a) \text{ e assim } (ax)^{2n}a = 0.$$

Consequentemente $(ax)^{2n+1} = 0$. ■

<u>3.8 - PROPOSIÇÃO</u> - Todo divisor do zero em R é nilpotente.

<u>Demonstração</u> - Seja b um divisor do zero em R. Então existe a em R não nulo tal que $ab = 0$.

Sejam $\lambda = \{x \in R \mid xb^m = 0$ para alguma $m \geq 1\}$ e $\rho = \{x \in R \mid b^m x = 0$ para algum $m \geq 1\}$.

Temos que λ é ideal à direita de R e ρ é ideal à esquerda de R.

Queremos provar que existe $t \geq 1$ tal que $b^t = 0$. Para isto provemos inicialmente que $\rho = \lambda$.

Seja então $r \in \lambda$; como $R = J(R)$, existe $r' \in R$ tal que $r + r' + r'r = 0$. Mas $rb^m = 0$, logo $r'rb^m = 0$, o que implica que $r'b^m = 0$, donde $r' \in \lambda$.

Pela hipótese (*), existe $n \geq 1$ tal que

$$(1+r)b^{mn}(1+r')b^{mn} = b^{mn}(1+r)b^{mn}(1+r').$$

Usando que $rb^m = r'b^m = 0$, obtemos que $b^{2mn} = b^{2mn}(1+r')$; logo $b^{2mn}r' = 0$ e $r' \in \rho$. Então $b^{2mn}r = 0$ e $r \in \rho$. Daí temos que $\lambda \subset \rho$. Analogamente provamos que $\rho \subset \lambda$ e temos $\rho = \lambda$.

Logo λ é um ideal bilateral de R e é não nulo pois $a \in \lambda$.

Pela hipótese (3) existe $c \in R$ e $k \geq 1$ tal que $c^k \in \lambda$, logo $c^k b^t = 0$, para algum $t \geq 1$.

Seja $U = \{x \in R: c^m x = 0$ para algum $m \geq 1\}$. Do mesmo modo que provamos que $\lambda = \rho$, provamos que U é ideal de R.

Se $U \neq (0)$, existe $\ell \geq 1$, tal que $c^\ell \in U$; logo $c^{\ell+r} = 0$, o que não pode ocorrer já que c não é nilpotente; logo $U = (0)$. Entretanto, $b^t \in U$, o que acarreta que b é nilpotente. ∎

<u>3.9 - PROPOSIÇÃO</u> - Se R não for comutativo então R é livre de torção.

<u>Demonstração</u> - Sendo R não comutativo, R tem divisores do zero e por (3.6) existe $a \in R$, $a \neq 0$ com $a^2 = 0$.

Dado um elemento x em R, existe um inteiro $k \geq 1$ tal que $(1+a)x^k(1+a)^{-1}x^k = x^k(1+a)x^k(1+a)^{-1}$ e como $(1+a)^{-1} = 1-a$, obtemos que

$$ax^{2k} - 2x^k a x^k + x^{2k} a = a x^k a x^k - x^k a x^k a \qquad \text{(I)}$$

Também existe um inteiro $\ell \geq 1$ tal que

$$(1-a)x^\ell(1-a)^{-1}x^\ell = x^\ell(1-a)x^\ell(1-a)^{-1}.$$

Desta igualdade obtemos que:

$$ax^{2\ell} - 2x^\ell a x^\ell + x^{2\ell} a = x^\ell a x^\ell a - a x^\ell a x^\ell. \qquad \text{(II)}$$

Suponhamos agora que R não é livre de torção. Então, como R é um anel primo, $\mathrm{car}R = p$, onde p é um número primo.

Vamos estudar inicialmente o caso em que $\mathrm{car}R \neq 2$.

Podemos encontrar um inteiro $n \geq 1$ tal que (I) e (II) sejam verificadas simultaneamente (por exemplo, $n = k\ell$).

Daí, somando (I) e (II) obtemos que:

$$2(ax^{2n}-2x^nax^n+x^{2n}a) = 0.$$

Como $\text{car}R \neq 2$ vem que $ax^{2n}-2x^nax^n+x^{2n}a = 0$, isto é,

$$(ax^n-x^na)x^n = x^n(ax^n-x^na) \qquad \text{(III)}$$

Usando (III) podemos provar por indução finita que $ax^{mn} - x^{mn}a = mx^{n(m-1)}(ax^n-x^na)$, para todo inteiro $m > 1$.

