Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

UM TEOREMA DE DENSIDADE PARA ANÉIS FRACAMENTE PRIMITIVOS

Dissertação de Mestrado

THAÍSA RAUPP TAMUSIUNAS

Porto Alegre, 11 de abril de 2008

Dissertação submetida por Thaísa Raupp Tamusiunas* , como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Prof. Dr. Alveri Alves Sant'Ana

Banca examinadora:
Prof. Dr. Alveri Alves Sant'Ana (IM - UFRGS, ORIENTADOR)
Prof. Dr. Antônio Paques (IM - UFRGS)
Prof. Dr. Miguel Angel Alberto Ferrero (IM - UFRGS)
Profª. Dra. Virgínia Silva Rodrigues (DEPTO de MAT - UFSC)

*Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

DEDICATÓRIA

Dedico esta dissertação aos meus pais, pelo apoio incondicional em todos os momentos.

Agradecimentos

Agradeço aos Mestres Luis Gustavo Doninelli Mendes, Alexandre Tavares Baraviera e Cydara Cavedon Ripoll, pelo exímio dom de dar aulas de Matemática, pela atenção, simpatia e por serem excelentes profissionais que eu desejo muito seguir.

Agradeço aos colegas André, Hugo, Débora, João, Vitalino e Marcelo, pelos momentos de estudo, por ajudarem a tirar minhas dúvidas e por tornarem minha vida acadêmica mais agradável e descontraída.

Agradeço à secretária da pós-graduação Rosane, por quebrar meu galho várias vezes no decorrer do curso.

Agradecimento especial ao meu professor e orientador Alveri Alves Sant'Ana, pela paciência, tempo e dedicação ao meu trabalho, me agüentando por dois seminários semanais e me ensinando Matemática com uma didática inigualável.

Agradeço aos meus pais, Sérgio e Marli, pelo incentivo ao estudo, pela ajuda financeira e por deixarem dentro de casa durante todos esses anos o meu maior exemplo: eles próprios.

Agradeço à vó Dina, pelas orações nos momentos difíceis, à minha irmã Michele, pelas correções ortográficas e dicas de português, e ao meu irmão Fabrício, pelo chopp nas horas em que eu precisava desopilar.

Agradeço ao meu namorado Eládio, pelos softwares matemáticos instalados no meu computador, pelo companheirismo e pela quase compreensão pelas infinitas vezes que precisei estar na UFRGS.

Agradeço às amigas Lívia e Kerlin, tio Laércio e tia Célia, por serem peças fundamentais na minha vida, meus alicerces fora da vida acadêmica.

Agradeço ao Zelmanowitz, por ter escrito o artigo “Weakly Primitive Rings”, sem o qual esta dissertação não existiria.

E por último, mas não menos importante, agradeço à mim, por ter me superado e aprendido coisas que eu jamais imaginei que conseguiria.

A todos vocês, muito obrigada.

Resumo

Um anel fracamente primitivo é aquele que possui um módulo criticamente compressível e fiel. O objetivo desta dissertação é estudar um teorema de densidade para anéis fracamente primitivos.

Abstract

A weakly primitive ring is a ring which has a faithful critically compressible module. The purpose of this dissertation is to study a density theorem for weakly primitive rings.

Índice

Introdução

O objetivo deste trabalho é tratar sobre a densidade em anéis fracamente primitivos. Essa escolha de terminologia foi dada por Julius Zelmanowitz, e deve-se ela ao ponto inicial dos estudos, que foi tratar de uma generalização do clássico Teorema da Densidade de Jacobson.

O Teorema da Densidade de Jacobson é uma importante generalização do Teorema de Wedderburn-Artin. Mais detalhadamente, se R é um anel e D é o anel de todos endomorfismos de M, onde M é um R-módulo à direita simples, então, pelo Lema de Schur, D é um anel de divisão. Tratando M como um espaço vetorial sobre um anel de divisão, então dados qualquer conjunto de vetores linearmente independentes sobre D, e qualquer outro conjunto de vetores com a mesma quantidade de elementos, existe um elemento $r \in R$ que associa cada vetor do primeiro conjunto a um vetor do segundo. Em particular, quando R é primitivo (ou seja, quando possui um módulo simples e fiel), então ele é isomorfo a um subanel denso de transformações lineares de um espaço vetorial sobre um anel de divisão.

Tendo ciência desta situação para anéis primitivos, Zelmanowitz percebeu que, com algumas adaptações, esse resultado podia ser expandido para uma classe maior de anéis, os chamados anéis fracamente primitivos. Para isto, foi preciso generalizar a noção de módulos simples (os assim chamados módulos criticamente compressíveis), bem como a noção de densidade (que chamaremos de "densidade fraca"). De forma sucinta, uma parte do teorema da densidade generalizado diz o seguinte: um anel R tem um módulo criticamente compressível e fiel se , e somente se, R é um subanel fracamente denso de transformações lineares de um espaço vetorial sobre um anel de divisão. Mais precisamente, se M é um R-módulo criticamente compressível e fiel, e $\overline{M}$ denota o fecho quase-injetivo de M, então $\Delta = End(\overline{M}_R)$ é um anel de divisão e R é um subanel fracamente denso do anel $End_\Delta(\overline{M})$. Reciprocamente, se R é um subanel fracamente denso de um anel $End_\Delta(V)$ para algum Δ-espaço vetorial V, então para uma escolha adequada de v em V, vR será um R-módulo criticamente compressível e fiel.

A fim de manter uma razoável organização na apresentação dos resultados, dividimos este trabalho em três capítulos, ordenados da seguinte maneira: no Capítulo 1, veremos alguns resultados preliminares para a teoria que segue, destacando, dentre eles, o Teorema de Wedderburn-Artin. No Capítulo 2, introduziremos a noção de primitividade e trabalharemos com alguns resultados básicos, chamando atenção aqui para o Teorema da Densidade de Jacobson-Chevalley e para o teorema que fornece uma estrutura para anéis primitivos à direita. Grande parte destes resultados foram retirados do livro "A First Course in Noncommutative Rings", de T. Y. Lam, livro este que contribuiu consideravelmente para o desenvolvimento deste trabalho. No Capítulo 3, apresentaremos os módulos criticamente compressíveis e algumas de suas caracterizações, e o Teorema da Densidade com algumas conseqüências, mostrando, em particular, que todo anel fracamente primitivo é primo.

Por toda esta dissertação, anéis não são necessariamente comutativos, e R^1 vai denotar R adjunção com o conjunto dos inteiros, e será utilizado quando o anel R não possuir unidade. Demais notações serão introduzidas no decorrer do texto.

Capítulo 1

Pré-requisitos

Começaremos este trabalho enunciando alguns resultados básicos para a teoria que sucede. Como foi dito na Introdução, grande parte destes resultados podem ser encontrados em §2, §3, §4 e §10 de [9].

1.1 Lema de Zorn

O Lema de Zorn é um axioma da Teoria dos Conjuntos, e será freqüentemente usado neste trabalho.

Lema de Zorn. *Se, em um conjunto A não-vazio e parcialmente ordenado, todo subconjunto $S \subseteq A$ totalmente ordenado tem uma cota superior em A, então A tem um elemento maximal.*

1.2 Condições de Cadeia

Dizemos que uma família de subconjuntos $\{C_i : i \in I\}$ em um conjunto C satisfaz a Condição da Cadeia Ascendente (ACC, do inglês *Ascending Chain Condition*) se não existir uma cadeia estritamente ascendente infinita

$$C_{i_1} \subsetneqq C_{i_2} \subsetneqq ...$$

na família. As seguintes formulações são equivalentes a esta condição:

(1) Para qualquer cadeia ascendente $C_{i_1} \subseteq C_{i_2} \subseteq ...$ na família, existe um inteiro n tal que $C_{i_n} = C_{i_{n+1}} = C_{i_{n+2}} = ...$

(2) Qualquer subfamília não-vazia de uma família dada tem um elemento maximal (com respeito à inclusão).

A Condição da Cadeia Descendente (DCC, do inglês *Descending Chain Condition*) para uma família de subconjuntos de C é definida similarmente, e podemos fazer uma analogia às afirmações (1) e (2).

Definição 1.2.1. *Sejam R um anel e M um R-módulo à direita. Dizemos que o módulo M é* Noetheriano*(resp.,* Artiniano*) se a família de todos os submódulos de M satisfaz ACC (resp., DCC).*

1.3 Estrutura de Anéis Semi-simples

Começaremos esta seção enunciando duas definições fundamentais para o estudo da teoria de módulos.

Definição 1.3.1. *Sejam R um anel e M um R-módulo à direita.*
(a) M é chamado de R-módulo simples *(ou* irredutível*) se $M \neq 0$, e M não possui*

outros submódulos além de (0) *e M.*
(b) M é chamado de R-módulo semi-simples *(ou* completamente redutível*) se todo R-submódulo de M é um R-módulo somando direto de M.*

Note que, de acordo com essas definições, o módulo nulo é semi-simples, mas não é simples. Uma aplicação direta da definição (b) acima nos fornece o seguinte:

Observação 1.3.2. *Qualquer submódulo (resp., módulo quociente) de um R-módulo semi-simples é semi-simples.*

Claramente, todo módulo simples é também semi-simples. Para entendermos melhor a relação entre simplicidade e semi-simplicidade, vamos provar o seguinte fato:

Lema 1.3.3. *Qualquer R-módulo à direita semi-simples não-nulo M contém um submódulo simples.*

Demonstração:

Seja m um elemento fixo não-nulo de M. Pelo que foi observado anteriormente, é suficiente tratar o caso em que $M = m.R$. Pelo Lema de Zorn, existe um submódulo maximal N de M com respeito à propriedade de que $m \notin N$. Tome um submódulo N' não-nulo tal que $M = N \oplus N'$. Finalizamos mostrando que N' é simples. De fato, se N'' é um submódulo não-nulo de N', então $N \oplus N''$ precisa conter m (pela maximalidade de N), e logo $N \oplus N'' = M$, o que implica que $N'' = N'$, como queríamos. ■

Este lema nos torna aptos a dar mais duas caracterizações de módulos semi-simples.

Teorema 1.3.4. *Para um R-módulo $M = M_R$, as seguintes propriedades são equivalentes:*

(1) *M é semi-simples.*

(2) *M é a soma direta de uma família de submódulos simples.*

(3) *M é a soma de uma família de submódulos simples.*

Convenção: A soma e a soma direta de uma família vazia de submódulos são entendidas como o módulo nulo. Esta convenção torna o argumento seguinte válido em todos os casos, incluindo o caso $M = (0)$.

Demonstração:

(1) $\Rightarrow$ (3). Seja M_1 a soma de todos submódulos simples em M, e escreva $M = M_1 \oplus M_2$, onde M_2 é um R-submódulo conveniente. Se $M_2 \neq (0)$, o lema implica que M_2 contém um R-módulo simples, mas o último precisa estar em M_1, o que gera uma contradição. Logo $M_2 = (0)$, isto é, $M_1 = M$.

(3) $\Rightarrow$ (1). Escreva $M = \sum_{i \in I} M_i$, onde M_i's são submódulos simples de M. Seja $N \subseteq M$ um submódulo dado. Para mostrar que N é um somando direto de M_R, considere subconjuntos de índices $J \subseteq I$ com as seguintes propriedades:

(a) $\sum_{j \in J} M_j$ é uma soma direta.

(b) $N \cap \sum_{j \in J} M_j = (0)$.

Pelo Lema de Zorn, podemos tomar um J maximal. Para este J, seja

$$M' := N + \sum M_j = N \oplus (\bigoplus M_j), \text{ com } j \in J.$$

Para finalizar, falta mostrar que $M' = M$ (e então N é um somando direto de M_R). Para isto, é suficiente mostrar que $M' \supseteq M_i$, para todo $i \in I$. Mas se algum $M_i \nsubseteq M'$, a simplicidade de M_i implica que $M' \cap M_i = (0)$. Disto, temos que

$$M' + M_i = N \oplus (\bigoplus M_j) \oplus M_i,$$

o que contradiz a maximalidade de J.

(3) $\Rightarrow$ (2). Segue do argumento acima aplicado a $N = (0)$.

(2) $\Rightarrow$ (3). É uma tautologia. ■

Aqui começaremos a estudar alguns resultados em anéis de matrizes, usando os conceitos de anéis simples e semi-simples.

Teorema 1.3.5. *Sejam R um anel e $M_n(R)$ o anel de matrizes $n \times n$ sobre R. Então qualquer ideal I de $M_n(R)$ tem a forma $M_n(U)$, onde U é um ideal de R unicamente determinado. Em particular, se R é um anel simples, então $M_n(R)$ também o é.*

A prova deste teorema pode ser vista no teorema 3.1 de [9].

No próximo teorema, vamos estudar em detalhes as propriedades de um anel de matrizes sobre um anel de divisão. Antes disso, porém, precisamos de uma definição.

Definição 1.3.6. *Dizemos que um anel R atua fielmente sobre um R-módulo à direita V se $Vr = 0$, com $r \in R$, implica que $r = 0$.*

Teorema 1.3.7. *Sejam D um anel de divisão e $R = M_n(D)$. Então:*
(1) *R é simples, semi-simples à direita, artiniano à direita e noetheriano à direita.*
(2) *R tem um único módulo à direita simples V (a menos de isomorfismos), R atua fielmente sobre V e $R_R \cong n.V$, como R-módulos.(onde $n.V$ denota a soma direta de n cópias do R-módulo V.)*
(3) *O anel de endomorfismos End(V_R), visto como um anel de operadores à esquerda sobre V, é isomorfo à D.*

A prova deste teorema pode ser encontrada no teorema 3.3 de [9].