Mas $\text{car}R = p$, logo $ax^{pn} - x^{pn}a = px^{n(p-1)}(ax^n-x^na) = 0$. Então $ax^{pn} = x^{pn}a$ o que implica que $a \in T(R)$. Por (2.13) temos que $a \in Z(R)$. Mas a é nilpotente e o centro de um anel primo ou é (0) ou é um domínio de integridade. Logo $\text{car}R = p \neq 2$ não é possível.

Vamos então ver o que ocorre se $\text{car}R = 2$. De (I) vem que

$$ax^{2k} + x^{2k}a = (ax^k)^2 + (x^ka)^2.$$

Seja $y = x^k$; então $ay^2 + y^2a = (ay)^2 + (ya)^2$. Multiplicando por a à esquerda e usando que $a^2 = 0$ temos $ay^2a = a(ya)^2$.

Seja $r \geq 1$ um inteiro tal que $(1+a)y^r(1+a)^{-1}$ comuta com y^r, então temos que

$$ay^{2r} + y^{2r}a = (ay^r)^2 + (y^ra)^2, \qquad \text{(IV)}$$

logo

$$ay^{2r}a = (ay^r)(ay^r)a \qquad \text{(V)}$$

Por (3.7) o ideal à direita aR é nil, e então $(ay)^{2^m} = 0$ para algum $m \geq 1$.

Mas usando (V) e indução finita provamos que

$$(ay)^{2^\ell} a = ay^{2^\ell} a, \text{ para todo inteiro } \ell \geq 1.$$

Logo

$$ay^{2^m} a = (ay)^{2^m} a = 0. \qquad \text{(VI)}$$

De (V) e (VI) obtemos que

$$ay^{2^{m+1}} + y^{2^{m+1}} a = (ay^{2^m})^2 + (y^{2^m} a)^2 = 0,$$

e daí vem que $ay^{2^{m+1}} = y^{2^{m+1}} a$. Como $y = x^k$, temos que

$$ax^{2^{m+1}k} = x^{2^{m+1}k} a.$$

Logo $a \in T(R)$ e consequentemente $a \in Z(R)$. Como a é nilpotente e R é primo, temos novamente uma contradição. ∎

Observemos que da demonstração acima, obtivemos também que sendo R livre de torção, se $a^2 = 0$ e $x \in R$, então $(ax^n - x^n a)x^n = x^n(ax^n - x^n a)$, para algum inteiro $n \geq 1$. Temos então o seguinte lema:

<u>3.10 - LEMA</u> - Seja $a \neq 0$ um elemento de R tal que $a^2 = 0$. Então, dado $x \in R$, existe um inteiro $n \geq 1$ tal que

$$(ax^n - x^n a)x^n = x^n(ax^n - x^n a).$$

<u>3.11 - LEMA</u> - Seja R um anel livre de 2-torção e sejam $a, b \in R$. Suponhamos que $a^2 = 0$ e que $(ab - ba)b = b(ab - ba)$. Então para qualquer $n \geq 3$, tem-se que

$$(a+b)^n = b^n + nb^{n-1}a + \frac{n(n-1)}{2} b^{n-2}(ab-ba) + \frac{n(n-1)(n-2)}{6} b^{n-3}aba.$$

Também temos que $abab^i = b^i aba$ para qualquer $i \geq 1$.

Demonstração - A demonstração da primeira parte deste lema segue por indução sobre n.

Se $(ab-ba)b = b(ab-ba)$ então $ab^2 + b^2a = 2bab$, logo $ab^2a = 2abab$ e $ab^2a = 2baba$. Como car $R \neq 2$, $(aba)b = b(aba)$, donde segue que $(aba)b^i = b^i(aba)$ para todo $i \geq 1$. ∎

Podemos agora concluir a demonstração do teorema:

Suponhamos então que R não seja comutativo. Temos então a seguinte situação: R é primo, livre de torção, sem ideais nil, tem divisores do zero e todos seus divisores do zero são nilpotentes. Além disto, por (3.10) se $a \neq 0$ e $a^2=0$, dado $x \in R$, existe um inteiro $n \geq 1$ tal que

$$(ax^n-x^na)x^n = x^n(ax^n-x^na).$$

Vamos provar que tudo isto nos leva a uma contradição.

Queremos provar que dado $x \in R$ e $a^2 = 0$, então $ax^r = x^ra$ para algum $r \geq 1$.

Se x é um divisor do zero, então x é nilpotente, logo $x^r = 0$ para algum $r \geq 1$ e $ax^r = x^ra$.

Suponhamos então que x não é divisor do zero. Então, para algum $n \geq 1$ temos $(ax^n-x^na)x^n = x^n(ax^n-x^na)$.

Seja $b = x^n$. Pela hipótese (*), existe um inteiro $m \geq 1$ tal que $(a+b)^mb^m = b^m(a+b)^m$. Podemos tomar $m \geq 3$.

Por (3.11) temos

$$(a+b)^m = b^m + mb^{m-1}a + \frac{m(m-1)}{2} b^{m-2}(ab-ba) + \frac{m(m-1)(m-2)}{6} b^{m-3}aba.$$

Temos que b^m, $b^{m-2}(ab-ba)$ e $b^{m-3}aba$ comutam com b e consequentemente com b^m e também $(a+b)^m$ comuta com b^m. Logo $mb^{m-1}a$ comuta com b^m e então $mb^{m-1}ab^m = b^m(mb^{m-1}a)$. Daí vem que $mb^{m-1}(ab^m-b^ma) = 0$.

Como R é livre de torção e $b = x^n$ não é divisor do zero, temos $ax^{mn} = x^{mn}a$.

Logo a comuta com uma potência de cada elemento de R e então $a \in T(R)$. Como R não tem ideais nil, $a \in Z(R)$. Mas a é nilpotente e um anel primo não tem nilpotentes centrais. Esta contradição demonstra o Teorema. ∎

<u>3.12 - OBSERVAÇÃO</u> - Em 1970 A.I.Lihtman [12] demonstrou o seguinte Teorema:

"Se R é um anel sem ideais nil e é radical sobre um subanel comutativo então R é comutativo."

O Teorema de Lihtman, é claramente um caso particular do resultado que demonstramos. De fato: Se R é radical sobre um subanel comutativo A de R, então dados $x,y \in R$, existem $n = n(x) \geq 1$ e $m = m(y) \geq 1$ tais que $x^n \in A$ e $y^m \in A$. Logo $x^n y^m = y^m x^n$. Se R não tem ideais nil, então R é comutativo.

Utilizando os Teoremas (2.13) e (1.2) podemos também demonstrar o Teorema de Lihtman.

Seja R radical sobre um subanel comutativo A, e sejam $a \in A$ e $x \in R$. Existe $n = n(x) \geq 1$ tal que $x^n \in A$; logo $ax^n = x^n a$, donde se conclui que $A \subset T(R)$.

Como R não tem ideais nil, vem que $T(R) = Z(R)$ e então $A \subset Z(R)$. Temos então que R é radical sobre seu centro e pelo Teorema (1.2), R é comutativo. ∎

§2 - ANÉIS RADICAIS SOBRE SUBANÉIS

O Teorema de Lihtman, nos diz que se um anel R é radical sobre um subanel comutativo A e se R não tem ideais nil, então R é comutativo.

Estes fatos nos motivam a estudar quais as propriedades de A são propriedades de R, quando soubermos que R é radical sobre A.

O teorema que aqui apresentaremos foi demonstrado por B. Felzenswalb, utilizando o Teorema (2.12).

Vamos provar que "*se* R *é um anel sem ideais nil e* R *radical sobre um subanel* A *que não tem elementos nilpotentes, então* R *não tem elementos nilpotentes*". Começaremos com o seguinte teorema:

3.13 - TEOREMA - Seja R um anel tal que R é radical sobre um subanel A. Se A não tem ideais à direita nil, então $N(R)$ contém todo ideal lateral nil de R.

Demonstração - Observemos que $\frac{R}{N(R)}$ é radical sobre $\frac{A+N(R)}{N(R)}$, desde que R é A-radical.

Mas $\frac{A+N(R)}{N(R)} \cong \frac{A}{A \cap N(R)} \cong A$ já que $A \cap N(R)$ é ideal nil de A e portanto $A \cap N(R) = (0)$.

Logo $\frac{R}{N(R)}$ é radical sobre A. Com isto, podemos reduzir ao caso em que R não tem ideais nil, isto é, que $N(R) = (0)$.

(i) Vamos provar o teorema inicialmente no caso em que R é livre de 2-torção.