Para produzir mais exemplos de anéis semi-simples, vamos fazer a seguinte observação sobre produto direto de anéis.

Proposição 1.3.8. *Sejam $R_1, ..., R_r$ anéis semi-simples à direita. Então seu produto direto $R = R_1 \times ... \times R_r$ é também um anel semi-simples à direita.*

Demonstração:

Seja $R_i = U_{i1} \oplus ... \oplus U_{im_i}$, onde cada U_{ij} é um ideal à direita minimal de R_i. Vendo R_i como um ideal em R, U_{ij} é também um ideal à direita minimal de R. Como

$$R_R = R_1 \oplus ... \oplus R_r = \bigoplus_{i,j} U_{ij},$$

concluímos que R é semi-simples à direita. ■

Segue então que, se $D_1, ..., D_r$ são anéis de divisão, então para números naturais arbitrários $n_1, ..., n_r$,

$$M_{n_1}(D_1) \times \ ... \ \times M_{n_r}(D_r)$$

é um anel semi-simples à direita.

O próximo teorema será generalizado no Capítulo 2. Antes disso, vamos enunciar um lema clássico que nos auxiliará na prova deste teorema.

Lema 1.3.9. ***(Lema de Schur).*** *Sejam R um anel e V_R um R-módulo à direita simples. Então $End(V_R)$ é um anel de divisão.*

Demonstração:

Seja $0 \neq f \in End(V_R)$. Então $\mathcal{I}m(f) \neq 0$ e $Ker(f) \neq V$. Como $\mathcal{I}m(f)$ e $Ker(f)$ são ambos submódulos de V, segue que $\mathcal{I}m(f) = V$ e $Ker(f) = 0$; isto é, f é invertível em $End(V_R)$, e portanto $End(V_R)$ é anel de divisão. ■

Teorema 1.3.10. ***(Wedderburn-Artin).*** *Seja R um anel semi-simples à direita. Então $R \cong M_{n_1}(D_1) \times \ ... \ \times M_{n_r}(D_r)$ para adequados anéis de divisão D_1, ..., D_r e inteiros positivos n_1, ..., n_r. Ainda temos que r é unicamente determinado, assim* *como os pares* (n_1, D_1)*, ...,* (n_r, D_r) *(a menos de permutação); e existem exatamente* r *módulos à direita simples sobre* R *mutuamente não-isomorfos.*

Demonstração:

Seja R um anel semi-simples à direita. Decomponha R_R como uma soma direta finita de ideais à direita minimais. Agrupando os que são isomorfos como R-módulos, podemos escrever

$$\text{(A) } R_R \cong n_1V_1 \oplus ... \oplus n_rV_r,$$

onde V_1,...,V_r são R-módulos à direita simples mutuamente não-isomorfos. Se V é qualquer R-módulo à direita simples, V é isomorfo a algum quociente de R_R e então (pelo Teorema de Jordan-Hölder) isomorfo a algum V_i. Portanto $\{V_1,...,V_r\}$ é um conjunto de R-módulos à direita simples mutuamente não-isomorfos.

Vamos determinar os anéis de R-endomorfismos dos dois módulos em (A), usando a convenção de que endomorfismos de módulos à direita são escritos à esquerda. Para R_R, os R-endomorfismos são dados pela multiplicação à esquerda por elementos de R, logo $End(R_R) \cong R$. Para determinar $End(n_1V_1 \oplus ... \oplus n_rV_r)$, seja $D_i = End(V_i)$. Pelo Lema de Schur, cada D_i é um anel de divisão, logo $End(n_iV_i) \cong M_{n_i}(D_i)$. Como não existem homomorfismos não-nulos de V_i para V_j, se $i \neq j$, temos

$$End(n_1V_1 \oplus ... \oplus n_rV_r) \cong End(n_1V_1) \times ... \times End(n_rV_r) \cong M_{n_1}(D_1) \times ... \times M_{n_r}(D_r).$$

Logo temos um isomorfismo de anéis $R \cong M_{n_1}(D_1) \times ... \times M_{n_r}(D_r)$.

Para provar a unicidade da decomposição, suponha que exista um outro isomorfismo de anéis

$$R \cong M_{n'_1}(D'_1) \times ... \times M_{n'_s}(D'_s),$$

onde $D'_1, ..., D'_s$ são anéis de divisão. Seja V'_i o único módulo à direita simples sobre $M_{n'_i}(D'_i)$. Podemos também ver V'_i como um módulo à direita simples sobre R; claramente, $V'_i \ncong V'_j$ como R-módulos se $i \neq j$. Pelo teorema 1.3.7 e proposição 1.3.8, temos

$$(A') \ {}_RR \cong n'_1V'_1 \oplus ... \oplus n'_sV'_s.$$

Pelo Teorema de Jordan-Hölder, vemos de (A) e (A') que $r = s$ e que, permutando os índices, $n_i = n'_i$ e $V_i \cong V'_i$ para todo i. Escrevendo $R_i = M_{n_i}(D'_i)$, temos pelo teorema 1.3.7 parte (3) que

$$D'_i \cong End_{R_i}(V'_i) \cong End_R(V'_i) \cong End_R(V_i) = D_i$$

para todo i. ■

Como $M_{n_1}(D_1) \times ... \times M_{n_r}(D_r)$ é semi-simples tanto à direita como à esquerda, temos a seguinte conseqüência interessante deste teorema:

Corolário 1.3.11. *Um anel R semi-simples à direita é sempre semi-simples à esquerda (e reciprocamente).*

1.4 O radical de Jacobson

Definição 1.4.1. *Chamamos de* radical de Jacobson *de um anel R, e denotamos por $J(R)$, a intersecção de todos os ideais maximais à direita de R.*

Lema 1.4.2. *Para $y \in R$, as seguintes afirmações são equivalentes:*
(i) $y \in J(R)$.
(ii) 1 - yx é invertível à direita para qualquer $x \in R$.
(iii) $My = 0$ para qualquer R-módulo à direita simples M.

Demonstração: $(i) \Rightarrow (ii)$ Seja $y \in J(R)$. Por absurdo, suponhamos que existe $x \in R$ tal que $1 - yx$ não é invertível à direita. Assim, o ideal à direita gerado por $1 - yx$ não é o próprio anel R e conseqüentemente existe um ideal à direita maximal P tal que $(1 - yx)R \subseteq P$. Como $y \in J(R) \subseteq P$, segue que $y \in P$. Portanto, devemos ter $1 \in P$, o que é uma contradição.

$(ii) \Rightarrow (iii)$ Suponhamos que exista $m \in M$ tal que $my \neq 0$. Então $myR = M$, pois M é simples. Em particular, existe $x \in R$ tal que $m = myx$, ou seja, $m(1 - yx) = 0$, o que produz $m = 0$ de nossa hipótese. Esta contradição prova a implicação desejada.

$(iii) \Rightarrow (i)$ Seja P um ideal à direita maximal de R. Então $M = R/P$ é um R-módulo à direita simples. Portanto, $0 = My = (R/P)y$, ou seja, $ry \in P$, para todo $r \in R$. Tomando $r = 1$, obtemos $y \in P$. Portanto $y \in \cap\{P : P$ é um ideal à direita maximal de $R\} = J(R)$, como queríamos mostrar. ■

Definição 1.4.3. *Para qualquer R-módulo à direita M, o* anulador *de M é definido por*

$$ann(M) := \{r \in R; Mr = 0\}.$$

É fácil ver que $ann(M)$ é um ideal (bilateral) de R. Como conseqüência direta do Lema 1.4.2, item (3), e da definição anterior, temos:

Corolário 1.4.4. *$J(R) = \bigcap ann(M)$, onde M percorre todos os R-módulos à direita simples. Em particular, $J(R)$ é um ideal de R.*

1.5 Anéis Primos e Semiprimos

Vamos iniciar esta seção recordando dois conceitos da teoria de anéis comutativos: as noções de ideal primo e radical primo.

Sejam R um anel comutativo e U um ideal em R. Dizemos que U é um *ideal primo* se $U \neq R$ e, para $a, b \in R$, $ab \in U$ implica que $a \in U$ ou $b \in U$.

Dizemos que U é um *ideal radical* se, para $a \in R$, $a^n \in U$, para algum $n \geq 1$, implica que $a \in U$.

Na álgebra comutativa, sabemos que U é um ideal radical se, e somente se U, é uma intersecção de ideais primos. E que, para qualquer ideal U, existe um ideal radical minimal contendo U, que é a intersecção de todos ideais primos contendo U. Este radical é denotado por $\sqrt{U}$, que também pode ser caracterizado por

$$\sqrt{U} = \{x \in R : x^n \in U \text{ para algum } n \geq 1\}.$$

Como um caso especial, nós temos $\sqrt{(0)} = Nil(R)$, o ideal de elementos nilpotentes de R.

Nosso objetivo agora é generalizar esses conceitos para o caso não-comutativo.

Definição 1.5.1. *Um ideal P em um anel R é dito um ideal primo se $P \neq R$ e, para ideais $U, B \subseteq R$,*

$$U.B \subseteq P \textit{ implica que } U \subseteq P \textit{ ou } B \subseteq P.$$

Para um elemento $a \in R$, vamos escrever $(a) = RaR$: este é o ideal gerado por a em R. A seguinte proposição nos fornece outras caracterizações de ideais primos.

Proposição 1.5.2. *Para um ideal $P \subsetneqq R$, as seguintes afirmações são equivalentes:*
(1) *P é primo.*
(2) *Para $a, b \in R$, $(a)(b) \subseteq P$ implica que $a \in P$ ou $b \in P$.*
(3) *Para $a, b \in R$, $aRb \subseteq P$ implica que $a \in P$ ou $b \in P$.*
(4) *Para ideais à direita U, B em R, $UB \subseteq P$ implica que $U \subseteq P$ ou $B \subseteq P$.*
(4′) *Para ideais à esquerda U, B em R, $UB \subseteq P$ implica que $U \subseteq P$ ou $B \subseteq P$.*

(5) *Se U e B são ideais de R tais que $U \supseteq P$, $B \supseteq P$ e $UB \subseteq P$, então $U = P$ ou $B = P$.*

Demonstração:

(1) $\Rightarrow$ (5): Seja U e B ideais de R tais que $U \supseteq P$, $B \supseteq P$ e $UB \subseteq P$. Como P é primo, segue que $U \subseteq P$ ou $B \subseteq P$. Logo $U = P$ ou $B = P$.

(5) $\Rightarrow$ (1): Sejam U, B ideais de R tais que $UB \subseteq P$. Tomando $U + P$, $B + P$ temos $(U + P)(B + P) = UB + PB + UP + P \subseteq P$, de onde concluímos que $U + P = P$ ou $B + P = P$. Logo $U \subseteq P$ ou $B \subseteq P$.

Agora resta-nos mostrar que (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1). As duas primeiras implicações são diretas, assim como a última. Portanto vamos nos deter na prova de (3) $\Rightarrow$ (4). Para isto, assuma que $UB \subseteq P$, mas $U \nsubseteq P$, onde U, B são ideais à direita. Fixe um elemento $a \in U \setminus P$. Para qualquer $b \in B$, temos que $aRb \subseteq UB \subseteq P$, logo por (3), $b \in P$, e isto mostra que $B \subseteq P$. ■

Sabemos da álgebra comutativa que o complementar de um ideal primo é um sistema multiplicativamente fechado. Vamos agora fazer uma definição que generaliza este fato para anéis quaisquer.

Definição 1.5.3. *Um conjunto não-vazio $S \subseteq R$ é chamado um m-sistema se, para quaisquer $a, b \in S$, existe $r \in R$ tal que $arb \in S$.*

Da Proposição 1.5.2 e da Definição 1.5.3, concluímos o seguinte:

Corolário 1.5.4. *Um ideal $P \subseteq R$ é primo se, e somente se, $R \backslash P$ é um m-sistema.*

Proposição 1.5.5. *Seja $S \subseteq R$ um m-sistema, e seja P um ideal maximal com respeito à propriedade de P ser disjunto de S. Então P é um ideal primo.*

Demonstração:

Suponha que a, b não pertençam à P, mas $(a)(b) \subseteq P$. Pela propriedade maximal de P, existem $s, s' \in S$ tal que $s \in P + (a), s' \in P + (b)$. Tome $r \in R$ com $srs' \in S$. Então

$$srs' \in (P + (a))R(P + (b)) \subseteq P + (a)(b) \subseteq P,$$

uma contradição. Logo P tem que ser um ideal primo. ■

Agora vamos generalizar a noção de $\sqrt{U}$.

Definição 1.5.6. *Para qualquer ideal U em um anel R, seja*
$\sqrt{U} := \{s \in R$*: todo m-sistema contendo s intercepta* $U\}$
$\subseteq \{s \in R : s^n \in U$, *para algum* $n \geq 1\}$.

Observação 1.5.7. *No caso comutativo, podemos checar que a inclusão "* $\subseteq$ *" é de fato uma igualdade.*

Teorema 1.5.8. *Para qualquer anel R e qualquer ideal $U \subseteq R$, $\sqrt{U}$ é igual à intersecção de todos os ideais primos contendo U. Em particular, $\sqrt{U}$ é um ideal em R.*

Demonstração:

Primeiro vamos mostrar a inclusão " $\subseteq$ ". Seja $s \in \sqrt{U}$ e P qualquer ideal primo $\supseteq U$. Considere o m-sistema $R \setminus P$. Este m-sistema não pode conter s, pois caso contrário ele interceptaria U e conseqüentemente, P. Logo $s \in P$.