Suponhamos que $\rho \neq (0)$ é ideal à direita nil de R. Afirmamos que existe $x \in \rho$, com $x^k = 0$, $x^{k-1} \neq 0$ e $k \geq 6$. De fato, se $x^5 = 0$ para todo $x \in \rho$, pelo Teorema de Levitzki, R teria um ideal nilpotente não trivial, o que não pode ocorrer já que R não tem ideais nil.

Se k é impar, $\frac{3(k-1)}{2} \geq k$ logo $\left(x^{\frac{k-1}{2}}\right)^3 = 0$.

Se k é par, $\frac{3(k-2)}{2} \geq k$ e $\left(x^{\frac{k-2}{2}}\right)^3 = 0$.

Tomando $y = x^{\frac{k-1}{2}}$ no caso em que k é impar e $y = x^{\frac{k-2}{2}}$ no caso em que k é par, temos $y^3 = o$ e $y^2 \neq 0$ (pois $x^{k-1} \neq 0$) e $y \in \rho$. Dado um elemento r em R, sempre podemos encontrar um inteiro n tal que:

(1) $r^n \in A$

(2) $(1+y)r^n(1+y)^{-1} = ((1+y)r(1+y)^{-1})^n \in A$

(3) $(1-y)x^n(1-y)^{-1} \in A$

(4) $(1+y)^{-1}r^n(1+y) \in A$

(5) $(1-y)^{-1}r^n(1-y) \in A$.

Como $y^3 = 0$, vem que $(1+y)^{-1} = 1-y+y^2$ e $(1-y)^{-1} = 1 + y + y^2$.

Desenvolvendo (2) e (3) e somando, obtemos que

$$2r^n + 2r^n y^2 - 2yr^n y \in A;$$

como $r^n \in A$, temos $2(r^n y - yr^n)y \in A \cap Ry$.

Mas Ry é um ideal à esquerda nil de R (pois $y \in \rho$ e ρ é ideal à direita nil de R). Logo $A \cap Ry$ é ideal à esquerda nil de A e então $A \cap Ry = (0)$.

Consequentemente $2(r^n y - yr^n)y = (0)$.

Analogamente, de (1), (4), (5) vem que

$$2y(-r^n y + y\ r^n) \in A \cap yR = (0).$$

Logo temos que $r^n y^2 = yr^n y = y^2 r^n$, já que R é livre de 2-torção.

Então, dado r arbitrário em R, encontramos $n \geq 1$ tal que $y^2 r^n = r^n y^2$, o que implica que $y^2 \in T(R)$. Como R não tem ideais nil, vem que $y^2 \in Z(R)$ (por 2.13).

Mas sendo y^2 nilpotente e central, y^2 gera um ideal nil de R, o que não é possível já que R não tem ideais nil. Logo $\rho = (0)$.

(ii) Suponhamos agora que $2R = (0)$. Seja $\rho \neq (0)$ ideal à direita nil de R. Raciocinando do mesmo modo que (i) podemos encontrar $x \in \rho$ tal que $x^3 = 0$ e $x^2 \neq 0$. Dado $a \in A$, seja $n \geq 1$ tal que:

(1) $(1+x)a^n(1+x)^{-1} \in A$

(2) $(1+x)^{-1}a^n(1+x) \in A$

(3) $(1+x^2)a^n(1+x^2)^{-1} \in A$.

Notemos que como $x^2 + x^2 = 0$ e $x^3 = 0$ então $(1+x^2)^{-1} = 1 + x^2$.
Desenvolvendo (1), (2) e (3) e somando, obtemos

$$a^n + xa^nx^2 + x^2a^nx + x^2a^nx^2 \in A.$$

Como $a^n \in A$, temos que $a_1 = xa^nx^2 + x^2a^nx + x^2a^nx^2 \in A$. Entretanto $a_1 \in \rho$, também, já que $x \in \rho$.
Logo $a_1 \in A \cap \rho = (0)$ já que $A \cap \rho$ é ideal à direita nil de A.

Daí vem que $0 = xa_1 = x^2a^nx^2$, e de (3) vem que

$$a^nx^2 + x^2a^n \in A.$$

Seja $b \in A$ e seja $c = (x^2a^n + a^nx^2)b$. Então $x^2c = 0$.

Mas $c \in A$, e pelo que provamos acima, existe $m \geq 1$ tal que $c^mx^2 + x^2c^m \in A$. Logo $c^mx^2 \in A$, já que $x^2c = 0$. Então temos que $c^mx^2 \in A \cap Rx = (0)$, pois $A \cap Rx \subset A \cap \rho = (0)$.