Reciprocamente, suponhamos que s não pertence à $\sqrt{U}$. Então, pela definição, existe um m-sistema S contendo s o qual é disjunto de U. Pelo Lema de Zorn, existe um ideal $P \supseteq U$ que é maximal com respeito a ser disjunto de S. Pela Proposição 1.5.5, P é um ideal primo e nós temos $s \notin P$, como queríamos.

■

Vamos agora definir a noção de ideal semiprimo.

Definição 1.5.9. *Um ideal C em um anel R é dito um* ideal semiprimo *se, para qualquer ideal U de R, $U^2 \subseteq C$ implica que $U \subseteq C$. (Observe que um ideal primo é sempre semiprimo).*

Proposição 1.5.10. *Para qualquer ideal C, as seguintes afirmações são equivalentes:*

(1) *C é semiprimo.*

(2) *Para $a \in R$, $(a)^2 \subseteq C$ implica que $a \in C$.*

(3) *Para $a \in R$, $aRa \subseteq C$ implica que $a \in C$.*

(4) *Para qualquer ideal à direita U em R, $U^2 \subseteq C$ implica que $U \subseteq C$.*

($4'$) *Para qualquer ideal à esquerda U em R, $U^2 \subseteq C$ implica que $U \subseteq C$.*

A prova é similar à da Proposição 1.5.2, por isso vamos omiti-la.

Semelhante à Definição 1.5.3, dizemos que um conjunto $S \subseteq R$ é um *n-sistema* se, para qualquer $a \in S$, existe um $r \in R$ tal que $ara \in S$. Logo, segue da proposição acima que um ideal $C \subseteq R$ é semiprimo se, e somente se, $R \setminus C$ é um n-sistema.

Vamos enunciar um lema que relaciona m-sistemas com n-sistemas.

Lema 1.5.11. *Sejam N um n-sistema em um anel R e $a \in N$. Então existe um m-sistema $M \subseteq N$ tal que $a \in M$.*

Demonstração:

Vamos definir M indutivamente como a seguir: $a_1 = a$, $a_2 = a_1 r_1 a_1 \in N$ (para algum r_1), $a_3 = a_2 r_2 a_2 \in N$ (para algum r_2), ..., etc. Para mostrar que M é um m-sistema, precisamos mostrar que, para quaisquer i, j, $a_i R a_j$ contém um elemento de M. Mas se $i \leq j$, $a_i R a_j$ contém $a_i R a_i$, que contém $a_{i+1} \in M$.

■

Teorema 1.5.12. *Para qualquer ideal $C \subseteq R$, as seguintes afirmações são equivalentes:*

(1) *C é um ideal semiprimo.*

(2) *C é uma intersecção de ideais primos.*

(3) *$C = \sqrt{C}$.*

Demonstração:

(3) $\Rightarrow$ (2) é claro, pois pelo Teorema 1.5.8, $\sqrt{C}$ é uma intersecção de ideais primos.

(2) $\Rightarrow$ (1). Pela Definição 1.5.9, fica claro que a intersecção de qualquer família de ideais semiprimos (ou primos) é um ideal semiprimo.

(1) $\Rightarrow$ (3). Para um ideal semiprimo C, precisamos mostrar que $\sqrt{C} \subseteq C$, já que $C \subseteq \sqrt{C}$ sempre acontece. Seja $a \notin C$. Então $N := R \setminus C$ é um n-sistema contendo a. Pelo Lema 1.5.11, existe um m-sistema $M \subseteq N$ tal que $a \in M$. Mas então M é disjunto de C, logo, pela Definição 1.5.6, $a \notin \sqrt{C}$. ■

Como conseqüência deste teorema, temos:

Corolário 1.5.13. *Para qualquer ideal $C \subseteq R$, $\sqrt{C}$ é o menor ideal semiprimo em R que contém C.*

No caso especial em que $C = 0$, a relação de inclusão vista na definição 1.5.6 mostra que $\sqrt{(0)}$ é sempre um nil ideal. Isto nos leva a uma nova noção de radical:

Definição 1.5.14. *Para qualquer anel R, definimos $Nil_*R := \sqrt{(0)}$. Este é chamado* nilradical inferior. *Ele é o menor ideal semiprimo em R, e é igual a intersecção de todos os ideais primos em R. Por causa disso, Nil_*R é também chamado de* radical primo *de R. Como Nil_*R é nil, temos que*

$$Nil_*R \subseteq J(R).$$

Definição 1.5.15. *Um anel R é dito um* anel primo *(resp.* semiprimo*) se o ideal nulo é um ideal primo (resp. semiprimo).*

Para facilitar a notação, a partir de agora escreveremos o ideal gerado por zero somente como "0".

Proposição 1.5.16. *Para qualquer anel R, as seguintes afirmações são equivalentes:*

(1) *R é um anel semiprimo.*

(2) $Nil_*R = 0$.

(3) *R não possui ideais nilpotentes não-nulos.*

(4) *R não possui ideais à esquerda nilpotentes não-nulos.*

Demonstração:

(1) $\Rightarrow$ (2). Como 0 é ideal semiprimo (da definição 1.5.15), e não existe ideal semiprimo menor que 0, segue da definição 1.5.14 que $Nil_*R = 0$.

(2) $\Rightarrow$ (1). Como $0 = Nil_*R$ é semiprimo, segue que R é anel semiprimo.

Vamos mostrar agora que (4) $\Rightarrow$ (3) $\Rightarrow$ (1) $\Rightarrow$ (4).

As duas primeiras implicações são diretas. Para (1) $\Rightarrow$ (4), seja R um anel semiprimo e seja U um ideal à esquerda nilpotente. Escolha n (≥ 1) minimal tal que $U^n = 0$. Se $n > 1$, então $(U^{n-1})^2 = U^{2n-2} \subseteq U^n = 0$, o que implica que $U^{n-1} = 0$ (pela Proposição 1.5.10), contradizendo a minimalidade de n. Logo $n = 1$ e $U = 0$. ■

Enunciaremos agora dois resultados utilizando os conceitos de anéis primos e semiprimos para anéis de matrizes.

Proposição 1.5.17. *Um anel R é primo (resp. semi-primo) se, e somente se, $M_n(R)$ é primo (resp. semi-primo).*

Demonstração:

Para a prova, vamos considerar apenas o caso primo. Assuma $M_n(R) \neq 0$ não primo. Então existem ideais não-nulos U, B em $M_n(R)$ tais que $U.B = 0$. Pelo Teorema 1.3.5, nós temos que $U = M_n(A)$ e $B = M_n(H)$, onde A, H são ideais (não-nulos) em R. Mas então $U.B = 0$ implica que $A.H = 0$, logo R não pode ser primo.

Reciprocamente, suponha que $R \neq 0$ não seja primo. Então existem ideais não-nulos A, H em R tais que $A.H = 0$. Mas então $M_n(A).M_n(H) = 0$, logo $M_n(R)$ não pode ser primo. ■

Vamos então relacionar anéis semi-simples com anéis semiprimos. Começaremos com um lema básico sobre ideais à direita minimais em um anel qualquer.

Lema 1.5.18. ***Lema de Brauer.*** *Seja U um ideal à direita minimal em um anel R. Então temos que $U^2 = 0$ ou $U = eR$ para algum idempotente $e \in U$.*

Demonstração:

Assuma $U^2 \neq 0$. Então $a.U \neq 0$ para algum $0 \neq a \in U$, e portanto $U.a = U$. Escolha $e \in U$ tal que $a = ea$. O conjunto

$$I = \{x \in U : xa = 0\}$$

é um ideal à direita contido propriamente em U, já que $e \notin I$. Portanto, $I = 0$.

Por outro lado, temos que $e^2 - e \in U$ e $(e^2 - e)a = 0$; então $e^2 - e = 0$, ou seja, $e^2 = e$. Como U_R é minimal, concluímos que $U = eR$. ■

O seguinte resultado fica claro.

Corolário 1.5.19. *Se U é um ideal à direita minimal em um anel semiprimo R, então $U = eR$ para algum idempotente $e \in U$.*

Temos então o seguinte resultado, cuja demonstração pode ser vista no teorema 10.24 de [9].

Teorema 1.5.20. *Para qualquer anel R, as seguintes afirmações são equivalentes:*
(1) *R é semi-simples.*
(2) *R é semiprimo e artiniano à direita.*
(3) *R é semiprimo e satisfaz DCC em ideais à direita principais.*

1.6 Injetividade

Nesta seção listaremos alguns resultados básicos sobre injetividade que serão utilizados no Capítulo 3. O que se discute aqui pode ser encontrado em [4]e [10].

Seja R um anel.

Definição 1.6.1. *Dizemos que um módulo M_R é injetivo se, para cada par de módulos A_R, B_R tal que existe h: $A \to B$ um monomorfismo, temos a propriedade que cada $f \in Hom(A_R, M_R)$ pode ser estendido a um elemento de $Hom(B_R, M_R)$.*

Podemos mostrar que M é injetivo se, e somente se, é um somando direto de todo módulo ao qual ele é submódulo.

Definição 1.6.2. *Seja B_R um submódulo não-nulo de M_R. Dizemos que B é um submódulo essencial de M se, para cada submódulo não-nulo C de M, $C \cap B \neq 0$.*

Recordando que uma extensão M de N através do monomorfismo f é dita essencial se $f(N)$ é um submódulo essencial de M, e é dita injetiva se N é injetivo, podemos mostrar a extensão essencial maximal de M coincide com a extensão injetiva minimal de M. Veremos este resultado com mais detalhes no decorrer desta seção.

Observação 1.6.3. *(1) $M \subseteq_e E$ se, e somente se, para qualquer elemento não-nulo $a \in E$, existe $r \in R$ tal que $0 \neq ar \in M$.*

(2) (Transitividade) Se $M \subseteq_e E$ e $E \subseteq_e E'$, então $M \subseteq_e E'$.

A noção de extensão essencial nos fornece uma nova interpretação de injetividade, como segue.

Lema 1.6.4. *Um módulo M é injetivo se, e somente se, não possui extensões essenciais próprias.*

Demonstração:

Primeiro assuma que M é injetivo, e considere qualquer extensão própria $E \supsetneq M$. Logo temos que $E = M \oplus N$, para algum submódulo $N \neq 0$. Aqui, $N \cap M = 0$, logo $E \supseteq M$ não é uma extensão essencial.

Reciprocamente, assuma que M não possui extensões essenciais próprias, e tome M imerso em um módulo injetivo I_R. Pelo Lema de Zorn, existe um submódulo $S \subseteq I$ maximal com respeito à propriedade de que $S \cap M = 0$. Então, no quociente I/S, qualquer submódulo não-nulo S'/S intercepta a imagem de M não trivialmente, logo $\Im m(M) \subseteq_e I/S$. Pela hipótese, precisamos ter $\Im m(M) = I/S$. Isto significa que $I = M \oplus S$, logo M é um módulo injetivo. ∎

Lema 1.6.5. *Qualquer módulo M_R possui uma extensão essencial maximal.*

Demonstração:

Fixe um módulo injetivo $I \supseteq M$, e considere qualquer família de extensões essenciais de M em I que são linearmente ordenadas por inclusão. Pelo Observação 1.6.3, parte (1), é claro que a união desta família é também essencial sobre M. Pelo Lema de Zorn, segue que podemos encontrar um submódulo E maximal com respeito à propriedade que $M \subseteq_e E \subseteq I$. Queremos mostrar que E é uma extensão essencial maximal de M. De fato, se isto não fosse verdade, poderíamos achar

$E \subsetneq E'$ tal que $M \subseteq_e E'$. (Note que E' é apenas algum R-módulo, e pode não estar em I.) Pela injetividade de I, a aplicação de inclusão $E \subseteq I$ pode ser estendida a alguma $g : E' \to I$. Claramente, $(Ker\ g) \cap M = 0$, logo $M \subseteq_e E'$ implica que $Ker g = 0$. Portanto podemos identificar E' com $g(E')$. Mas então $M \subseteq_e E'$ contradiz a escolha maximal de E. ■

Teorema 1.6.6. *Para módulos $M \subseteq I$, as seguintes afirmações são equivalentes:*
(1) I é extensão essencial maximal sobre M.
(2) I é módulo injetivo, e essencial sobre M.
(3) I é extensão injetiva minimal sobre M.

Demonstração:

(1) $\Rightarrow$ (2). Pela transitividade (Observação 1.6.3, (2)), (1) implica que I não possui extensão essencial própria. Logo, pelo Lema 1.6.4, I é injetivo.

(2) $\Rightarrow$ (3). Seja I' um módulo injetivo tal que $M \subseteq I' \subseteq I$. Logo $I = I' \oplus N$, para algum submódulo $N \subseteq I$. Como $N \cap M = 0$, precisamos ter $N = 0$ (já que $M \subseteq_e I$), logo $I' = I$.

(3) $\Rightarrow$ (1). Assuma que I é extensão injetiva minimal sobre M. A prova do Lema 1.6.5 produz um submódulo $E \subseteq I$ que é essencial maximal sobre M. Usando (1) $\Rightarrow$ (2), sabemos que E é injetiva, e portanto $E = I$, o que prova (1). ■

Definição 1.6.7. *Chamamos de fecho injetivo $\widehat{M_R}$ de M_R ao menor módulo injetivo tal que $M_R \subseteq \widehat{M_R}$, ou seja, é uma extensão essencial maximal de M_R.*

Mostramos assim que o fecho injetivo existe, e é único, a menos de isomorfismos.

Definição 1.6.8. *Considere M_R um módulo. Chamamos de* endomorfismo parcial *a todo homomorfismo de N em M_R, onde N é um submódulo de M.*

Definição 1.6.9. *Dizemos que um módulo M_R é quase-injetivo se todo endomorfismo parcial pode ser estendido a um endomorfismo.*

Salientamos que todo módulo está contido em um módulo quase-injetivo, logo temos a seguinte definição.

Definição 1.6.10. *Chamamos de* fecho quase-injetivo $\overline{M}_R$ *de* M_R *ao menor módulo quase-injetivo tal que* $M_R \subseteq \overline{M}_R$.

Podemos mostrar que o fecho quase-injetivo também é único, a menos de isomorfismos.

O próximo resultado estabelece uma relação entre fecho injetivo e módulo quase-injetivo.

Proposição 1.6.11. *Seja* M_R *um módulo qualquer. Se* $\Lambda = End(\widehat{M})$*, então:*
(1) $\Lambda\widehat{M}$ *é a intersecção de todos submódulos quase-injetivos de* $\widehat{M}$ *contendo M;*
(2) $\Lambda\widehat{M}$ *é quase-injetivo;*
(3) M *é quase-injetivo se, e somente se,* $M = \Lambda\widehat{M}$.

Demonstração:

(2) Se $f : N \to \Lambda\widehat{M}$ é uma aplicação de um submódulo N de $\Lambda\widehat{M}$ em $\Lambda\widehat{M}$, então f é induzida por algum $\lambda \in \Lambda$. Como $\lambda(\Lambda\widehat{M}) \subseteq \Lambda\widehat{M}$, λ induz $\overline{\lambda} \in End(\Lambda\widehat{M})$, e $\overline{\lambda}$ por sua vez induz f, mostrando que $\Lambda\widehat{M}$ é quase-injetivo.

(1) Seja P um submódulo quase-injetivo de $\widehat{M}$ contendo M. Queremos mostrar que $P \supseteq \Lambda\widehat{M}$, logo é suficiente mostrar que $\alpha P \subseteq P$, $\forall\ \alpha \in \Lambda$. Para isto, note que $Q(\alpha) = \{x \in P; \alpha x \in P\}$ é um submódulo de P, e temos apenas que mostrar que $Q(\alpha) = P\ \forall\ \alpha \in \Lambda$. Como $q \to \alpha q$, $q \in Q = Q(\alpha)$, é uma aplicação de Q em P, e P é quase-injetivo, existe $\alpha_1 \in End(P)$ tal que $\alpha_1 q = \alpha q \forall\ q \in Q$. Como $\widehat{M}$ é injetivo, existe $\alpha' \in \Lambda$ tal que $\alpha' x = \alpha_1 x\ \forall\ x \in P$. Como $\alpha' P \subseteq P$, se $(\alpha' - \alpha)P = 0$, temos $\alpha P \subseteq P$. Assim se $Q(\alpha) \neq P$, então $(\alpha' - \alpha)P \neq 0$. Se $M' \supseteq M$, necessariamente $\widehat{M'} \supseteq P$, e conseqüentemente $(\alpha' - \alpha)P \cap P \neq 0$. Mas se $x, 0 \neq y \in P$ são tais que $y = (\alpha' - \alpha)x \in (\alpha' - \alpha)P \cap P$, então já que $\alpha' x = \alpha_1 x \in P$, temos que

$\alpha x = \alpha_1 x - y \in P$. Mas então $x \in Q(\alpha)$, logo $\alpha x = \alpha_1 x$,e portanto $y = 0$, uma contradição.

(3) É uma conseqüência imediata de (1) e (2). ■

Capítulo 2

Anéis Primitivos

Neste capítulo ainda estaremos seguindo [9], parágrafos §10 e §11.

Antes de iniciarmos a próxima seção, precisamos da definição de anel semiprimitivo. Dizemos, então, que um anel é *J-semi-simples*, ou *semiprimitivo*, se $J(R) = 0$.

2.1 Estrutura de Anéis Primitivos

Proposição 2.1.1. *Um anel R é semiprimitivo se, e somente se, R possui um módulo à direita semi-simples e fiel M.*

Demonstração:

Assuma R semiprimitivo, ou seja, $J(R) = 0$. Seja $\{M_i\}$ um conjunto de R-módulos à direita simples mutuamente não-isomorfos. Então $M = \bigoplus M_i$ é semi-simples, e

$$ann(M) = \bigcap ann(M_i) = J(R)$$

pelo Lema 1.4.2. Como $J(R) = 0$, M é um R-módulo fiel.

Reciprocamente, suponha que exista tal M. Como $J(R)$ atua como zero em todos R-módulos à direita simples (pelo Lema 1.4.2), nós temos $(J(R)).M = 0$. Então a fidelidade de M implica que $J(R) = 0$, logo R é semiprimitivo.

■

Definição 2.1.2. *Um anel R é dito* primitivo à direita *(resp.,* esquerda*) se R possui um módulo à direita (resp., esquerda) simples e fiel.*

Enquanto a noção de semiprimitividade é simétrica (direita-esquerda), a noção de primitividade não é. Bergman, no seu artigo "A ring primitive on the right but not on the left", e Jategaonkar, em "A counterexample in ring theory and homological algebra", construíram exemplos de anéis primitivos a um lado e não ao outro. Maiores informações podem ser encontradas em [2] e [8].

Antes de estudarmos anéis primitivos à direita com mais detalhes, é importante estendermos a noção de primitividade à direita de anéis para ideais.

Definição 2.1.3. *Um ideal $U \subseteq R$ é dito* primitivo à direita *(resp.,* esquerda*) se o anel quociente R/U é primitivo à direita (resp., esquerda).*

Proposição 2.1.4. *Um ideal U em R é primitivo à direita se, e somente se, U é o anulador de um R-módulo à direita simples.*

Demonstração:

Primeiro, suponha que R/U é um anel primitivo à direita, e seja M um R/U-módulo à direita simples e fiel. Então, visto como um R-módulo, M_R permanece simples, e o seu anulador em R é U.

Reciprocamente, suponha $U = ann(M)$, onde M é um R-módulo à direita simples. Então M pode ser visto como um R/U-módulo simples, e como tal, é fiel. Logo R/U é um anel primitivo à direita. ■

Do Corolário 1.4.4 e da Proposição 2.1.4, concluímos que:

Corolário 2.1.5. *O radical de Jacobson $J(R)$ é a intersecção de todos ideais primitivos à direita (resp. esquerda) em R.*

Vamos então tentar relacionar anéis primitivos à direita com as outras classes de anéis que vimos anteriormente.

Proposição 2.1.6. *Um anel simples é primitivo à direita (e esquerda). Um anel primitivo à direita é semiprimitivo e primo.*

Demonstração:

A primeira afirmação é direta, já que se R é simples, R precisa atuar fielmente em *qualquer* R-módulo não-nulo. O fato de que um anel primitivo à direita é semiprimitivo vem da Proposição 2.1.1 e da Definição 2.1.2, já que um módulo simples é, em particular, semi-simples. Vamos então mostrar que um anel primitivo à direita é primo.

Seja R um anel primitivo à direita, e seja M um R-módulo à direita simples e fiel. Considere qualquer ideal não-nulo U em R. Claramente, $M.U$ é um R-submódulo de M, e a fidelidade de M_R implica que $M.U \neq 0$. Logo $M.U = M$. Se B é outro ideal não-nulo em R, temos que

$$M(UB) = (MU)B = M.B = M,$$

e portanto $UB \neq 0$, e isto prova que R é primo. ■

Lema 2.1.7. *Sejam R um anel semiprimo e $a \in R$. Se aR é um ideal à direita minimal, então Ra é um ideal à esquerda minimal.*

Demonstração:

É suficiente mostrar que, para qualquer elemento não-nulo $ra \in Ra$, temos que

$a \in Rra$. Como R é semiprimo, $rasra \neq 0$ para algum $s \in R$. Seja $\varphi : aR \to aR$ o R-homomorfismo definido por

$$\varphi(x) = asrx, \text{ para qualquer } x \in aR.$$

Como $\varphi(a) = asra \neq 0$ e aR é simples, φ é um isomorfismo. Seja ψ o inverso de φ. Então

$$a = (a)\varphi\psi = (asra)\psi = (as)\psi ra \in Rra.$$

■

O próximo resultado mostra que, para anéis contendo ideais à direita minimais, a primitividade é simétrica.

Teorema 2.1.8. *Seja R um anel com um ideal à direita minimal U. As seguintes propriedades são equivalentes:*
(1) *R é primo.*
(2) *R é primitivo à direita.*
(3) *R é primitivo à esquerda.*
Se estas propriedades valem, então R tem também um ideal à esquerda minimal B. Qualquer R-módulo à direita (resp., esquerda) simples e fiel é isomorfo à U_R *(resp.,* ${}_RB$*).*

Demonstração:

(2) $\Rightarrow$ (1) segue da Proposição 2.1.6.

(1) $\Rightarrow$ (2) Assuma (1). Queremos que U seja um R-módulo à direita fiel. De fato, se $r \in R$ é tal que $Ur = 0$, então $U(rR) = 0$, logo pela Proposição 1.5.2, $rR = 0$, isto é, $r = 0$. Como U_R é também um módulo simples, (2) segue.

De maneira análoga podemos mostrar que (1) $\Leftrightarrow$ (3).

Agora considere qualquer R-módulo à direita simples fiel M. Então $m.U \neq 0$, para algum $m \in M$. Pela irredutibilidade de M, temos que $M = m.U$. A aplicação

$$U \to m.U = M$$

mandando $a \in U$ em $ma \in M$ é claramente um isomorfismo de R-módulos de U em M. Pelo lema anterior, R também tem um ideal minimal à esquerda, logo as demais conclusões seguem da simetria direita-esquerda. ∎

Finalizamos esta seção apresentando alguns exemplos de anéis primitivos.

Proposição 2.1.9. *Um anel comutativo R é primitivo (à direita) se, e somente se, é um corpo.*

Demonstração:

Se R é corpo, então, visto como um R-módulo sobre si mesmo, ele é simples e fiel, e portanto R é primitivo.

Reciprocamente, seja R primitivo e seja M um R-módulo simples e fiel. Então $M \cong R/m$, para algum ideal maximal m em R. Como $m.M = 0$, segue que $m = 0$. Assim, R não tem ideais próprios, donde R é corpo. ∎

Em princípio, anéis primitivos estão em toda parte. De fato, se R um anel qualquer não-nulo, e M um R-módulo à direita simples, então $R/ann(M)$ é um anel primitivo à direita. Para fornecer um exemplo mais explícito, vamos proceder da seguinte maneira: Seja k um anel de divisão, ${}_kV$ um k-espaço vetorial à esquerda, e $E = End({}_kV)$, operando pela direita de V. Claramente, V é um E-módulo simples e fiel, logo E é um anel primtivo à direita. Se $dim_k(V) = n < \infty$, então $E \cong M_n(k)$ é um anel artiniano simples. Mas se $dim_k(V)$ é infinita, então V nos dá um exemplo de anel primitivo à direita não-simples, não-comutativo e não-artiniano. A classe de anéis primitivos à direita construída acima é importante porque, como veremos mais adiante, um anel R primitivo à direita "se parece"com $E = End({}_kV)$.

2.2 O Teorema da Densidade de Jacobson e Chevalley

Nosso próximo passo é provar o Teorema da Densidade de Jacobson e Chevalley. Para isto, vamos definir a noção de densidade.

Sejam R, k dois anéis, e $M = {}_kV_R$ um (R,k)-bimódulo. Escrevemos $E = End({}_kV)$, que opera sobre V pela direita. Dizemos que R *atua densamente* sobre ${}_kV$ se, para qualquer $f \in E$ e quaisquer $v_1, ..., v_n \in V$, existe $r \in R$ tal que $v_i r = (v_i)f$, para $i = 1, 2, ..., n$.

Para explicar porque esta propriedade é referida como "densidade", vamos fazer a seguinte observação:

Seja T a topologia sobre E definida tomando como base todos os conjuntos da forma

$$\{g \in E : (v_i)g = v_i' \ (1 \leq i \leq n)\},$$

onde n é um número natural, e v_i, v_i' são elementos arbitrários de V. É fácil ver que R atua densamente sobre ${}_kV$ (no sentido definido acima) se, e somente se, olhando a aplicação natural de R para E, a imagem de R é um subanel denso de R com respeito à topologia T.

Antes de enunciarmos o Teorema da Densidade, precisamos de uma definição e um resultado preliminar.

Definição 2.2.1. *Dizemos que um módulo M é totalmente invariante quando $f(M) \subseteq M$, para todo $f \in End(\widehat{M})$.*

Lema 2.2.2. *Na notação acima, assuma que M_R é um R-módulo semi-simples, e que $k = End(M_R)$. Então qualquer R-submódulo W de V é um E-submódulo (claramente, a recíproca também vale).*

Demonstração:

Tome um R-submódulo W' de V tal que $V = W \oplus W'$, e seja $e \in k$ a projeção de V em W com respeito a essa decomposição. Então, para qualquer $f \in E$, temos

$$(W)f = (eW)f = e(Wf) \subseteq W,$$

logo W é um E-submódulo de V. ■

Vamos enunciar agora o resultado principal deste capítulo:

Teorema 2.2.3. ***Teorema da Densidade (Jacobson, Chevalley).*** *Sejam R um anel e V um R-módulo à direita semi-simples. Então, para $k = End(V_R)$, R atua densamente sobre ${}_kV$.*

Demonstração:

Seja $E = End({}_kV)$. Para $f \in E$ e $v_1, ..., v_n \in V$, procuramos um elemento $r \in R$ tal que $v_i r = (v_i)f, i = 1, 2, ..., n$. A idéia da prova é aplicar o lema anterior para o R-módulo semi-simples $\widetilde{V} = V^n$ (soma direta de n cópias de V). Primeiro, note que

$$\begin{aligned} \widetilde{k} &:= End(\widetilde{V}_R) = End(V_R^n) \\ &\cong M_n(End(V_R)) = M_n(k). \end{aligned}$$

Agora defina $\widetilde{f} : \widetilde{V} \longrightarrow \widetilde{V}$ tomando $\widetilde{f} = (f, f, ..., f)$. Queremos que $\widetilde{f} \in End({}_{\widetilde{k}}\widetilde{V})$ (para poder aplicar o lema).