Mas $c^{m+1} = c^m(x^2a^n + a^n x^2)b = c^ma^nx^2b \in Rx^2b$. Agora, Rx^2b é ideal à esquerda nil de R; logo c^{m+1} é nilpotente o que implica que c é nilpotente.

Como b é um elemento qualquer de A, temos que $(x^2a^n + a^nx^2)A$ é ideal à direita nil de A. Mas A não tem ideais à direita nil, logo temos que $x^2a^n = a^nx^2$.

Do fato de R ser A-radical, temos que dado $r \in R$, existe $t \geq 1$ tal que $r^t \in A$. Pelo que provamos acima, temos que $x^2r^{tn} = x^2r^{tn}$ para algum $n \geq 1$; logo $x^2 \in T(R)$ e portanto $x^2 \in Z(R)$, pois R não tem ideais nil.

Novamente, como R não tem ideais nil, obtemos um elemento nilpotente em Z(R) é uma contradição. ∎

Com isto, podemos agora provar o seguinte teorema:

<u>3.14 - TEOREMA</u> - Seja R um anel sem ideais nil que é radical sobre um subanel A. Se A não tem elementos nilpotentes, então R não tem elementos nilpotentes.

<u>Demonstração</u> - Vamos provar que se existisse $x \in R$ nilpotente, então R teria um ideal à direita nil.

Seja então $x \in R$, $x \neq 0$ nilpotente e seja n um inteiro positivo tal que $x^n = 0$ e $x^{n-1} \neq 0$. Tomando $a = x^{n-1}$; é claro que $a^2 = 0$.

Dado um elemento r em R existe $n \geq 1$ tal que $(ar)^n \in A$ e $(1+a)(ar)^n(1-a) \in A$. Daí decorre que $(ar)^n a \in A$.

Chamando $b = (ar)^n a$, temos que $b^2 = 0$ e consequentemente $b = 0$, já que A não tem elementos nilpotentes.

Logo $(ar)^n ar = (ar)^{n+1} = 0$, o que implica que aR é ideal à direita nil de R.

Como A não tem elementos nilpotentes, A não tem ideais à direita nil, logo, por (3.13), $aR \subset N(R)$. Como $N(R) = (0)$ temos que $aR = (0)$.

Se considerarmos $\rho = \mathbb{Z}a + aR = \mathbb{Z}a$ temos que ρ é um ideal à direita nil de R; novamente por (3.13), $\rho \subset N(R) = (0)$. Daí vem que $a = 0$, o que é uma contradição.

Consequentemente R não tem elementos nilpotentes não nulos. ∎

- □ -

REFERÊNCIAS

[1] - Faith,C. "Algebraic division rings extensions", *Proc. Amer. Math. Soc.*, *11*, (1960), 43-53.

[2] - Felzenswalb, B. "Rings radical subrings", *Israel J. of Math.*,*Vol. 23, nº 2*, (1976), 156-164.

[3] - Herstein, I.N., "A theorem on rings", *Canad. J. Math.*, *5*, (1953), 238-241.

[4] - Herstein, I.N., "Two remarks on the commutativity of rings", *Canad. J. Math.*, *7*, (1955), 411-412.

[5] - Herstein, I.N., "On the hypercenter of a ring", *J. of Algebra*, *36*, (1975), 151-157.

[6] - Herstein, I.N., "A commutativity theorem", *J. of Algebra*, *38*, (1976), 112-118.

[7] - Herstein, I.N., *Noncommutative rings*, Carus Monograph nº 15, Mathematical Association of America, Washington,D.C., 1968.

[8] - Herstein, I.N., *Topics in ring theory*, Chicago Lectures in Mathematics, University of Chicago Press, IL, 1969.

[9] - Jacobson,N., "Structure theory for algebraic algebras of bounded degree", *Ann. of Math.*, *46*, (1945), 695-707.

[10] - Jacobson,N., *Structure of rings*, American Mathematical Society, Colloquium Publications, (1956).

[11] - Kaplansky,I., "A theorem on division rings, *Canad. J. Math.*, *3*, (1951), 290-292.

[12] - Lihtman, A.I., "On rings radical over commutative subrings, *Mat. Sbornik, Tom. 83 (125), nº 4*, (1970), 511-521.

- □ -