Para ver isto, seja $\widetilde{e} \in \widetilde{k}$, e represente $\widetilde{e}$ como a matriz (e_{ij}), onde $e_{ij} \in k$, já que $\widetilde{k} \cong M_n(k)$. Então, para qualquer $(w_1, ..., w_n) \in \widetilde{V}$, onde consideraremos $(w_1, ..., w_n)$ como uma matriz coluna, temos:

$$(\widetilde{e}(w_1, ..., w_n))\widetilde{f} = (\sum e_{1j}w_j, ..., \sum e_{nj}w_j)\widetilde{f}$$

$$= ((\sum e_{1j}w_j)f, ..., (\sum e_{nj}w_j)f)$$

$$= (\sum e_{1j}(w_j)f, ..., \sum e_{nj}(w_i)f)$$

$$= \widetilde{e}((w_1)f, ..., (w_n)f)$$

$$= \widetilde{e}((w_1, ..., w_n)\widetilde{f}),$$

como queríamos.

Agora considere o R-submódulo cíclico $\widetilde{W}$ de $\widetilde{V}$ gerado por $(v_1, ..., v_n) \in \widetilde{V}$. Pelo lema anterior (aplicado em $\widetilde{W} \subseteq \widetilde{V}$), $\widetilde{W}$ é totalmente invariante, ou seja, $(\widetilde{W}\widetilde{f}) \subseteq \widetilde{W}$. Logo,

$$(v_1, ..., v_n)\widetilde{f} = ((v_1)f, .., (v_n)f) \in \widetilde{W} = (v_1, ..., v_n).R,$$

já que $\widetilde{W}$ é $\widetilde{E}$-submódulo.

Portanto existe $r \in R$ tal que $(v_i)f = v_i r$ para $i = 1, 2, ..., n$. ■

Corolário 2.2.4. *Sejam R, V, k e E como no Teorema da Densidade. Se ${}_kV$ é finitamente gerado como um k-módulo (à esquerda), então a aplicação natural $\rho : R \to E$ é sobrejetiva.*

Demonstração:

Seja $v_1, ..., v_n \in V$ um conjunto finito de geradores de V como um k-módulo à esquerda. Seja $f \in E$. Pelo Teorema da Densidade, existe um $r \in R$ tal que $v_i r = (v_i)f$ para todo i. Para qualquer $v \in V$, escreva $v = \sum a_i v_i$ onde $a_i \in k$. Então

$$vr = \sum(a_i v_i)r = \sum a_i(v_i r) = \sum a_i((v_i)f) = (\sum a_i v_i)f = (v)f,$$

logo $f = \rho(r)$. ■

Um caso de grande interesse no Teorema da Densidade é quando V é um R-módulo *simples.* Neste caso, o anel de endomorfismos $k = End(V_R)$ é um anel de divisão (pelo Lema de Schur), logo V é um espaço vetorial à esquerda sobre k. Isto sugere que a álgebra linear pode nos fornecer uma regra no estudo da ação de R sobre o módulo simples V_R.

Para proceder mais formalmente, vamos relembrar uma definição útil da álgebra linear. Seja ${}_kV$ um espaço vetorial à esquerda sobre um anel de divisão k, e seja $E = End({}_kV)$. Um subconjunto $S \subseteq E$ é dito *m-transitivo* sobre V se, para qualquer conjunto de $n \leq m$ vetores linearmente independentes $v_1, ..., v_n$ e qualquer outro conjunto $v'_1, ..., v'_n$ em V, existe $s \in S$ tal que $(v_i)s = v'_i$ para todo i. Dizemos que S é *um conjunto denso de transformações lineares* sobre ${}_kV$ se S é m-transitivo para todo m finito. A seguinte proposição nos mostra que esta terminologia é consistente com a que vimos anteriormente.

Proposição 2.2.5. *Seja V um (k,R)-bimódulo, onde k é um anel de divisão. Sejam* $E = End({}_kV)$ *e* $\rho : R \to E$ *a aplicação natural. Então R atua densamente sobre* ${}_kV$ *se, e somente se,* $\rho(R)$ *é um anel denso de transformações lineares sobre V.*

Demonstração:

Suponha que R atua densamente sobre ${}_kV$. Então para todo $f \in E$, e para quaisquer v_1,...,v_n, $v_ir = (v_i)f$, para algum $r \in R$. Por um resultado da Álgebra Linear, temos que dados $v_1, ..., v_n$ linearmente independentes em ${}_kV$, e $v'_1, ..., v'_n \in {}_kV$, existe $f : {}_kV \to {}_kV$ tal que $(v_i)f = v'_i$, para $i = 1, ..., n$. Logo, para este f em particular, existe $r \in R$ tal que $v_ir = (v_i)f = v'_i$. Portanto $\rho(r) \in \rho(R)$ é tal que $(v_i)\rho(r) = v'_i$.

Agora, assuma que $\rho(R)$ é um anel denso de transformações lineares sobre V. Seja $f \in E$ e seja $v_1, ..., v_n \in V$. Reindexando os índices de forma conveniente, podemos assumir que $v_1, ..., v_m$ são k-linearmente independentes, e que cada v_i é uma k-combinação linear de $v_1, ..., v_m$. Como $\rho(R)$ é m-transitivo sobre V, existe $r \in R$ tal que $v_ir = (v_i)f$ para $i \leq m$. Pela linearidade, segue que esta equação vale para todo $i \leq n$. ∎

Combinando os três últimos resultados, obtemos uma generalização do Teorema de Wedderburn-Artin, apresentado no Capítulo 1. Em algumas literaturas, este resultado também é conhecido como"Teorema da Densidade".

Teorema 2.2.6. ***Estrutura para anéis primitivos à direita***. *Seja R um anel primitivo à direita e V um R-módulo à direita simples e fiel. Seja k o anel de divisão $End(V_R)$. Então R é isomorfo ao anel denso de transformações lineares sobre ${}_kV$. Mais ainda:*

(1) *Se R é artiniano à direita, então $n{:=}dim({}_kV)$ é finita, e $R \cong M_n(k)$.*

(2) *Se R não é artiniano à direita, então $dim({}_kV)$ é infinita, e para qualquer inteiro $n > 0$, existe um subanel R_n de R que admite um epimorfismo de anéis sobre $M_n(k)$.*

(Note que (1) vem do Teorema de Wedderburn-Artin para anéis artinianos à direita simples, já que estes são exatamente os anéis primitivos à direita e artinianos à direita. A prova a seguir é independente, e mais geral, que a dada no Capítulo 1.)

Demonstração:

Como V_R é fiel, a aplicação natural

$$\rho : R \to E := End({}_kV)$$

é injetiva. Por 2.2.3 e pela Proposição 2.2.5, $\rho(R)$ é um anel denso de transformações lineares sobre ${}_kV$. Isto prova a primeira parte.

Para provar as duas últimas afirmações, faremos as seguintes argumentações.

Suponha agora $dim({}_kV) = n < \infty$. Pelo Corolário 2.2.4, temos que $\rho(R) = E$, logo $R \cong M_n(k)$, e R é artiniano à direita.

Suponha agora que $dim({}_kV)$ é infinita. Fixe uma sequência de vetores linearmente independentes $v_1, v_2, ...$ em V, e seja

$$V_n = \sum_{i+1}^{n} kv_i, \text{ onde } 1 \leq n < \infty.$$

Sejam

$R_n = \{r \in R : (V_n)r \subseteq_n V\}$ (um subanel de R);

$U_n = \{r \in R : (V_n)r = 0\}$ (um ideal de R_n e um ideal à direita de R).

Então R_n/U_n atua fielmente sobre o k-espaço V_n. Pela n-transitividade de R (sobre V), qualquer transformação linear sobre k de V_n pode ser vista como a ação de algum $r \in R_n$. Portanto a aplicação natural $R_n/V_n \to End(_k(V_n))$ é um isomorfismo, resultando que $R_n/U_n \cong M_n(k)$. Mais ainda, pela $(n+1)$-transitividade, existe um $r \in R$ tal que

$$v_1 r = ... = v_n r = 0, \text{ mas } v_{n+1} r \neq 0,$$

logo $U_n \supsetneqq U_{n+1}$ para todo n. Assim, $U_1 \supseteq U_2 \supseteq ...$ é uma cadeia de ideais à direita em R estritamente decrescente, logo R não é artiniano à direita.

Assim, se R é artiniano, a segunda parte mostra que $dim(_kV) < \infty$ e a primeira parte mostra que $R \cong M_n(k)$.

Se R não é artiniano, a primeira parte mostra que $dim(_kV)$ é infinita e a segunda parte produz um subanel R_n que admite um epimorfismo sobre $M_n(k)$. ■

Capítulo 3

Anéis Fracamente Primitivos

O objetivo deste capítulo é descrever uma teoria básica de uma classe de anéis primos: os anéis fracamente primitivos. Com esta base, chegaremos em um resultado que generaliza o clássico Teorema da Densidade de Jacobson. A partir de agora, seguiremos o trabalho “Weakly Primitive Rings”de Julius Zelmanowitz (ver [15]).

Para facilitar a notação, neste capítulo escreveremos o anulador de M como $(0 : M)$, lembrando que $(0 : M) = \{r \in R : Mr = 0\}$. Lembramos ainda que um módulo uniforme é aquele onde cada par de submódulos não-nulos tem uma intersecção não-nula.

3.1 Módulos Criticamente Compressíveis

Um R-módulo não-nulo M é chamado *compressível* se pode ser imerso em cada um de seus submódulos não-nulos, e é chamado *criticamente compressível* se ele for compressível e, adicionalmente, não puder ser imerso em nenhum de seus fatores próprios. Observe que um submódulo não-nulo de um módulo criticamente compressível é também criticamente compressível.

No decorrer do texto vamos precisar das seguintes definições. Consideremos R um anel e M um R-módulo à direita.

Definição 3.1.1. *Chamamos de* submódulo singular *de M à direita ao conjunto Sing(M) =* $\{x \in M$*; (0:x) é essencial*$\}$*. M é dito singular se Sing(M) = M; e não-singular se Sing(M) = 0.*

Definição 3.1.2. *M é dito* monoforme *se todo endomorfismo parcial não-nulo de M é um monomorfismo.*

Proposição 3.1.3. *Para um módulo compressível M, as seguintes condições são equivalentes:*
(i) M é criticamente compressível.
(ii) M é monoforme.
Mais ainda, qualquer módulo que satisfaz (ii) é uniforme.

Demonstração:

$(i) \Rightarrow (ii)$. Seja $f : N \to M$ um endomorfismo parcial não-nulo de M. Como M é compressível, existe um monomorfismo $g : M \to f(N)$. Mas então a composição

$$M \xrightarrow{g} f(N) \cong N/Kerf \hookrightarrow M/Kerf$$

produz um monomorfismo de M em $M/Kerf$. Como M é criticamente compressível, segue que $Kerf = 0$, ou seja, f é monomorfismo.

$(ii) \Rightarrow (i)$. Suponha que $f : M \to M/N$ é um monomorfismo, com N um submódulo de M. Escreva $f(M) = L/N$ para algum submódulo L de M, com $N \subsetneq L \subseteq M$. Vamos chamar de $\pi : L \to L/N$ o homomorfismo canônico. Logo $h = f^{-1}\pi$

é um endomorfismo parcial não-nulo de M, e portanto é um monomorfismo (pela hipótese). Mas $N = Ker\ \pi \subseteq Ker\ h = 0$, logo $N = 0$.

Finalmente, vamos mostrar que se M satisfaz (ii) e K, L são submódulos não-nulos de M, então $K \cap L \neq 0$, ou seja, M é uniforme. De fato, se $K \cap L = 0$, a projeção de $K + L$ em L produz um endomorfismo parcial não-nulo de M com núcleo não-nulo. ■

Vamos tomar um momento para citar que grupos abelianos compressíveis são cíclicos infinitos ou cíclicos de ordem prima, e são de fato criticamente compressíveis. Um módulo simples é certamente criticamente compressível. A seguinte proposição, que pode ser encontrada em [12] nos fornecerá mais exemplos.

Proposição 3.1.4. *Seja M um R-módulo à direita uniforme não-singular tal que $Hom_R(M, N) \neq 0$ para cada submódulo não-nulo N de M. Então M é criticamente compressível.*

Demonstração:

Seja $0 \neq m$ um elemento arbitrário em M. Como o módulo é não-singular, o anulador de m não é um ideal essencial, isto é, existe um ideal à direita não-nulo I_m em R que não intercepta $(0 : m)$. Logo $mq \neq 0$ para todo $0 \neq q \in I_m$. Como m é arbitrário, temos a coleção de ideais

$$\{I_m; I_m \text{ é um ideal à direita em R e } 0 \neq m \in M\}.$$

Precisamos mostrar que todo endomorfismo parcial em M_R é um monomorfismo. Note que isto implica a compressibilidade, já que todo endomorfismo é, em particular, parcial. De fato, seja $f : U_R \to V_R$ um endomorfismo parcial, onde U e V são R-submódulos em em M e, mais ainda, V é a imagem de U. Se f não for um monomorfismo, então $f(u) = 0$ para algum $u \in U$. Suponha que $f(w) \neq 0$. Note que o submódulo uR é totalmente anulado pelo endomorfismo parcial f, mas

$f(wq) \neq 0$ para todo $q \in I_{f(w)}$. Logo f não pode anular elementos não-nulos do submódulo $wI_{f(w)}$. Entretanto, M_R é um módulo uniforme, e então $uR \cap wI_{f(w)} \neq 0$, o que gera uma contradição. De fato, neste caso, cada elemento não-nulo desta intersecção pode ser anulado e não anulado simultaneamente por f. ■

Exemplo 3.1.5. *Um ideal à direita uniforme de um anel não-singular primo é criticamente compressível.*

Como vimos na seção 1.6, um módulo quase-injetivo M é aquele onde cada endomorfismo parcial pode ser estendido a um endomorfismo de M, e todo módulo pode ser imerso em um menor módulo quase-injetivo $\overline{M}$, que nós chamamos de fecho quase-injetivo de M (que é único, a menos de isomorfismos). Vimos ainda pela Proposição 1.6.11 que $\overline{M} \cong \Lambda M$, onde Λ é o anel de endomorfismos do fecho injetivo de M. Como uma conseqüência imediata deste resultado, temos que um módulo é quase-injetivo se, e somente se, é um submódulo totalmente invariante do seu fecho injetivo. Disto, segue que $\overline{M} = \Delta M$, onde $\Delta = End(\overline{M}_R)$.

Proposição 3.1.6. *(i) Se M_R é monoforme, então os elementos de $D = End(M_R)$ têm extensões únicas para elementos de $\Delta = End(\overline{M}_R)$, e Δ é um anel de divisão. (ii) Se M_R é criticamente compressível, então D é um domínio de Ore à direita com anel de quociente à direita Δ.*

Demonstração:

(i) Suponha primeiro que $\lambda \in Hom_R(M, \overline{M})$, com $Ker\lambda \neq 0$. Queremos mostrar que $\lambda = 0$. Para isto, seja $\lambda_1 = \lambda \mid_{\lambda^{-1}(M \cap \lambda M)}$. Note que $\lambda^{-1}(M \cap \lambda M)$ é um submódulo de M. Se $\lambda \neq 0$, então $\lambda_1 \neq 0$. Como λ_1 é um endomorfismo parcial não-nulo de M, λ_1 precisa ser um monomorfismo (já que M_R é monoforme). Mas $Ker\lambda_1 = Ker\lambda \cap \lambda^{-1}(M \cap \lambda M) \neq 0$, já que M é uniforme (pela Proposição 3.1.3). Logo chegamos em uma contradição, o que estabelece que $\lambda = 0$.

Agora assuma que $\lambda \in End(\overline{M}_R)$ com $Ker\lambda \neq 0$. Vamos mostrar que $\lambda = 0$.

Para isto, seja μ um elemento arbitrário de $\Lambda = End(\widehat{M}_R)$, onde $\widehat{M}_R$ é o fecho injetivo de M contendo $\overline{M}$. Então $\lambda\mu\mid_M \in Hom_R(M, \overline{M})$, já que $\overline{M}$ é um submódulo totalmente invariante de $\widehat{M}_R$. Mais ainda, se $\mu(M) \neq 0$, então $\mu(M) \cap Ker\lambda \neq 0$, já que $\overline{M}_R$ é uniforme, logo $Ker\lambda\mu\mid_M \neq 0$. Pelo que vimos no parágrafo anterior, temos que $\lambda\mu(M) = 0$. Como $0 \neq \mu \in \Lambda$ foi arbitrário, concluímos que $\lambda\overline{M} = \lambda\Lambda M = 0$.

Logo segue diretamente que elementos de D têm extensões únicas em Δ. Conseqüentemente, podemos enxergar D como um subanel de Δ.

Vamos agora mostrar que $\Delta = End(\overline{M}_R)$ é uma anel de divisão. Para isto, seja $0 \neq \lambda \in \Delta$ um endomorfismo arbitrário. Pelo que vimos anteriormente, λ é um monomorfismo. Seja λ_1 uma extensão de λ para um endomorfismo de $\widehat{M}_R$; logo λ_1 também é um monomorfismo (caso contrário, λ não seria monomorfismo). Como M_R é uniforme, $\widehat{M}_R$ é indecomponível (ou seja, não conseguimos escrever $\widehat{M}_R$ como soma direta de submódulos), e então $\lambda_1\widehat{M} = \widehat{M}$ e segue que λ_1 é invertível. Seja $\mu_1 \in \Lambda$ o inverso de λ_1; isto é, $\mu_1\lambda_1 = 1 = \lambda_1\mu_1$ em $\widehat{M}$. Como $\overline{M}$ é um submódulo totalmente invariante de $\widehat{M}$, $\mu\lambda = 1 = \lambda\mu$, onde $\mu = \mu_1\mid_{\overline{M}}$. Logo λ possui inverso e Δ é um anel de divisão.

(ii) Agora assuma adicionalmente que M_R é compressível. Vamos mostrar que Δ é um anel de quociente à direita de D. Seja $0 \neq \lambda \in \Delta$. Então $N = M \cap \lambda^{-1}M \neq 0$, já que M é um submódulo totalmente invariante de $\overline{M}$, e podemos escolher $0 \neq \mu \in Hom_R(M, N) \subseteq D$. Então $0 \neq \lambda\mu \in D$, ou em outras palavras, $\lambda = \gamma\mu^{-1}$, para algum $\gamma \in D$. Segue daí que Δ é anel de quociente à direita de D. ■

O próximo resultado estabelece quando um módulo criticamente compressível é simples.

Corolário 3.1.7. *Se M_R é criticamente compressível, então M_R é simples precisamente quando é quase-injetivo.*

Demonstração:

Um módulo simples M é trivialmente quase-injetivo, pois o único submódulo não-nulo possível é o próprio M. Logo assuma M criticamente compressível e quase-injetivo. Pela Proposição 3.1.6, $End(M_R)$ é um anel de divisão. Então M, sendo compressível, não pode ter submódulos próprios. ■

3.2 O Teorema da Densidade

Começamos com um lema técnico, mas que nos será útil no que segue.

Lema 3.2.1. *Seja M_R um módulo quase-injetivo tal que se $mR = 0$, com $m \in M$, então $m = 0$. Sejam $m_1, ..., m_t \in M$. Então $(0 : m) \supseteq \bigcap_{i=1}^{t}(0 : m_i)$ se, e somente se, $m = \sum_{i=1}^{t} \lambda_i m_i$, para alguma escolha de $\lambda_1, ..., \lambda_t \in End(M_R)$*

Demonstração:

Assuma que $(0 : m) \supseteq \bigcap_{i=1}^{t}(0 : m_i)$. Isto implica que a aplicação

$$\gamma : (m_1, ..., m_t)R \to mR$$

dada por $\gamma((m_1, ..., m_t)r) = mr$, está bem definida.

Note que $(m_1, ..., m_t) \in M^{(t)} = M \oplus ... \oplus M$. Como M_R é quase-injetivo, γ pode ser estendido a um elemento de $Hom_R(M^{(t)}, M)$, que também vamos denotar por γ.

Agora sejam $\varepsilon_i, \pi_i, i = 1, ..., t$ a injeção canônica e a projeção canônica para $M^{(t)}$, respectivamente. Então $\sum_{i=1}^{t} \varepsilon_i \pi_i = 1$ sobre $M^{(t)}$. Assim para qualquer $r \in R$, temos

$$mr = \gamma((m_1, ..., m_t)r) = \gamma(\sum_{i=1}^{t} \varepsilon_i \pi_i (m_1 r, ..., m_t r)) = \sum_{i=1}^{t} (\gamma \varepsilon_i)(m_i r).$$

Agora seja $\lambda_i = \gamma\varepsilon_i \in End(M_R)$. Como $r \in R$ foi tomado arbitrário, temos que $(m - \sum_{i=1}^{t} \lambda_i m_i)R = 0$, e segue pela hipótese que $m = \sum_{i=1}^{t} \lambda_i m_i$.

A outra implicação é direta, e por isso vamos ocultá-la. ■

Para facilitar a apresentação do teorema, vamos chamar uma terna $(\Delta, {}_\Delta V_R, M_R)$ de *R-reticulado* se V é um (Δ, R)-bimódulo, com Δ um anel de divisão, $\Delta M = V$, e R atua fielmente sobre M (logo podemos assumir $R \subseteq End({}_\Delta V)$). Dizemos que um anel é *fracamente primitivo* se possui um módulo criticamente compressível e fiel.

Teorema 3.2.2. ***(O Teorema da Densidade).*** *Para um anel R, as seguintes condições são equivalentes:*

(i) R é fracamente primitivo.

(ii) Existe um R-reticulado (Δ, V, M) tal que, dados $v_1, ..., v_k \in V$ linearmente independentes sobre Δ, existe $0 \neq a \in \Delta$ tal que, para quaisquer elementos $n_1, .., n_k \in M$, podemos encontrar $r \in R$ com $an_i = v_i r \in M$ para cada i = 1,...,k.

(iii) Existe um R-reticulado (Δ, V, M) tal que, dado qualquer $\tau \in End({}_\Delta V)$ e Δ-subespaços finitamente gerados U e $U' = \sum_{i=1}^{k} \Delta m_i$ sobre V, com $m_1, ..., m_k \in M$, existem $r, s \in R$ com $(\tau r - s)|_U = 0$ e $r|_{U'}$ um automorfismo.

Demonstração:

$(i) \Rightarrow (ii)$. Seja M_R um módulo criticamente compressível e fiel. Sabemos da Proposição 3.1.6 que $D = End(M_R)$ é um domínio de Ore à direita com anel total de quociente $\Delta = End(\overline{M}_R)$ (o qual é um anel de divisão), onde $\overline{M}_R = \Delta M$. Temos portanto um R-reticulado $(\Delta, \overline{M}, M)$, e podemos considerar R como subanel de $End_\Delta \overline{M}$.

Primeiro vamos mostrar que $vR \neq 0$ para qualquer elemento $v \neq 0$ em $\overline{M}$. (Vamos fazer isso para usar o Lema 3.2.1). Como M_R é compressível e $vR^1 \cap M \neq 0$

(já que $\overline{M}$ é uma extensão essencial de M), podemos escolher um monomorfismo $a \in Hom_R(M, vR^1 \cap M)$. Como M_R é fiel, existe $m \in M$ e $r \in R$ com $mr \neq 0$. Logo $0 \neq am = vs$ para algum $s \in R^1$, e então

$$0 \neq a(mr) = (am)r = vsr \in vR.$$

Agora sejam $v_1, ..., v_k \in \overline{M}$ dados, linearmente independentes sobre Δ. Para $i = 1, ..., k$, seja $A_i = \bigcap_{j \neq i}(0 : v_j)$, que é um ideal à direita de R. Pelo Lema 3.2.1, $v_iA_i \neq 0$ para cada i, e segue que $(\bigcap_{i=1}^{k} v_iA_i) \cap M \neq 0$. Como M_R é compressível, podemos escolher um monomorfismo $a \in Hom_R(M, (\bigcap_{i=1}^{k} v_iA_i) \cap M)$. Então dados $n_1, ..., n_k \in M$, existe $r_i \in A_i$, para $i = 1, ..., k$, com $an_i = v_ir_i \in M$ para cada i. Logo tomando $r = \sum_{i=1}^{k} r_i$, segue que $an_i = v_ir \in M$.

$(ii) \Rightarrow (iii)$. Sejam (Δ, V, M) um R-reticulado, $\tau \in End({}_{\Delta}V)$, U e U' dois subespaços finitamente gerados de V. Seja então $U' = \sum_{i=1}^{k} \Delta m_i$. S.p.g., podemos assumir $m_1, ..., m_k$ linearmente independentes sobre Δ, pois se eles forem linearmente dependentes, podemos eliminar aqueles elementos que são uma combinação linear dos demais.

Como $V = \Delta M$ (já que (Δ, V, M) é um R-reticulado), temos que $U \subseteq \sum_{i=k+1}^{l} \Delta m_i$ $= V'$, para alguma escolha de $m_{k+1}, ..., m_l \in M$. Eliminando alguns dos $m_i' s$ para $k+1 \leq i \leq l$, se necessário, podemos assumir que o conjunto $\{m_1, ..., m_k, m_{k+1}, ..., m_l\}$ forma uma $\Delta - base$ para $W = U' + V'$. Vamos então encontrar elementos r, s em R tais que $(\tau r - s) |_W = 0$ e $r |_{U'}$ é um automorfismo.

Seja $W_h = \sum_{i=1}^{h} \Delta m_i$ e $W_0 = 0$. Vamos provar por indução em h, $0 \leq h \leq l$, que existem $r, s \in R$ com $(\tau r - s) |_{W_h} = 0$ e $r |_{U'}$ é um automorfismo.

Se $h = 0$, $W_0 = 0$, logo podemos escolher $r \in R$, por uma aplicação de (ii), com $m_ir = am_i$, $i = 1, ..., k$ e algum $a \in \Delta$, $(a \neq 0)$. Assim, $(\tau r - s) |_{W_0} = 0$, para $s \in R$

arbitrário e $r\mid_{U'}$ é um automorfismo.

Agora assuma que $1 \leq h < l$. Indutivamente podemos supor que existe $r', s' \in R$ com $(\tau r' - s')\mid_{W_{h-1}} = 0$ e $r'\mid_{U'}$ é um automorfismo.

Chamando $\tau' = \tau r' - s'$, é suficiente produzir $r, s \in R$ com $(\tau' r - s)\mid_{W_h} = 0$ e $r'\mid_{U'}$ um automorfismo. De fato, dado qualquer $v \in W_h$, $v\tau(r'r) = v(\tau r')r = v(\tau' + s')r = v(s + s'r)$ e $r'r\mid_{U'}$ é um automorfismo.

Temos que a base de W_h é dada por $\{m_1, ..., m_h\}$, a base de W_{h-1} dada por $\{m_1, ..., m_{h-1}\}$ e a base de $W = U' + V'$ dada por $\{m_1, ..., m_k, m_{k+1}, ..., m_l\}$. Vamos dividir em dois casos:

1º caso) $m_h\tau' \notin U' + W_h$

Aplicando (ii), escolhemos um elemento $0 \neq a \in \Delta$ relativo aos elementos linearmente independentes $m_1, ..., m_j, m_h\tau'$, onde $j = max(h, k)$. Então existem elementos r, s em R tais que

$$am_i = m_i r \text{ para } 1 \leq i \leq j,\ am_h = (m_h\tau')r,$$

onde os n_i's da hipótese são $m_1, ..., m_h$ e

$$a0 = m_i s \text{ para } i \neq h,\ am_h = m_h s,\ a0 = (m_h\tau')s.$$

Agora vamos mostrar que $r\mid_{U'}$ é automorfismo.

Se $h > k$, $m_i r = am_i$ é um automorfismo, já que estamos multiplicando por a elementos que são L.I. De fato, a aplicação é dada por $\varphi : U' \to U'$, onde $\varphi(m_i) = am_i$.

Se $k > h$, a aplicação é dada por $\varphi : U' \to U'$, onde $\varphi(m_i) = am_i$. se $1 \leq i \leq k$ e $\varphi(m_h\tau') = am_h$, que podemos facilmente ver que é um automorfismo.

Para $1 \leq i \leq h$, $m_i\tau' r \overset{H.I.}{=} 0 = m_i s$, e $m_h\tau' r = am_h = m_h s$. Logo $(\tau' r - s)\mid_{W_h} = 0$.

2º caso) $m_h\tau' \in U' + W_h$

Se $m_h\tau' = 0$, escolha $0 \neq a \in \Delta$ e $r \in R$ tais que $am_i = m_ir$ para $1 \leq i \leq k$, e tome $s = 0$. Nesta situação, temos que $r\mid_{U'}$ é um automorfismo, já que $am_i = m_ir$, e então basta tomar a aplicação $r = \varphi : U' \to U'$, onde $\varphi(m_i) = am_i$. Temos também que $\tau'r - s\mid_{W_h}= 0$, pois pela hipótese de indução $\tau'r - s\mid_{W_h}= 0$ e $m_h\tau' = 0$.

Portanto, vamos supor $0 \neq m_h\tau' = \sum_{\mu=1}^{\lambda} c_{i_\mu}m_{i_\mu}$, com cada $0 \neq c_{i_\mu} \in \Delta$ e $1 \leq i_1 < ... < i_\lambda \leq j = max(h, k)$.

Novamente por (ii) escolhemos um elemento $0 \neq a \in \Delta$ com respeito aos elementos L.I. $m_1, ..., m_j$; e escolhemos $0 \neq b \in \Delta$ com respeito aos elementos L.I. $a^{-1}c_{i_1}m_{i_1}, ..., a^{-1}c_{i_j}m_{i_j}$ e os m_i's restantes ($1 \leq i \leq j$, i diferente de qualquer i_μ). Então existe $r, s \in R$ com:

$$bm_{i_\mu} = (a^{-1}c_{i_\mu}m_{i_\mu})r \in M \text{ para } 1 \leq \mu \leq \lambda,$$
$$bm_i = m_ir \text{ para } i \text{ diferente de qualquer } i_\mu \text{ e}$$
$$a0 = m_is \text{ para } i \neq h,\ a(\sum_{\mu=1}^{\lambda} bm_{i_\mu}) = m_hs.$$

Observe que a última escolha é possível, pois $\sum_{\mu=1}^{\lambda} bm_{i_\mu} \in M$; e, claramente, $r\mid_{U'}$ é automorfismo.

Agora, para $1 \leq i \leq h$, $m_i\tau'r \overset{H.I.}{=} 0 = m_is$ e $m_h\tau'r = \sum_{\mu=1}^{\lambda} c_{i_\mu}m_{i_\mu}r = \sum_{\mu=1}^{\lambda} aa^{-1}c_{i_\mu}m_{i_\mu}r = \sum_{\mu=1}^{\lambda} abm_{i_\mu}r = m_hs$. Logo $(\tau'r - s)\mid_{W_h}= 0$, como queríamos.

$(iii) \Rightarrow (i)$. Seja M como em (iii). Vamos mostrar que todo R-submódulo cíclico não trivial de M é um módulo criticamente compressível e fiel.

Afirmação 1. Para qualquer $0 \neq m \in M$, mR^1 é fiel.

Para isto, seja $0 \neq t \in R$. Logo $Mt \neq 0$, já que M_R é fiel ((Δ, V, M) é um R-reticulado). Portanto podemos escolher $0 \neq n \in M$ com $nt \neq 0$.

Escolha $\tau \in End(_{\Delta}V)$ com $m\tau = n$ e tome $r, s \in R$ tais que $\tau r = s$ em Δm e $r \mid_{\Delta n}$ é um automorfismo. Então

$$mst = m\tau rt = nrt \neq 0,$$

pois $0 \neq nr \in \Delta n$ e $nt \neq 0$. Logo $mR^1 t \neq 0$ e mR^1 é fiel.

Afirmação 2. mR^1 é compressível.

Seja N_R um submódulo de mR^1 não-nulo. Seja $0 \neq n \in N$ e tome $\tau \in End(_{\Delta}V)$ com $n\tau = m$. Escolha $r, s \in R$ com $\tau r = s$ em Δn e $r \mid_{\Delta m}$ um automorfismo. Então existe $a \in \Delta$ com $0 \neq mr = am$ e logo $0 \neq am = mr = n\tau r = ns \in N$. Portanto, $a \in Hom_R(mR^1, N)$ e $Ker\ a = \{mx \in mR^1 / amx = 0\} = 0$ (isto porque $a(mx) = a(m)x = mrx = (mx)r$, mas $r \mid_{\Delta m}$ é isomorfismo, logo $(mx)r = 0$ implica que $mx = 0$).

Afirmação 3. mR^1 é criticamente compressível.

Pela Proposição 3.1.3, basta mostrar que mR^1 é monoforme. De fato, podemos provar que M_R é monoforme. Para isto, seja N_R um submódulo de M_R e seja $0 \neq \lambda \in Hom_R(N, M)$, digamos $\lambda m \neq 0$ para algum $m \in N$.

Dado $0 \neq n \in N$ arbitrário, escolha $\tau \in End_{\Delta}V$ com $n\tau = m$ e tome $r, s \in R$ com $\tau r = s$ em Δn e $r \mid_{\Delta \lambda m}$ um automorfismo. Então

$$(\lambda n)s = \lambda(ns) = \lambda(n\tau r) = \lambda(mr) = (\lambda m)r \neq 0,$$

logo $\lambda n \neq 0$ e segue que λ é um monomorfismo. ■

Dizemos que R é um *anel fracamente denso* de transformações lineares (à direita) quando o item (ii) do Teorema acima acontece; e dizemos que R é uma *ordem local* (à direita) em $End(_{\Delta}V)$ quando (iii) acontece.

Muitas variações das afirmações do Teorema da Densidade são possíveis. Vamos listar algumas delas, fazendo alguns comentários.

1. Podemos enfatizar que quando M_R é um módulo criticamente compressível e fiel, R é um subanel fracamente denso de $End({}_\Delta\overline{M})$, onde $\Delta = End(\overline{M}_R)$.

2. Se R é um anel fracamente denso de transformações lineares com respeito ao R-reticulado (Δ, V, M), então R é uma ordem local em $End({}_\Delta V)$.

3. Na afirmação (ii), o elemento $a \in \Delta$ é, de fato, escolhido em $D = End(M_R)$.

4. Quando provamos $(iii) \Rightarrow (i)$, usamos somente a propriedade $\Delta M \subseteq V$, e não $\Delta M = V$. E precisamos da hipótese apenas para subespaços 2-dimensionais.

5. Na demonstração de $(ii) \Rightarrow (iii)$ podemos observar que dois aspectos da hipótese foram fundamentais. Primeiro, o elemento $a \in \Delta$ depende somente dos elementos linearmente independentes $v_1, ..., v_k$ e não dos $n_i's$ (veja o 1º caso); e segundo, usamos o fato de que v_i pode ser escolhido em $V \setminus M$ (veja o 2º caso).

6. Na demonstração de $(ii) \Rightarrow (iii)$, com $m_1, ..., m_k \in M$ linearmente independentes sobre Δ, escolhendo r, s em R tais que $(\tau r - s)|_U = 0$ e $r|_{U'}$ é um automorfismo, podemos aplicar (ii) novamente para encontrar elementos $0 \neq a \in \Delta$, $t \in R$ com $am_i = m_i rt$. Então, substituindo r e s por $r_1 = rt$ e $s_1 = st$ respectivamente, temos $(\tau r_1 - s_1) \mid_U = 0$ e $m_i r_1 = am_i \neq 0$, para cada i. De fato, a escolha do elemento r em (iii) pode ser feita de maneira que r "atue como um escalar"sobre os elementos linearmente independentes $m_1, ..., m_k$.

7. Finalmente, vamos enunciar uma afirmação equivalente a condição (iii). Os detalhes da prova são muito parecidos com os que apresentamos anteriormente, e por isso não vamos colocá-los aqui.

$(iii)'$ Existe um R-reticulado (Δ, V, M) tal que dado qualquer $\tau \in End({}_\Delta V)$ e elementos $m_1, ..., m_k \in M$ linearmente independentes sobre Δ, podemos encontrar $r, s \in R$ com $m_i \tau r = m_i s$ e $0 \neq m_i r \in \Delta m_i$, para cada i.

Lembramos aqui duas definições que serão necessárias. Seja Q um subanel de

R. Dizemos que Q é uma *ordem à direita* em R se $1 \in R$, existem elementos regulares de Q que são invertíveis em R, e todo elemento de R é da forma ba^{-1}, com $a, b \in Q$ e a regular. Seja M um R-módulo à direita. Dizemos que M_R tem *dimensão uniforme* n se existe um submódulo essencial $V \subseteq_e M$ que é uma soma direta de n submódulos uniformes.

Recordamos também que um anel R é dito um anel de Goldie à direita se R satisfaz ACC para anuladores à direita e possui dimensão uniforme à direita finita. O próximo resultado é clássico e apresenta propriedades básicas dos anéis de Goldie. Uma prova pode ser encontrada em [13].

Teorema 3.2.3. ***Teorema de Goldie.*** *As seguintes condições em um anel R são equivalentes:*

(i) R é Goldie à direita semiprimo;

(ii) R é semiprimo, Sing R = 0 e dimensão uniforme à direita de R é finita;

(iii) R tem um anel quociente à direita Q que é artiniano semi-simples. Mais ainda, R é primo se, e somente se, Q é simples.

No caso em que M é um R-módulo criticamente compressível e fiel com $dim({}_\Delta\overline{M}) = k < \infty$, tomando $U = U' = \overline{M}$ na condição (iii) do Teorema da Densidade, vemos que R é uma ordem à direita no anel artiniano simples $End({}_\Delta\overline{M}) \cong \Delta_k$. Logo obtemos a seguinte caracterização de ordens em anéis artinianos simples.

Corolário 3.2.4. *R é uma ordem à direita em um anel artiniano simples se, e somente se, R possui um módulo criticamente compressível e fiel M tal que $\bigcap_{i=1}^{t}(0 : m_i) = 0$ para algum conjunto finito de elementos $m_1, ..., m_t$ em M (ou equivalentemente, tal que $dim({}_\Delta\overline{M}) < \infty$).*

Demonstração:

Assuma que R é uma ordem à direita em um anel artiniano simples. Então R é um anel primo, possui dimensão finita, é não-singular, e satisfaz a condição da cadeia descendente para ideais anuladores à direita. Tome M um ideal à direita uniforme de R, e escolha $m_1, ..., m_t \in M$ tal que $(0 : m_1, ..., m_t)$ é minimal (percorrendo todos anuladores de subconjuntos finitos de M). Então claramente $(0 : m_1, ..., m_t, m) = (0 : m_1, ..., m_t)$ para qualquer $m \in M$ e, portanto, $(0 : m_1, ..., m_t) = (0 : M) = 0$, já que R é primo. Mais ainda, como foi no Exemplo 3.1.5, M é um módulo criticamente compressível.

Reciprocamente, se tal módulo existe, então podemos aplicar o Lema 3.2.1 para ver que $dim({}_{\Delta}\overline{M}) < \infty$. Então, pelas observações que precedem este corolário, e aplicando (iii) do teorema para $V = \overline{M}$, temos que R é uma ordem à direita em $End({}_{\Delta}\overline{M})$. ■

3.3 Propriedades de Anéis Fracamente Primitivos

Nesta seção vamos discutir algumas propriedades interessantes dos anéis fracamente primitivos. Em particular, temos que todo anel fracamente primitivo é primo. Começaremos com o seguinte resultado:

Lema 3.3.1. *Se M_R é um módulo compressível, então $(0 : M)$ é um ideal primo de R, e (0:M) = (0:N) para qualquer submódulo não-nulo N de M.*

Demonstração:

Assuma I e J ideais de R tais que $I \supsetneq (0 : M)$ e $J \supsetneq (0 : M)$. Então $MI \neq 0$, logo podemos escolher um monomorfismo $f \in Hom_R(M, MI)$, já que M_R é compressível. Como também temos $MJ \neq 0$, $0 \neq f(MJ) = f(M)J \subseteq MIJ$. Logo $IJ \nsubseteq (0 : M)$ e, pela Proposição 1.5.2, item (5), isto prova que $(0 : M)$ é um ideal primo.

A segunda afirmação é clara, pois qualquer submódulo não-nulo de M contém uma cópia de M. ■

Temos então a seguinte conseqüência:

Corolário 3.3.2. *Um anel R fracamente primitivo é primo.*

Demonstração:

Seja M_R um módulo criticamente compressível e fiel. Então $0 = (0 : M)$ é primo (pelo lema), e portanto R é primo. ■

No Teorema 2.2.6 vimos que um anel primitivo R é um anel de matrizes finito Δ_n sobre um anel de divisão Δ, ou possui subanéis, um para cada inteiro $t \geq 1$, que mapeia homomorficamente Δ_t. O próximo teorema nos fornece uma generalização deste resultado para anéis fracamente primitivos.

Teorema 3.3.3. *Se R é um anel fracamente primitivo, então:*
(i) R é uma ordem à direita em um anel de matrizes Δ_t, para algum anel de divisão Δ, e neste caso R contém um subanel isomorfo à D_t para alguma ordem à direita D de Δ; ou
(ii) Para cada inteiro positivo t, existe uma ordem à direita D de Δ e um subanel de R que mapeia homomorficamente e sobrejetivamente D_t.

Demonstração:

Seja M um R-módulo criticamente compressível e fiel. Pelo Teorema da Densidade, R é um subanel fracamente denso de $End({}_{\Delta}\overline{M})$, onde $\Delta = End(\overline{M}_R)$.

Suponha que $dim({}_{\Delta}\overline{M}) \geq t$ e escolha $m_1, ..., m_t \in M$ linearmente independentes sobre Δ. Para cada $i = 1, ..., t$, seja $A_i = \bigcap_{j \neq i}(0 : m_j)$. Pelo Lema 3.2.1, $A_i \nsubseteq (0 : m_i)$ para cada i, pois caso contrário, $m_i = \sum_{i \neq j} \lambda_j m_j$, o que não pode acontecer, porque os $m_i's$ são linearmente independentes. Portanto $N = \bigcap_{i=1}^{t} m_i A_i$ é um submódulo não-nulo de M_R, já que o fato de M_R ser criticamente compressível implica que M_R é monoforme, e portanto, uniforme (Proposição 3.1.3), logo $m_i A_i \cap m_j A_j \neq 0$. Seja $D = \{a \in \Delta / aM \subseteq N\}$; um cálculo fácil verfica que D é uma ordem à direita em Δ. De fato, dado $0 \neq \lambda \in \Delta$, $\lambda^{-1}N \cap N \neq 0$; então, escolhendo $0 \neq a \in D$ tal que $aM \subseteq \lambda^{-1}N \cap N$ temos que $0 \neq \lambda a \in D$. Logo existe $b \in D$ tal que $\lambda a = b$, ou seja, $\lambda = ba^{-1}$, com $a, b \in D$ e a regular em D.

Agora tome $W = \sum_{i=1}^{t} Dm_i$, $W' = \sum_{i=1}^{t} D^1 m_i$. Observe que $Hom_D(W', W) \cong D_t$. Dado $\varphi \in Hom_D(W', W)$, φ é bem determinado pelos valores $m_i\varphi = \sum_{j=1}^{t} d_{ij} m_j$, $d_{ij} \in D$, $i = 1, ..., t$. Como cada $d_{ij} m_j \in N$, podemos escrever cada $d_{ij} m_j = m_i r_{ij}$, para algum $r_{ij} \in A_i$. Então, $m_i\varphi = \sum_{j=1}^{t} m_i r_{ij} = m_i r_i$, onde $r_i = \sum_{j=1}^{t} r_{ij} \in A_i$. Colocando $r = \sum_{i=1}^{t} r_i$, temos que $m_i\varphi = m_i r$, para cada i. Tomando o conjunto $S = \{r \in R / W'r \subseteq W\}$, a aplicação que manda $r \mapsto$ (multiplicação à direita por r em W') nos fornece um homomorfismo de S sobre $Hom_D(W', W) \cong D_t$ com núcleo $K = \{r \in R / W'r = 0\}$.

Se, de fato, $dim({}_{\Delta}\overline{M}) = t$, então $m_1, ..., m_t$ fomam uma base para ${}_{\Delta}\overline{M}$ e $K = 0$, já que M_R é fiel. Neste caso, R é uma ordem à direita em $End({}_{\Delta}\overline{M})$ pelo Corolário 3.2.4, e S é um subanel de R isomorfo à D_t. ■

Observamos que a escolha de D neste teorema depende somente do inteiro t. Então, de fato, podemos escrever $D = D^{[t]}$. Se examinarmos a prova mais cuidadosamente, podemos perceber que se $dim({}_{\Delta}\overline{M}) = \infty$ e $m_1, m_2, ... \in M$ são linearmente independentes sobre Δ, então $D^{[1]} \supset D^{[2]} \supset ...$

3.4 Anéis Primos com Ideais Criticamente Compressíveis

Em [1], um anel primo com um ideal à direita uniforme não-singular é caracterizado como uma ordem local (em um anel de transformações lineares de um espaço vetorial sobre um anel de divisão) que contém transformações lineares de posto finito. Nosso próximo resultado associa esta classe de anéis com anéis fracamente primitivos.

Teorema 3.4.1. *Para um anel R, as seguintes afirmações são equivalentes:*
(i) R é um anel primo com um ideal à direita uniforme e não-singular.
(ii) R é uma ordem local no anel de transformações lineares $End({}_\Delta V)$ e R possui uma transformação linear não-nula de posto finito.
(iii) R tem um ideal à direita criticamente compressível e fiel.

Demonstração:

$(i) \Rightarrow (ii)$. Seja U um ideal à direita uniforme e não-singular de R. Como R é primo, pelo que vimos no Exemplo 3.1.5, U é um R-módulo criticamente compressível e fiel. Logo R é um subanel fracamente denso de $End({}_\Delta\overline{U})$, onde $\Delta = End(\overline{U}_R)$, e R é uma ordem local (pelo Teorema da Densidade). Seja $0 \neq u \in U$; então para qualquer elemento $v \in \overline{U}$, $(0 : vu) \supseteq (0 : u)$. Logo pelo Lema 3.2.1, $vu \in \Delta u$. Como $v \in \overline{U}$ é arbitrário, $\overline{U}u \subseteq \Delta u$. Portanto, o elemento $u \in U$ representa uma transformação linear de ${}_\Delta\overline{U}$ de posto 1, que é não-nula já que $Uu \neq 0$.

$(ii) \Rightarrow (iii)$. Suponha que R é uma ordem local com respeito ao R-reticulado (Δ, V, M), e seja $0 \neq r \in R$ uma transformação linear de posto finito sobre ${}_\Delta V$. Primeiro, vamos mostrar que R contém uma transformação linear de posto 1.

Como $V = \Delta M$, podemos escrever $Vr \subseteq \sum_{i=1}^{t} \Delta m_i$ com $m_1, ..., m_t \in M$, linearmente independentes sobre Δ.

S.p.g., podemos assumir que $\sum_{i=1}^{t} \lambda_i m_i \in Vr$, com cada $\lambda_i \in \Delta$ e $\lambda_1 \neq 0$. Escolha $\tau \in End({}_\Delta V)$ com $m_1\tau = m_1$ e $m_i\tau = 0$ para $1 < i \leq t$. Pela hipótese, existe $r_1, s_1 \in R$ tais que $\tau r_1 = s_1$ sobre $U = \sum_{i=1}^{t} \Delta m_i$ e $r_1 \mid_{\Delta m_1}$ é um automorfismo. Então $Vrs_1 \subseteq \sum_{i=1}^{t} \Delta m_i s_1 = \sum_{i=1}^{t} \Delta m_i \tau r_1 = \Delta m_1 r_1 = \Delta m_1$ e, similarmente, $(\sum_{i=1}^{t} \lambda_i m_i)s_1 = (\sum_{i=1}^{t} \lambda_i m_i)\tau r_1 = \lambda_1 m_1 r_1 \neq 0$ em Vrs_1. Logo $rs_1 \in R$ representa uma transformação linear de posto 1.

Vamos assumir agora que $r \in R$ é uma transformação linear de posto 1 sobre ${}_\Delta V$, e vamos mostrar que o ideal à direita rR é um ideal à direita criticamente compressível e fiel. É claro que rR é fiel, pois R é um anel primo.

Para ver que rR é compressível, seja $0 \neq I_R \subseteq rR$. Então $Ir \neq 0$, pois caso contrário $I^2 = 0$, o que contradiz o fato de R ser primo. Logo podemos escolher $0 \neq t \in I$ com $tr \neq 0$. Como r tem posto 1, $Vtr = Vr$. Logo para qualquer elemento $s \in R$,

$$rs = 0 \Leftrightarrow Vrs = 0 \Leftrightarrow Vtrs = 0 \Leftrightarrow trs = 0.$$

Portanto a aplicação $rR \to I$ definida por $rs \mapsto trs$ está bem definida e é um monomorfismo de rR em I, e segue que rR é compressível.

Falta mostrarmos que rR é criticamente compressível. Para isto, suponha que $f : rR \to rR/I$ é um R-homomorfismo com $0 \neq I_R \subseteq rR$; precisamos mostrar que $Kerf \neq 0$. Como fizemos anteriormente, podemos escolher um elemento $t \in I$ com $tr \neq 0$. Tome qualquer elemento não-nulo $s \in rR$, e escreva $f(s) = s' + I$, com $0 \neq s' \in rR$. Como $V = \Delta M$, podemos escolher um elemento $m \in M \setminus Ker\ r$; então $V = Ker\ r \oplus \Delta M$ já que r possui posto 1. Observe que, pelo mesmo motivo, para qualquer elemento não-nulo r' de rR, $Ker\ r' = Ker\ r$. Logo $mr' \neq 0$, e a ação de r' sobre V está completamente determinada pelo valor mr'.

Agora defina a transformação linear $\tau \in End({}_{\Delta}V)$ por $(mt)\tau = ms'$ e $(Ker\ r)\tau = 0$; isto é possível porque $tr \neq 0$ implica que $mtr \neq 0$, e portanto $V = Ker\ r \oplus \Delta mt$. Usando a hipótese que R é uma ordem local em $End({}_{\Delta}V)$, existe u e v em R com $\tau u = v$ em Δmt e com $u\mid_{\Delta ms+\Delta ms'}$ um automorfismo. Logo $0 \neq msu$ e $0 \neq ms'u = mt\tau u = mtv$. Portanto, $s'u = tv \in I$ e $f(su) = f(s)u = s'u + I = I$, de onde concluímos que $0 \neq su \in Kerf$.

$(iii) \Rightarrow (i)$. Suponha que I é um ideal à direita criticamente compressível e fiel. Então R é um anel primo (pelo Corolário 3.3.2) e I_R é um módulo uniforme (pela Proposição 3.1.3). Logo precisamos mostrar que I_R é não-singular. Como $I^2 \neq 0$, podemos escolher $t \in I$ com $tI \neq 0$. Considere $f \in End(I_R)$ definido por $f(r) = tr$; $f \neq 0$, logo f é um monomorfismo, já que I_R é monoforme (Proposição 3.1.3). Então $I \cap (0 : t) = 0$, e portanto $t \notin Sing(I)$. Mas I_R é compressível, e isto implica que $Sing(I) = I$ ou $Sing(I) = 0$. Logo precisamos ter $Sing(I) = 0$, ou seja, I é um R-módulo não-singular. ∎

Referências Bibliográficas

[1] S. A. Amitsur, *Rings of Quocients and Morita contexts*, J. Algebra, 17 (1971), 273-298.

[2] G. M. Bergman, *A Ring Primitive on the Right but not on the Left*, Proc. Amer. Math. Soc., 15(3)(1964), 473-475.

[3] R. K. Dennis; B. Farb, *"Noncommutative Algebra"*, Graduate Texts in Mathematics, Springer-Verlag, 1993.

[4] C. Faith, *"Lectures on Injective Module and Quocient Rings"*, Lectures Notes in Math., Vol. 49, Springer-Verlag, Berlin, 1967.

[5] M. Ferrero, *"Teorema de Estructura para Álgebras Semisimples"*, Escuela Venezolana de Matemáticas, 2002.

[6] M. Ferrero, *"Ideais Primos em Extensões de Anéis"*, XIII Escola de Álgebra - UNICAMP, Campinas, 1994.

[7] N. Jacobson, *"Structure of rings"*, Amer. Math. Soc. Colloq. Publ., Vol. 37, Providence, R. T., 1964.

[8] A. V. Jategaonkar, *A Counterexample in Ring Theory and Homological Algebra*, J. Algebra, 12(1969), 418-440.

[9] T. Y. Lam, *"A first course in noncommutative rings"*, Springer-Verlag, 1991.

[10] T. Y. Lam, *"Lectures on Modules and Rings"*, Graduate Texts in Mathematics, Springer, 1942.

[11] J. Lambek, *"Lectures on Rings and Modules"*, Chelsea Publishing Company, New York, NY, 1976.

[12] S. V. Limarenko, *Weakly Primitive Superrings*, Journal of Mathematical Sciences, vol. 139, nº 4, 2006.

[13] J. C. McConnell; J. C. Robson, *"Noncommutative Noetherian Rings"*, A Wiley-Interscience series of Texts, Monographs and Tracts, Pure and Applied Mathematics, 1988.

[14] A. Sant'Ana, *Distributividade em anéis e módulos*, Escola de Verão 2008 - UFSC, 2008.

[15] J. Zelmanowitz, *Weakly Primitive Rings*, Comm. Algebra, 9 (1981), 23-45.